Michelle Morris,
Managing Director / Rheolwr Gyfarwyddwr

T: 01495 356011 **Ext./Est:** 6011

E: committee.services@blaenau-gwent.gov.uk

Contact:/Cysylltwch â: Democratic Services

Cyngor Bwrdeistref Sirol
Blaenau Gwent
County Borough Council

THIS IS A MEETING WHICH THE PUBLIC ARE ENTITLED TO ATTEND

1st October, 2020

Dear Sir/Madam

JOINT EDUCATION AND LEARNING & SOCIAL SERVICES SCRUTINY COMMITTEE (SAFEGUARDING)

A meeting of the Joint Education and Learning & Social Services Scrutiny Committee (Safeguarding) will be held in virtually via Microsoft Teams - if you would like to attend this meeting live via Microsoft Teams please contact committee.services@blaenau-gwent.gov.uk on Thursday, 8th October, 2020 at 10.00 am.

Please note that a pre and post meeting will be held 30 minutes prior to the start and following the conclusion of the meeting for members of the committee.

Yours faithfully

Michelle Morris
Managing Director

AGENDA **Pages**

1. SIMULTANEOUS TRANSLATION

You are welcome to use Welsh at the meeting, a minimum notice period of 3 working days is required should you wish to do so. A simultaneous translation will be provided if requested.

2. APOLOGIES

To receive.

3. DECLARATIONS OF INTERESTS AND DISPENSATIONS

To consider any declarations of interests and dispensations made.

4. JOINT EDUCATION & LEARNING AND SOCIAL SERVICES SCRUTINY COMMITTEE (SAFEGUARDING) MINUTES 5 - 12

To receive the Minutes of the Joint Education & Learning and Social Services Scrutiny Committee (Safeguarding) held on 2nd December, 2019.

(Please note the Minutes are submitted for points of accuracy only)

5. ACTION SHEET - 2ND DECEMBER 2019 13 - 14

To receive the Action Sheet.

6. TIME OF FUTURE MEETINGS

To consider.

7. 360 DEGREE SAFE ONLINE SAFETY POLICY FOR SCHOOLS 15 - 100

To consider the report of the Interim Corporate Director Education.

8. LOCAL GOVERNMENT EDUCATION SERVICES SAFEGUARDING POLICY 101 - 174

To consider the report of the Interim Corporate Director Education.

9. SAFEGUARDING PERFORMANCE INFORMATION FOR SOCIAL SERVICES – 1ST APRIL 2019 TO 31ST MARCH 2020 175 - 190

To consider the report of the Corporate Director Social Services.

10. ADULT SAFEGUARDING REPORT 1ST APRIL 2019 TO 31ST MARCH 2020 191 - 198

To consider the report of the Corporate Director Social Services.

To: Councillor S. Thomas (Chair)
Councillor D. Bevan
Councillor G. Collier
Councillor M. Cook
Councillor G. A. Davies
Councillor G. L. Davies
Councillor M. Day
Councillor P. Edwards
Councillor L. Elias
Councillor K. Hayden
Councillor W. Hodgins
Councillor J. Holt
Councillor C. Meredith
Councillor M. Moore
Councillor J. C. Morgan
Councillor J. P. Morgan
Councillor L. Parsons
Councillor G. Paulsen
Councillor K. Rowson
Councillor T. Sharrem
Councillor T. Smith
Councillor B. Summers
Councillor H. Trollope
T. Baxter
A. Williams

All other Members (for information)
Manager Director
Chief Officers

This page is intentionally left blank

COUNTY BOROUGH OF BLAENAU GWENT

REPORT TO: **THE CHAIR AND MEMBERS OF THE JOINT EDUCATION & LEARNING AND SOCIAL SERVICES SCRUTINY COMMITTEE (SAFEGUARDING)**

SUBJECT: **JOINT EDUCATION & LEARNING AND SOCIAL SERVICES SCRUTINY COMMITTEE (SAFEGUARDING) – 2ND DECEMBER, 2019**

REPORT OF: **DEMOCRATIC SUPPORT OFFICER**

PRESENT: COUNCILLOR S. THOMAS (CHAIR)

Councillors: H. Trollope
M. Cook
G.A. Davies
P. Edwards
K. Hayden
W. Hodgins
J. Holt
J. Millard
J.C. Morgan
K. Pritchard
K. Rowson
T. Smith
B. Summers

AND: Corporate Director of Social Services
Head of Education Transformation
Service Manager for Development & Commissioning
Service Manager, Children's Services (Safeguarding)
Safeguarding in Education Manager
Scrutiny & Democratic Officer / Advisor

ITEM	SUBJECT	ACTION
No. 1	**SIMULTANEOUS TRANSLATION** It was noted that no requests had been received for the simultaneous translation service.	

No. 2	**APOLOGIES** Apologies for absence were received from Councillors D. Bevan, L. Elias, C. Meredith, A. Moore, G. Paulsen and T. Sharrem.	
No. 3	**DECLARATIONS OF INTEREST AND DISPENSATIONS** There were no declarations of interest or dispensations reported.	
No. 4	**JOINT EDUCATION & LEARNING AND SOCIAL SERVICES SCRUTINY COMMITTEE (SAFEGUARDING)** The Minutes of the Joint Education & Learning and Social Services Scrutiny Committee (Safeguarding) Meeting held on 15th July, 2019 were submitted. The Committee AGREED that the Minutes be accepted as a true record of proceedings.	
No. 5	**ACTION SHEET – 15TH JULY, 2019** The action sheet arising from the meeting of the Joint Education & Learning and Social Services Scrutiny Committee (Safeguarding) held on 15th July, 2019 was submitted, whereupon:- **Item 6 – Safeguarding Performance Information for Social Services and Education** A Member suggested that to capture the information regarding in year transfers graphs be included with the data. The Education Transformation Manager said that regarding out of county pupils no detailed information was available, although the Department did try to pursue this information with schools and other local authorities. The Committee AGREED, subject to the foregoing, that the action sheet be noted.	

No. 6	**EXECUTIVE DECISION SHEET FOR THE JOINT EDUCATION & LEARNING AND SOCIAL SERVICES SCRUTINY COMMITTEE (SAFEGUARDING)** Consideration was given to the Executive Decision Sheet. The Committee AGREED that the Executive Decision Sheet be noted.	
No. 7	**SAFEGUARDING PERFORMANCE INFORMATION FOR SOCIAL SERVICES AND EDUCATION – 1ST APRIL TO 30TH JUNE 2019** Consideration was given to the report of the Service Manager, Children's Services and the Strategic Education Improvement Manager, which was presented to provide Members with safeguarding performance information from the Council with a focus on analysis from Children's Social Services and Education from 1st April to the 30th June, 2019. The Service Manager, Children's Services spoke to the report and highlighted the main points contained therein. **Impact on Budget** With reference to court applications and legal costs, the Service Manager said that the number of court applications was stable and the Safeguarding Team were now working at full capacity and both had a positive impact on the budget, although it was sometimes necessary to commission an external consultant for Court appearances. The Director of Social Services commented that market testing had been undertaken and work was ongoing to see if other local authorities could provide Blaenau Gwent with this service. A Member requested that for future reporting graphs be located near to the relevant text for clarification. The Service Manager said that the format of the report would be looked at for clarification purposes. **Social Services** A Member enquired if the police were the highest source of referrals. The Service Manager said that the Detective	

Sergeant (DS) role in the Information Advice and Assistance service (IAA) was making positive contributions to the safeguarding process. Referrals from police had not reduced but the quality of information received had improved which resulted in better decision making through preventative services such as the Early Action Together programme. The Member also enquired regarding Leisure Trust referrals. The Service Manager confirmed that all staff were trained in level 1 safeguarding to recognise signs of abuse and some referrals from police may have originated from Leisure Trust staff. The Head of Education Transformation commented that the Leisure Trust had lead officers for safeguarding but referrals may be low as most leisure provision was open access and assured Members that arrangements were secure.

Categories of abuse

In response to a Member's question regarding the main category of abuse, the Service Manager said that the main category was neglect, this was the highest form due to reasons such as parenting, home or being exposed to vulnerabilities re poverty lack of finances. The second highest was emotional abuse, mental health abuse would present as emotional abuse so the secondary category would go hand in hand. Although challenging preventative measures were used through partnership working, education and informing parents of the impact of emotional abuse on the child.

A Member pointed out an error on page 37, Fig 2.4 Breakdown of children on child protection register, the information relating to Unknown should read Male.

Councillors Martin Cook and Wayne Hodgins left the meeting at this juncture.

Education Information

The Safeguarding in Education Manager presented the Education information.

A Member enquired regarding the high number of restrictive physical interventions during the Autumn term. The Head of Education Transformation explained the Autumn term

	generally was the longest term; however, the trend was consistent with previous reporting information. The Directorate was looking at trends and would provide commentary to support the data presented within future reports. A Member commented that Members needed to be confident that physical intervention incidents were being reduced and that it was important that performance data be submitted in a timely manner for Members consideration of up to date information. The Safeguarding in Education Manager assured Members that they could be confident that the performance data was correct and that work was being undertaken to try to reduce restrictive physical interventions. In relation to Elected Home Educated (EHE) pupils, the Head of Education Transformation said that lengthy Scrutiny discussions had taken place and the Council was working in line with Welsh Government requirements. With reference to Operation Encompass a Member enquired if referrals passed onto schools was actioned. The Safeguarding in Education Manager said that Operation Encompass allowed schools to be aware that an incident had occurred and respond appropriately to that pupil's situation. Feedback from teachers had been positive, they found the information helpful in raising their awareness and understanding of pupils circumstances. In response to a Member's question regarding trends for September 2018 to September 2019 for Elected Home Educated pupils (EHE), the Head of Education Transformation said that the Education Service would be aware of the reasons parents choose to home educate with many parents deciding on this approach at the start of the academic year. Six secondary age pupils had become EHE in April to July 2019, the Education Welfare Service would have reviewed the reasons why the pupils had been removed. A Member enquired how many pupils were EHE as at December 2019. The Head of Education Transformation	Head of Education Transforma

	said that as the figure changed regularly he would forward this information onto Members directly. A Member commented that home visits for EHE pupils were currently once a year and enquired what progress the Directorate had been made regarding this issue. The Director of Social Services said that current Welsh Government regulations stated once a year home visits. A letter had been sent to the Welsh Government with a view to strengthen safeguarding in EHE pupils from all the regional Directors of Education and Directors of Social Services and there was a consultation on a new proposal, he hoped that the number of home visits would change in future and he would take Members views forward. It was noted that Social Workers would undertake visits if there were safeguarding concerns. The Committee AGREED to recommend that the report be accepted and endorse Option 1; namely that the approach and information detailed in the report be accepted.	tion
No. 8	**ADULT SAFEGUARDING REPORT – 1ST APRIL TO 30TH JUNE 2019** Consideration was given to the report of the Head of Adult Services which was presented to provide Members with safeguarding performance information relating to Adult Services from 1st April to the 30th June, 2019. The Service Manager for Development & Commissioning spoke to the report and highlighted the main points contained therein. In response to a Member's question regarding the Intermediate Care Fund (ICF), the Director of Social Services said that funding had been secured up to March 2021 and discussions were underway for securing funding beyond this point but there were no guarantees. A Member referred to domestic abuse cases for this quarter and enquired if they were the same or different issues reported in the last quarter. The Service Manager said that some issues were similar, however, it was difficult to report as some issues overlapped. The majority of cases were internal and timelines had been strengthened, for example	

	where a theft had occurred and the police were involved if no evidence could be found this would then become an internal issue. A Member enquired if there had been any prosecutions. The Service Manager said that one individual at risk was being managed and presented to the police. If there were allegations against a carer the Agency would need to suspend that carer and replace with another. A Member referred to the high number of unknowns on the person alleged responsible table. The Service Manager explained that this was due to no specific individual being identified, for example a neighbour may have reported a fall by a service user or a carer may be concerned about a family member taking money. There would be a screening process to gather evidence and map and monitor effectively, but no proof may have been found. Another Member referred to the sources of referrals. The Service Manager explained that there could be several referrals from different sources regarding the same individual, this would be classed as one referral so no duplication would take place. The Committee AGREED to recommend that the report be accepted and endorse Option 2, namely that the report be accepted as provided and recommend approval at the Executive Committee.	
No. 9	**<u>QUALITY ASSURING SAFEGUARDING IN LOCAL GOVERNMENT EDUCATION SERVICES (LGES)</u>** Consideration was given to the report of the Strategic Education Improvement Manager which was presented to seek Members views on the revised quality assurance protocol for safeguarding arrangements in Local Government Education Services (LGES). The Safeguarding in Education Manager spoke to the report and highlighted the main points contained therein. A Member raised concerns regarding transfers of pupils from one school to another and out of county transfers and commented that it was incumbent on the school to pass on	

	transfer information and felt that the Admission Policy was not being implemented by schools correctly i.e. completing the transfer forms fully. The Head of Education Transformation said that the Admission Policy was renewed annually and was presented to Education & Learning Scrutiny Members for consideration, however, he would work to ensure that implementation of the policy would be carried out more effectively. Members acknowledged this course of action. Another Member also raised concerns in relation to transfer information not being passed onto schools. He commented that staff and pupils could be at risk of violence and aggression if information was not passed on. He also enquired what support was in place for school staff who had allegations made against them. The Head of Education Transformation said that a task and finish group led by the Chief Officer Commercial to discuss violence and aggression against staff was to be arranged and one key point for discussion would be school-based staff. A Member commented that a policy should be considered that if a parent was banned from one school they should be banned from all schools in the borough due to safeguarding issues. The Committee AGREED, subject to the foregoing, to recommend that the report be accepted and endorse Option 1, namely that Members scrutinised the revised protocol and contributed to the continuous assessment of effectiveness.	

Blaenau Gwent County Borough Council

Action Sheet

Joint Education and Learning and Social Services (Safeguarding) Scrutiny Committee – 2nd December 2019

Item	Action to be Taken	By Whom	Action Taken
7	**Safeguarding Performance Information for Education and Social Services**		
	Members enquired whether the graphs relating to the text in the report, could be included in the covering report for easy reference.	Alison Ramshaw, Service Manager	New format of reporting to be considered to include graphs alongside text in future reporting.
	Elective Home Education: A Member requested the latest figure in relation to the number of EHE pupils.	Lynn Phillips, Head Education Transformation	As at March 2020 there are 74 pupils registered as EHE.

This page is intentionally left blank

Executive Committee and Council only

Date signed off by the Monitoring Officer: N/A

Date signed off by the Section 151 Officer: N/A

Committee: **Joint Education and Learning and Social Services (Safeguarding) Scrutiny Committee**

Date of meeting: **8th October 2020**

Report Subject: **360 degree Safe Online Safety Policy for Schools**

Portfolio Holder: **Cllr J Collins Executive Member for Education**

Report Submitted by: **Lynn Phillips, Interim Corporate Director of Education**
Sarah Dixon, Safeguarding in Education Manager

Reporting Pathway								
Directorate Management Team	**Corporate Leadership Team**	**Portfolio Holder / Chair**	**Audit Committee**	**Democratic Services Committee**	**Scrutiny Committee**	**Executive Committee**	**Council**	**Other (please state)**
x	x	23.09.20			08.10.20	09.12.20		

1. **Purpose of the Report**

1.1 This report presents the 360 Degree Safe Cymru Online Safety Policy for schools and provides an opportunity to seek Members' views on the policy template prior to the adoption of the model policy for schools.

2. **Scope and Background**

2.1 The requirement to ensure that learners are able to use the internet and related communications technologies appropriately and safely is part of a school's wider duty of care. The 360 Degree Safe Cymru Online Safety Policy is provided by South West Grid for Learning (SWGfL) in partnership with Welsh Government. The Online Safety Policy is intended to help schools produce a suitable online safety policy document, which will consider all current and relevant issues in a whole school context.

2.2 Since April 2014, South West Grid for Learning has worked in partnership with the Welsh Government to raise awareness of online safety issues and to improve online safety policy and practice for schools and colleges in Wales. The 360 Degree Safe Cymru Online Safety Policy suggests policy statements which would be essential in any school online safety policy, based on good practice. There are a range of alternative statements that schools should consider, and choose those that are most suitable, given their particular circumstances. The adoption of the 360 Degree Safe Cymru Online Safety policy as the Council's online safety policy for schools will provide clarity and consistency across school estate.

3. **Options for Recommendation**

3.1 **Option 1** - Members are asked to scrutinise and suggest amendments to the policy prior to approval by the Executive Committee.

Option 2 - Members to support the policy as presented and recommend approval by the Executive Committee.

4. **Evidence of how does this topic supports the achievement of the Corporate Plan / Statutory Responsibilities / Blaenau Gwent Well-being Plan**

This report is in line with the following objectives as set out in the Blaenau Gwent Wellbeing Plan:

- Blaenau Gwent wants everyone to have the best start in life.
- Blaenau Gwent wants safe and friendly communities.

5. **Implications Against Each Option**

Option 1
Impact on Budget (short and long term impact)

There are no direct financial implications arising from option 1 in this report.

5.1 **Risk including Mitigating Actions**
There is a risk that without a robust online safety policy, the safety and well-being of children and young people could be negatively impacted. The adoption of an appropriate policy ensures that this risk is mitigated.

A range of key stakeholders have contributed to the development of this policy, which is supported by Welsh Government.

5.2 **Legal**
Welsh Government Circular 158/2015, 'Keeping Learners Safe' contains guidance for local authorities and governing bodies on arrangements for safeguarding children under section 175 of the Education Act 2002. E-safety is referenced within this document as a safeguarding responsibility in specific circumstances.

5.3 **Human Resources**
There are no direct staffing or workforce implications arising from this report.

Option 2
Impact on Budget (short and long term impact)

There are no financial implications arising from option 2 in this report

Risk including Mitigating Actions

There is a risk that without a robust online safety policy, the safety and well-being of children and young people could be negatively impacted. The adoption of an appropriate policy ensures that this risk is mitigated.

A range of key stakeholders have contributed to the development of this policy, which is supported by Welsh Government.

5.4 ***Legal***
Welsh Government Circular 158/2015, 'Keeping Learners Safe' contains guidance for local authorities and governing bodies on arrangements for safeguarding children under section 175 of the Education Act 2002

E-safety is referenced within this document as a safeguarding responsibility in specific circumstances.

5.5 ***Human Resources***
There are no direct staffing or workforce implications arising from this report.

6. **Supporting Evidence**

6.1 **Performance Information and Data**
Local Authority policies have previously been distributed to governing bodies for adoption by schools and all schools have policies in place for internet safety and acceptable use agreements.

The proposed 360 Degree Safe Cymru Online Safety Policy consists of an online safety policy and a series of appendices containing more detailed templates and forms. They have been developed with support by Online Safety professionals through the South West Grid for Learning (SWGfL) in partnership with Welsh Government.

The policy provides guidance and an indication of what should be included. It allows each school to ensure that the content will be relevant for the individual circumstances of each school.

6.2 **Expected outcome for the public**
The proposed policy template provides a framework to support schools in developing confident, digital citizens who know how to stay safe online.

6.3 **Involvement (consultation, engagement, participation)**
The proposed policy demonstrates an integrated approach to online safety across schools.

Views have been sought from schools through the Designated Safeguarding Persons (DSP). There were no objections to taking forward the policy approach.

The copyright of the policy is held by South West Grid for learning. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. A range of individuals and organisations have contributed to the development of the policy and appendices, including:

- Members of the SWGfL online safety group;

- Representatives of Welsh local authorities;
- Representatives from a range of Welsh schools/colleges involved in consultation and pilot groups;
- Plymouth University online safety.

South West Grid for Learning and the Education Achievement Service are in agreement with the Council plan to adopt this policy.

6.4 **Thinking for the Long term (forward planning*)***
Welsh Government encourages schools to make full use of digital technologies to engage learners and improve learner outcomes. The proposed policy supports this learning opportunity.

6.5 **Preventative focus**
In order to become confident digital citizens, children need to know how to stay safe online, both under supervision and independently. The proposed policy supports this.

6.6 **Collaboration / partnership working**
The Council collaborates with a range of partners and corporate services to discharge its Local Government Education Service functions.

South West Grid for Learning and Education Achievement Service are in agreement with the Council proposal to adopt this policy.

6.7 **Integration** (across service areas)
The proposed policy is for all schools. The proposed policy template would cover other pre-existing LA policies that will be superseded upon the implementation of this policy

6.8 **EqIA**
An EQIA for the online safety policy template has been undertaken and no adverse impact has been identified.

7. **Monitoring Arrangements**

7.1 Adoption of the policy templates will be monitored on a termly basis through the Safeguarding Matrix which is part of the embedded approach within the Directorates.

Background Documents /Electronic Links

Appendix 1 – 360 degree Safe Cymru Online Safety Policy Template

- 360 Degree Safe Cymru: updated template policies and acceptable use guidance:

Online safety policy template

for schools

Contents

Introduction

The online safety policy template

These school online safety policy templates are intended to help school leaders produce a suitable online safety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the safeguarding, behaviour and anti-bullying policies.

The requirement to ensure that learners are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their online safety policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

These policy templates suggest policy statements which, in the view of Welsh Government, would be essential in any school online safety policy, based on good practice. In addition there are a range of alternative statements that schools should consider and choose those that are most suitable, given their particular circumstances.

An effective school online safety policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school community.

It is suggested that consultation in the production of this policy should involve:

- governors
- teaching staff and support staff
- learners
- community users and any other relevant groups.

Due to the ever-changing nature of digital technologies, it is best practice that the school reviews the online safety policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Schools are subject to an increased level of scrutiny of their online safety practices by Estyn Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children are safe from terrorist and extremist material on the internet.

Given the range of optional statements and guidance notes, this template document is much longer than the resulting policy is likely to be. It is intended that, while covering a complex and ever changing aspect of the work of the school, the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

The template uses a number of alternative terms, e.g. school. These need to be deleted as relevant.
Within this template, sections which include information or guidance are shown in **BLUE**. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections are highlighted in BOLD text, it is strongly suggested that these should be an essential part of a school online safety policy.
Where sections in the template are written in ITALICS it is anticipated that schools would wish to carefully consider whether or not to include that section or statement in their completed policy.

Online safety policy template
for schools

The first part of this document (approximately 25 pages) provides a template for an overall online safety policy for the school. The appendices contain acceptable use agreement templates and more detailed, specific policy templates. It will be for schools to decide which of these documents they choose to amend and adopt.

[Name of school]

Online safety policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Development/monitoring/review of this policy

This online safety policy has been developed by a working group/committee (or insert name of group) made up of: (delete/add as relevant)

- *Headteacher/senior leaders*
- *Online safety officer/coordinator*
- *Staff – including practitioners//support staff/technical staff*
- *Governors*
- *Parents and carers*
- *Community users.*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development/monitoring/review

This online safety policy was approved by the *governing body/governors sub-committee on:*	*Insert date*
The implementation of this online safety policy will be monitored by the:	*Insert name of group/individual (suggested groups – online safety coordinator/officer/group, senior leadership team, other relevant group)*
Monitoring will take place at regular intervals:	*Insert time period (suggested to be at least once a year)*
The *governing body/governors sub-committee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Insert time period (suggested to be at least once a year)*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Insert date*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Insert names/titles of relevant persons/agencies, e.g. LA ICT manager, LA safeguarding officer, police*

The school will monitor the impact of the policy using: *(delete/add as relevant)*

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys/questionnaires of:*
  - *learners*
  - *parents and carers*
  - *staff.*

If possible – may need the assistance of service provider

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals[1] and groups within the school.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the G*overning Body/governor's sub-committee* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governor[2] to include:

- regular meetings with the online safety coordinator/officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs and monitoring of filtering logs (where possible)
- reporting to relevant governors/sub-committee/meeting.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to the online safety coordinator/officer
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[3]
- The headteacher/senior leaders are responsible for ensuring that the online safety coordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The headteacher/senior leaders will receive regular monitoring reports from the online safety coordinator/officer

Online safety coordinator/officer

NOTE: It is strongly recommended that each school should have a named member of staff with a day to day responsibility for online safety; some schools may choose to combine this with the designated senior person role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school.

The online safety coordinator/officer:

- leads the online safety group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the local authority/relevant body
- liaises with (school/local authority) technical staff

[1] In a small school some of the roles described below may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

[2] It is suggested that the role may be combined with that of the Safeguarding Governor.

[3] See flow chart on dealing with online safety incidents – included in a later section – 'Responding to incidents of misuse' and relevant *local authority HR/other relevant body* disciplinary procedures.

- receives reports of online safety incidents[4] and creates a log of incidents to inform future online safety developments
- meets regularly with online safety governor to discuss current issues, review incident logs and if possible, filtering change control logs
- attends relevant meeting/sub-committee of governors
- reports regularly to headteacher/senior leadership team.

Network manager/technical staff

NOTE: If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.

The network manager/technical staff (or local authority/managed service provider) is responsible for ensuring that:

- the *school* technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of the *network/internet/learning platform/Hwb/remote access/e-mail* is regularly monitored in order that any misuse/attempted misuse can be reported to the *headteacher/senior leader; online safety coordinator/officer* (insert others as relevant) for investigation/action/sanction
- *(if present) monitoring software/systems are implemented and updated as agreed in school policies*
- *the filtering policy (*if one exists*), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person* (see appendix 'Technical security policy template' for good practice).

Teaching and support staff

These individuals are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the *headteacher/senior leader; online safety coordinator/officer (insert others as relevant)* for investigation/action
- all digital communications with learners/parents and carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the online safety and acceptable use agreements
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices

[4] The school will need to decide how these incidents will be dealt with and whether the investigation/action will be the responsibility of the Online safety coordinator/officer or another member of staff, e.g. headteacher/senior leader/designated senior person/class teacher/head of year, etc.

- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches.*

Designated senior person

NOTE: It is important to emphasise that these are safeguarding issues, not technical issues; the technology provides additional means for safeguarding issues to develop. Schools may choose to combine the role of designated senior person and online safety officer.

The designated senior person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data[5]
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

If the roles of the designated senior person and the online safety officer are not combined, it is suggested that they work in collaboration due to the safeguarding issues often related to online safety.

Online safety group

The online safety group[6] provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to senior leaders and the governing body.

Members of the online safety group (or other relevant group) will assist the online safety coordinator/officer (or other relevant person, as above) with:

- the production/review/monitoring of the school online safety policy/documents
- *the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes*
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and the learners about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool.

An online safety group terms of reference template can be found in the appendices.

Learners

These individuals:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (this should include personal devices – where allowed)
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

[5] See 'Personal data policy' in the Appendix..

[6] Schools will need to decide the membership of the online safety group. It is recommended that the group should include representation from learners and parents/carers.

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through *parents'/carers' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents'/carers' sections of the website, Hwb, learning platform and online learner records
- their children's personal devices in the school (where this is allowed).

Community users

Community users who access school systems/website/Hwb/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. A community users acceptable use agreement template can be found in the appendices (A6)

Policy statements

Education – learners

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways (Note: statements will need to be adapted, depending on school structure and the age of the learners).

- **A planned online safety curriculum across a range of subjects, (e.g. ICT/PSE/DCF) and topic areas and should be regularly revisited.**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.**
- **Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.**
- **Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.**
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- *Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.*
- *Staff should act as good role models in their use of digital technologies the internet and mobile devices.*

- *In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through: (select/delete as appropriate)

- *curriculum activities*
- *letters, newsletters, web site, learning platform, Hwb*
- *parents and carers evenings/sessions*
- *high profile events/campaigns, e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g.* hwb.wales.gov.uk/ www.saferinternet.org.uk/ www.childnet.com/parents-and-carers (see Appendix for further links/resources).

Education – the wider community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- providing family learning courses in use of new digital technologies, digital literacy and online safety
- online safety messages targeted towards grandparents and other relatives as well as parents.
- the school learning platform, Hwb, website will provide online safety information for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk).

Education and training – staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

- **a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify online safety as a training need within the performance management process*
- **all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.**
- *the online safety coordinator/officer (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*

- *the online safety coordinator/officer (or other nominated person) will provide advice/guidance/training to individuals as required.*

Training – governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways such as:

- attendance at training provided by the local authority/National Governors Association/or other relevant organisation, (e.g. SWGfL)
- participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements. The school should also check their local authority/other relevant body policies on these technical issues if the service is not provided by the authority.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: (schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy) A more detailed technical security policy template can be found in the Appendix.

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements** (these may be outlined in local authority/other relevant body policy and guidance).
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Good practice in preventing loss of data from ransomware attacks requires a rigorous and verified back-up routine, including the keeping of copies off-site.
- **All school networks and system will be protected by secure passwords.**
- **The master account passwords for the school systems should be kept in a secure place, e.g. school safe. Consideration should also be given to using two factor authentication for such accounts** (further guidance is available in the 'Technical security policy template' in the Appendix).
- **All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group** (or other group).
- **All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **Passwords must not be shared with anyone.**
- **All users will be provided with a username and password** by xxxxx (insert name or title) who will keep an up to date record of users and their usernames (see section on password generation in 'Technical security policy template' in the Appendix).
- **Passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number**

and special characters. Passwords should be easy to remember, but difficult to guess or crack.

- **Records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be be securely kept when not required by the user.** *Password complexity in foundation phase should be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- (Insert name or role) is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (The school will need to decide on the merits of external/internal provision of the filtering service – see Appendix). There is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
- *The school has (if possible) provided enhanced/differentiated user-level filtering* (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.).
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. N.b. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet (see Appendix for information on 'appropriate filtering/monitoring').
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. (schools may wish to add details of the monitoring programmes that are used).
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.

An agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See school personal data policy template in the appendix for further detail.)

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A range of mobile technology implementations is possible.

For further reading, please refer to the *NEN Technical Strategy Guidance Note 5 – Bring your own device* - /www.nen.gov.uk/advice/bring-your-own-device-byod

A more detailed mobile technologies policy template can be found in the Appendix. The school may however choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate mobile technologies policy. It is suggested that the school should in this overall policy document outline the main points from their agreed policy. A checklist of points to be considered in included below.

- The school acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies.
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems).

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[7]	Student owned	Staff owned	Staff owned
Allowed in school				Yes/No[8]	Yes/No[8]	Yes/No[8]
Full network access						
Internet only						
No network access						

Aspects that the school may wish to consider and include in their online safety policy, mobile technologies policy or acceptable use agreements include the following:

School owned/provided devices:

- Who they will be allocated to.
- Where, when and how their use is allowed – times/places/in/out of school.

[7] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[8] The school should add below any specific requirements about the use of mobile/personal devices in school.

- If personal use is allowed.
- Levels of access to networks/internet (as above).
- Management of devices/installation of apps/changing of settings/monitoring.
- Network/broadband capacity.
- Technical support.
- Filtering of devices.
- Access to cloud services.
- Data protection.
- Taking/storage/use of images.
- Exit processes, what happens to devices/software/apps/stored data if user leaves the school.
- Liability for damage.
- Staff training.

Personal devices

- Which users are allowed to use personal mobile devices in school (staff/learners/visitors).
- Restrictions on where, when and how they may be used in school.
- Storage.
- Whether staff will be allowed to use personal devices for school business.
- Levels of access to networks/internet (as above).
- Network/broadband capacity.
- Technical support (this may be a clear statement that no technical support is available).
- Filtering of the internet connection to these devices.
- Data protection.
- Taking/storage/use of images.
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices.
- How visitors will be informed about school requirements.
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm (select/delete as appropriate).

- **When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images.
- *Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those*

images should only be taken on school equipment;, the personal equipment of staff should not be used for such purposes.

- *Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Learners must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of learners are published on the school website* (may be covered as part of the AUA signed by parents or carers at the start of the year - see parents and carers acceptable use agreement in the Appendix).
- *Learners' work can only be published with the permission of the learner and parents or carers.*

Data protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- **it has a Data Protection Policy. (see appendix for template policy)**
- **it implements the data protection principles and is able to demonstrate that it does so.**
- **it has paid the appropriate fee Information Commissioner's Office (ICO)**
- **it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.** The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- **it has an 'information asset register' in place and knows exactly what personal data it holds, where, why and which member of staff has responsibility for managing it**
- **the information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
- **it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention schedule" to support this**
- **data held must be accurate and up to date where this is necessary for the purpose you hold it for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**
- **it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice** (see Privacy Notice section in the appendix)
- **procedures must be in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them**
- **data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier**
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- **it has undertaken appropriate due diligence and has GDPR compliant contracts in place with any data processors**
- **it understands how to share data lawfully and safely with other relevant data controllers. In Wales, schools should consider using the Wales Accord on Sharing Personal Information toolkit to support regular data sharing between data controllers**
- **there are clear and understood policies and routines for the deletion and disposal of data**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

When personal data is stored on any mobile device or removable media the:

- **data must be encrypted and password protected.**
- **device must be password protected.** (be sure to select devices that can be protected in this way)
- **device must be protected by up to date virus and malware checking software**
- **data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.**

Staff must ensure that they: (schools may wish to include more detail about their own data/password/encryption/secure transfer processes)

- **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
- **can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school**
- **only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children**
- **will not transfer any school personal data to personal devices except as in line with school policy**
- **use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data**
- **transfer data using encryption and secure password protected devices.**

(The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.)

The Personal Data Advice and Guidance in the appendix (B2) provides more detailed information on the school's responsibilities and on good practice.

Communication technologies

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies, e.g. few schools allow learners to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the learners. The table has been left blank for school to choose its own responses.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults			Learners				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones/cameras								
Use of other mobile devices, e.g. tablets, gaming devices								
Use of personal e-mail addresses in school, or on school network								
Use of school e-mail for personal e-mails								
Use of messaging apps								
Use of social media								
Use of blogs								

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table.

When using communication technologies the school considers the following as good practice:

- **the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored.** *Staff and learners should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)*
- **users must immediately report to the nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content.** *These communications may only take*

place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications

- *whole class/group e-mail addresses may be used at Foundation Stage, while learners at Key Stage 2 and above will be provided with individual school e-mail addresses for educational use.* (Schools may choose to use group or class e-mail addresses for younger age groups, e.g. at Foundation Stage)
- *learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff*

Social media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- training being provided including acceptable use, social media risks, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to learners, parents and carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- *The school permits reasonable and appropriate access to private social media sites.*

Monitoring of public social media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school..
- The school should effectively respond to social media comments made by others according to a defined policy or process.

School use of social media for professional purposes will be checked regularly by a senior leader and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

The social media policy template in Appendix B4 provides more detailed guidance on the school's responsibilities and on good practice.

Unsuitable/inappropriate activities

Some internet activity such as accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities such as online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of, school when using school equipment or systems. The school policy restricts usage as follows.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images – the making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	

	promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)						
Online gaming (non educational)						
Online gambling						
Online shopping/commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting, e.g. YouTube						

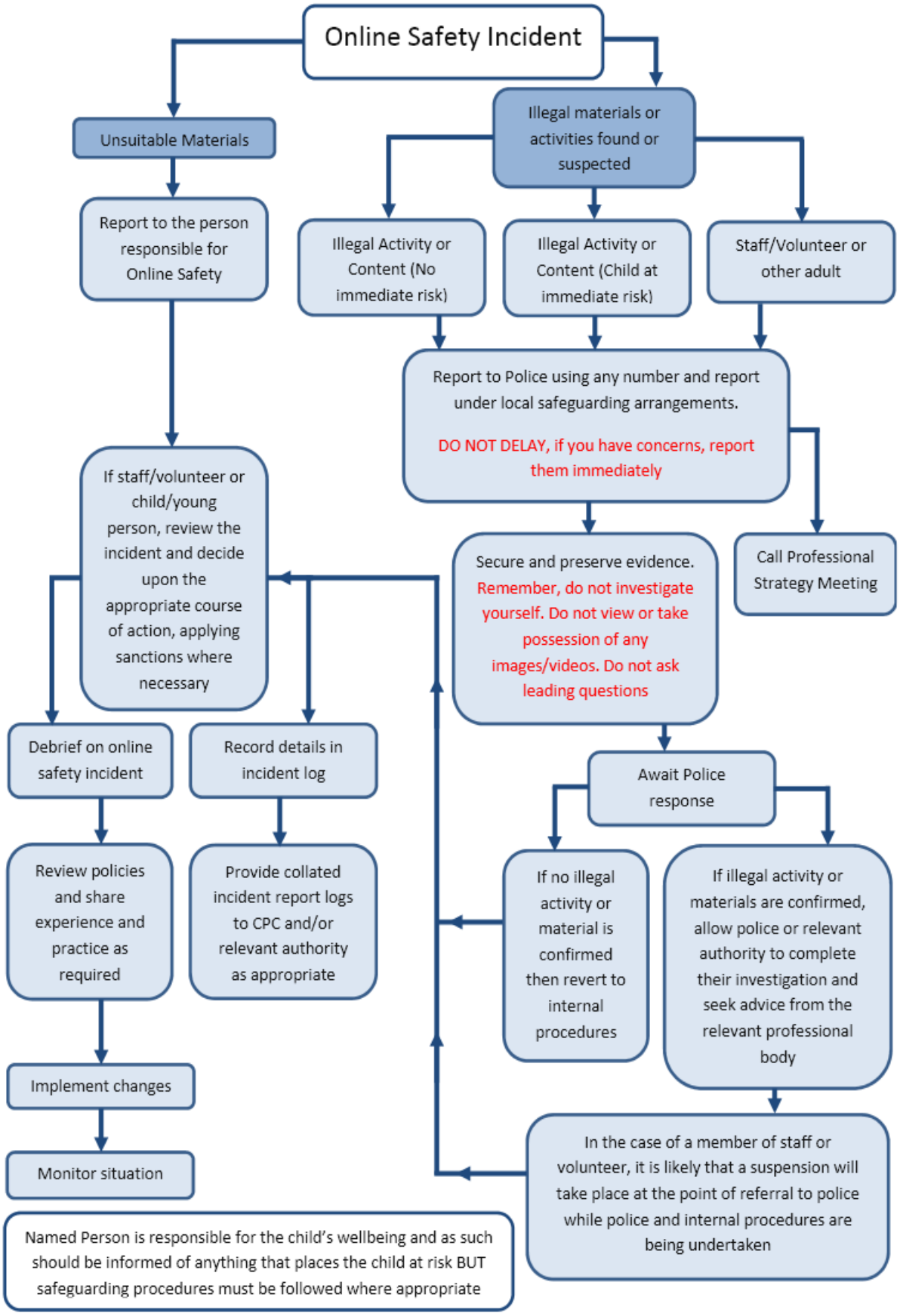
(The school should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools to decide their own responses).

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see 'User actions' above).

Illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed.

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority or national/local organisation (as relevant).
  - police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

Learner actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Headteacher/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction, e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons.									
Unauthorised use of mobile phone/digital camera/other mobile device.									
Unauthorised use of social media/messaging apps/personal e-mail.									
Unauthorised downloading or uploading of files.									
Allowing others to access school network by sharing username and passwords.									
Attempting to access or accessing the school network, using another learners' account.									
Attempting to access or accessing the school network, using the account of a member of staff.									
Corrupting or destroying the data of other users.									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.									
Continued infringements of the above, following previous warnings or sanctions.									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.									
Using proxy sites or other means to subvert the school's filtering system.									
Accidentally accessing offensive or pornographic material and failing to report the incident.									
Deliberately accessing or trying to access offensive or pornographic material.									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.									

Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering, etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		X	X	X				
Inappropriate personal use of the internet/social media/personal e-mail								
Unauthorised downloading or uploading of files.								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.								
Careless use of personal data, e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules.								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.								
Using personal email/social networking/messaging to carrying out digital communications with learners.								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.								
Using proxy sites or other means to subvert the school's filtering system.								
Accidentally accessing offensive or pornographic material and failing to report the incident.								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations.								
Continued infringements of the above, following previous warnings or sanctions.								

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

https://dysgu.hwb.gov.wales/playlists/view/dfdcd1d6-21b0-46ac-b6bb-fc83402ef3d7/en#page1

Acknowledgements

Welsh Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this school online safety policy templates and of the 360 degree safe Cymru online safety self review tool:

- Members of the SWGfL online safety group
- Representatives of Welsh local authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups
- Plymouth University online safety

Appendices – Section A - Acceptable Use Agreement

A1 Learner Acceptable Use agreement template (younger children)

- A2 Learner Acceptable Use agreement template (older children)
- A3 Staff and Volunteers Acceptable Use Agreement template
- A4 Parents /Carers Acceptable Use Agreement template
- A5 Community Users Acceptable Use Agreement template

Appendices – Section B – Specific Policies

- B1 Technical security policy template
- B2 Personal data advice and guidance

- B3 Mobile technologies policy template
- B4 Social media policy template

- B5 Online safety group terms of reference

Appendices – Section C – Supporting documents and links

- C1 Responding to incidents of misuse – flowchart
- C2 Record of reviewing sites (for internet misuse)

- C3 Reporting log template

- C4 Training needs audit template

- C5 Summary of legislation

- C6 Links to other organisations and documents

- C7 Glossary of terms

A1 Learner Acceptable Use Agreement template – for younger learners (Foundation)

This is how we stay safe when we use computers:

I will ask a teacher or another adult from the school if I want to use the computers.

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer/tablet.

Signed (child): .....

(The school will need to decide whether or not they wish the learners to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient, if the school requires signatures)

Signed (parent): .....

This AUA is based on one produced by St Mark's Church of England/Methodist Ecumenical VA Primary School, Weston super Mare.

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the Parent/Carer Acceptable use agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

A2 Learner Acceptable Use Agreement (AUA) template – for older learners

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final AUA document. Schools should review and amend the contents of this AUA to ensure that it is consistent with their online safety policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUA will be more concise.

School policy

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safer internet access at all times.

This Acceptable use agreement is intended to ensure:

- that learners will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Acceptable use agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will only use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), if I have permission of a member of staff to do so. (schools should amend this section to take account of their policy on each of these issues).

I will act as I expect others to act toward me:

- I will respect others' work and property and will only access, copy, remove or alter any other user's files, with the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will only take or distribute images of others with their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal device(s) in school if I have permission (schools should amend this section in the light of their mobile devices policies). I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a school device, if I have permission
- I will only use social media sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social media).

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- where work is protected by copyright, I will not try to download copies (including music and videos)
- when I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying, use of images or personal information)
- I understand that if I fail to comply with this acceptable use agreement, I will be subject to disciplinary action. This may include (schools should amend this section to provide relevant actions as per their behaviour policies) loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below / on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Learner acceptable use agreement form

This form relates to the learner acceptable use agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. (Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed), e.g. mobile phones, gaming devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this school, e.g. communicating with other members of the school, accessing school email, learning platform, website, etc.

Name of Learner:.....

Group/Class .....

Signed: .....

Date: .....

Parent/Carer Countersignature (optional)

Note: It is for schools to decide whether or not they require parents/carers to sign the Parent/carer acceptable use agreement (see template later in this document). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

A3 Staff (and volunteer) acceptable use agreement template

Sections that include advice or guidance are written in **BLUE**. It is anticipated that schools will remove these sections from their final AUA document. Schools should review and amend the contents of this AUA to ensure that it is consistent with their online safety policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUA will be more concise.

School policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safer internet access at all times.

This acceptable use agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of digital technologies in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technologies to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable use agreement

I understand that I must use school digital technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technologies. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school (schools should amend this section in the light of their policies which relate to the use of systems and equipment out of school)
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

I will be professional in my communications and actions when using school ICT systems:

- I will only access, copy, remove or alter any other user's files, with their express permission

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will only use my personal equipment to record these images, if I have permission to do so. Where these images are published, (e.g. on the school website/learning platform) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with learners and parents/carers. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications)
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schoo :

- When I use my mobile devices laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (schools should amend this section in the light of their policies which relate to the use of staff devices)
- I will not use personal email addresses on the school digital technology systems. (schools should amend this section in the light of their email policy – some schools will choose to allow the use of staff personal email addresses on the premises)
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material or adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
- I will only install or attempt to install/store programmes on devices or if this is allowed in school policies (schools/academies should amend this section in the light of their policies on installing programmes/altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school/LA Personal data policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A4 Parent/carer acceptable use agreement template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which create new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (Schools will need to decide whether or not they wish parents to sign the acceptable use agreement on behalf of their child)

Permission Form

Parent/Carers Name:..... Learner's Name .....

As the parent/carer of the above learner(s), I give permission for my son/daughter to have access to the internet and to digital technology systems at school.

Either: (KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (Foundation)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and digital technology systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the digital technology systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

Who will have access to this form.

Where this form will be stored.

How long this form will be stored for.

How this form will be destroyed.

Signed ..... Date: .....

Use of Digital/Video Images

The use of digital / video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's **delete as relevant** first name/initials will be used.

The school will comply with data protection legislation and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital / video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carers Name: .....

Learner Name(s):.....

As the parent /carer of the above learner, I agree to the school taking digital/video images of my child/children. I agree to these images being used:	Yes / No
• to support learning activities.	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
Insert statements here that explicitly detail where images are published by the school	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Use of Biometric Systems

If the school uses biometric systems (e.g. fingerprint / palm recognition technologies) to identify learners for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" and Data Protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual learners in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as learners do not need to remember to bring anything with them (to the canteen or library) so nothing can be lost, such as a swipe card.

The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints / palms are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a learner's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

As the school is collecting special category personal data and **delete as appropriate** sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	the data shared with the service provider
who will have access to this form	what data will be shared
where this form will be stored	who the data will be shared with
how long this form will be stored for	who will have access to the data
how this form will be destroyed	where the data will be stored
	how long the data will be stored for
	how the data will be destroyed

	how consent to process the biometric data can be withdrawn.

Parent/Carer Name: .....

Learner Name(s): .....

As the parent /carer of the above learner(s), I agree to the school using biometric recognition systems, as described above	Yes / No
I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school	Yes / No

Signed: .....

Further guidance

- Each parent /carer of the child should be notified by the school that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school to process children's biometrics at least one parent /carer must consent and no parent / carer has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parents' /carer's consent.
- Schools must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the learner attends the school, but new permission is required if there are changes to the biometric systems in use.

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for learners.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses **insert cloud service provider name** for learners and staff. This permission form describes the tools and learner responsibilities for using these services.

The following services are available to each learner as part of the school's online presence in **insert cloud service provider name**

Using **insert cloud service provider name** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other learner and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
who will have access to this form	what data will be shared

where this form will be stored	who the data will be shared with
how long this form will be stored for	who will have access to the data.
how this form will be destroyed.	where the data will be stored.
	how long the data will be stored for.
	how the data will be destroyed.
	how a request for deletion of the data can be made.

Do you consent to your child to having access to this service?	Yes / No

Learner Name(s): .....

Parent / Carers Name: .....

Signed: .....

Date: .....

Learner acceptable use agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement. It is suggested that when the learner AUA is written that a copy should be attached to the parents/carers AUA to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

A5 Acceptable Use Agreement for community users template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices

- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that users are protected from potential risk in their use of these systems and devices.

Acceptable use agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.

As the school is collecting personal data by issuing this form, it should inform community users about:

who will have access to this form
where this form will be stored
how long this form will be stored for
how this form will be destroyed

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name ..... Signed ..... Date: .....

B1 School technical security policy template (including filtering and passwords)

Suggestions for use

Within this template sections which include information or guidance are shown in **BLUE**. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD text, it is the view of the Welsh Government that these would be an essential part of a school online safety policy.

The template uses various terms such as school. Users will need to choose which term to use for their circumstances and delete the other accordingly.

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

If the school has an externally managed ICT service, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the managed service provider is fully aware of the school online safety policy/ acceptable use agreements. The school should also check their local authority/other relevant body policies/guidance on these technical issues if the managed service is not provided by the authority.

Responsibilities

The management of technical security will be the responsibility of (insert title) (schools will probably choose the Network Manager/Technical Staff/Head of Computing or other relevant responsible person)

Technical Security

Policy statements

The school will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- **school technical systems will be managed in ways that ensure that the school meets recommended technical requirements** (if not managed by the Local Authority, these may be outlined in Local Authority/other relevant body technical/online safety policy and guidance)
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, local authority or managed provider level)
- all users will have clearly defined access rights to school technical systems. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.*
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security *(see password section below)*
- (insert name or role) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- *mobile device security and management procedures are in place* (where mobile devices are allowed access to school systems). (schools may wish to add details of the mobile device security procedures that are in use).
- *school/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.* (schools may wish to add details of the monitoring programmes that are used)
- *remote management tools are used by staff to control workstations and view users activity*
- *an appropriate system is in place* (to be described) *for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed)*
- an agreed policy is in place (to be described) for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school system
- *an agreed policy is in place* (to be described) *regarding the downloading of executable files and the installation of programmes on school devices by users*
- *an agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school*
- an agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices (see school personal data policy template in the appendix for further detail)
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see school personal data policy template in the appendix for further detail)

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important. Where sensitive data is in use – particularly when accessed on mobile devices – schools may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in this policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the device when in transit – to avoid both being lost/stolen together.

Policy Statements:

- **These statements apply to all users.**
- **All school networks and systems will be protected by secure passwords.**
- **All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).**
- **All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **Passwords must not be shared with anyone.**
- **All users will be provided with a username and password** by xxxxx (insert name or title) (see section on password generation in technical notes) who will keep an up to date record of users and their usernames.

Password requirements:

- **Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.**
- **Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school**
- **Passwords must not include names or any other personal information about the user that might be known by others**
- **Passwords must be changed on first login to the system**
- *The school may wish to recommend to staff and learners (depending on age) that they make use of a 'password vault' these can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.*
- *Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

Learner passwords:

Primary schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class log-ons for Foundation Phase (though increasingly children are using their own passwords to access programmes). Schools need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the Acceptable Use Agreement (AUA). Use by learners in this way should always be supervised and members of staff should never use a class log on for their own network/internet access. Schools should also consider the implications of using whole class log-ons when providing access to learning environments and applications, which may be used outside school.

- **Records of learner usernames and passwords for foundation phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.** *Password complexity in foundation phase should be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- Users will be required to change their password if it is compromised. Some schools may choose to reset passwords at the start of each academic year to avoid large numbers of forgotten password reset requests where there is no user-controlled reset process. (Note: passwords should not be regularly changed but should be secure and unique to each account.)

- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Schools may wish to add to this list for all or some learners any of the relevant policy statements from the staff section above.

Notes for technical staff/teams

- **Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts**.
- **An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.** (A *school* should never allow one user to have sole administrator access)
- **Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.**
- *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by* xxxxx (*insert title*) (schools may wish to have someone other than the school's technical staff carrying out this role e.g. an administrator who is easily accessible to users). *Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.*
- *Where automatically generated passwords are not possible, then a good password generator should be used by xxxxx (insert title) to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
- *Requests for password changes should be authenticated by* (the responsible person) *to ensure that the new password can only be passed to the genuine user* (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a learner)
- **Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.** *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
- **In good practice, the account is "locked out" following six successive incorrect log-on attempts.**
- **Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).**

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way. Please see our blog for more details on this.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement

Learners will be made aware of the school's password policy:

- in lessons (the school should describe how this will take place)
- through the Acceptable Use Agreement

Audit/Monitoring/Reporting/Review:

The responsible person (insert title) will ensure that full records are kept of:

- User Ids and requests for password changes
- *User log-ons*
- *Security incidents related to this policy*

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. When considering the filtering policy, schools must consult with their provider to ensure that all aspects of the policy will be supported.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Schools need to consider carefully the issues raised and decide:

- whether to introduce differentiated filtering for different groups/ages of users, if technically possible
- whether to remove filtering controls for some internet use (eg social networking sites) at certain times of the day or for certain users
- who has responsibility for such decisions and the checks and balances put in place
- what (if any) other system and user monitoring systems will be used to supplement the filtering system and how these will be used.

Responsibilities:

The responsibility for the management of the school's filtering policy will be held by (insert title). They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- be logged in change control logs
- be reported to a second responsible person (insert title)
- *either... be reported to and authorised by a second responsible person prior to changes being made* (recommended)
- *or... be reported to a second responsible person* (insert title) *every X weeks/months in the form of an audit of the change control logs*
- *be reported to the online safety group every X weeks/months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements:

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. Ideally, the monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *Either - The school maintains and supports the managed filtering service provided by the internet service provider (ISP)* (or other filtering service provider)
- *and/or – the school manages its own filtering service* (NB. If a school decides to remove the external filtering and replace it with another internal filtering system, this should be clearly explained in the policy and evidence provided that the headteacher would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff/learners)
- *the school has provided enhanced/differentiated user-level filtering through the use of the (insert name) filtering programme* (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students, etc.*)*
- *in the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Principal (or other nominated senior leader)*
- *mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *any filtering issues should be reported immediately to the filtering provider*
- *requests from staff for sites to be removed from the filtered list will be considered by the technical staff or Service Provider* (insert name or title) (n.b. an additional person should be nominated – to ensure protection for the network manager or any other member of staff, should any issues arise re unfiltered access). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the online safety group.

Education/Training/Awareness:

Learners will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, training sessions

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

Changes to the Filtering System:

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in school or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites, e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).

- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
- any audit/reporting system.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

Monitoring:

Some schools supplement their filtering systems with additional monitoring systems. If this is the case, schools should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreements. *Monitoring will take place as follows:* (details should be inserted if the school so wishes).

Audit/Reporting:

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- *the second responsible person* (insert title)
- *online safety group*
- *online safety governor/governors committee*
- *external filtering provider/local authority/police on request*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

Further Guidance:

Schools may wish to seek further guidance. The following is recommended:

- NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/
- NEN –School e-Security Checklist
- Somerset Technical Guidance for schools – this checklist is particularly useful where a school uses external providers for its technical support/security:
- Prevent duty - schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).
- Welsh Government - Respect and Resilience - Community Cohesion - Guidance and associated tool to support the development of community cohesion and prevent extremism in schools and other educational settings in Wales.
- In response to the above, the UK Safer Internet Centre produced guidance for schools on "Appropriate filtering and appropriate monitoring".

B2 School personal data advice and guidance

Suggestions for use

This document is for advice and guidance purposes only. It is anticipated that schools will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school is encouraged to seek their own legal counsel when considering their management of personal data.

The template uses the terms learners to refer to the children or young people at the institution.

School personal data handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any-personal data breach
- the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation
- it is a legal requirement for all schools to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. It is important to stress that the data protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

Introduction

Schools and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data, that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority / Parent Organisation).

Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represents a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaces the Data Protection Act 1998. These two documents are intended to be read side-by-side.

The GDPR provides the principles and rights which apply across the European Union. The Data Protection Act 2018 covers the areas outside of the EU GDPR and provides the UK-specific details such as; how to handle education and safeguarding information.

Are schools in Wales required to comply?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools and the personal data required in a variety of forms to operate a school this means that all educational establishments in the UK are required to comply.

Guidance for schools is available on the Information Commissioner's Office website including information about the new regulations.

Personal Data

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is information that relates to an identified or identifiable living individual This will include:

- personal information about members of the school community – including learners, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- curricular / academic data e.g. class lists, learner progress records, reports, references
- professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Special categories of personal data

The following is a list of personal data listed in the GDPR as a 'special category'.

"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

Consent

Consent (which is one of the lawful bases to use data) under the regulation has changed. Consent is defined as:

“in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual’s wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data”

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner’s Office (ICO) gives clear advice on when it’s appropriate to use consent as a lawful base. It states:

“Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.”

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it’s important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.

- if your school or requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

Consent is just one of the six lawful bases for processing data:

1. Consent
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
3. Legal obligation: the processing is necessary for you to comply with the law
4. Vital interests: the processing is necessary to protect someone’s life
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
6. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks).

Previously maintained schools were able to rely on the ‘legitimate interests’ justification. But under the new laws, this has been removed for Public Bodies (which includes schools). However, public bodies should consider using the Public Task lawful base whenever they are undertaking a task that is part of their statutory function.

Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what are the risks to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

The school should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school should implement a document retention schedule that defines the length of time data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

In the GDPR, organisations are required to keep records of processing activity. This must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, how and to whom data has been shared
- log the disposal and destruction of the data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the data

Data Breaches

From 25 May 2018, if you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The school should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident

- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

Data Mapping

The process of data mapping is designed to help schools identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your learners then this processor has obligations on behalf of the school to ensure that processing takes place in compliance with data protection laws.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – Unlikely to be used in a school context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the individual. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

Individuals have the right to know:

- if the Controller holds personal data about them
- a description of that data
- the purpose for which the data is processed
- the sources of that data
- to whom the data may be disclosed
- a copy of all the personal data that is held about them.

A school must not disclose

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Your school or must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

Fee

The school should pay the relevant fee to the Information Commissioner's Office (ICO).

Responsibilities

Every maintained school is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with data protection laws

The school may also wish to appoint a Data Manager. Schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school to consider whether the requested information should be released into the public domain. FOI links to data protection law whenever a request includes personal data. Good advice would encourage the school to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- ensure that a well-managed records management and information system exists in order to comply with requests
- ensure a record of refusals and reasons for refusals is kept, allowing the school to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools complete the Guide to Information for Schools.

Information to Parents/carers – the Privacy Notice

In order to comply with the fair processing requirements in data protection law, the school will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

Parental permission for use of cloud hosted services

Schools that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act
- They must provide alternative means for accessing services where a parent or pupil has refused consent

New advice to schools makes it clear that they are not able to use pupils' biometric data without parental consent. Schools may wish to incorporate the parental permission procedures into revised consent processes. (see Appendix A4 Parent / Carer Acceptable Use Agreement)

Privacy and Electronic Communications

Schools should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

B3 School Mobile Technologies Policy Template (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying

policy, acceptable use agreement, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

A policy that completely prohibits pupil/student, staff or visitors from bringing mobile technologies to the school/academy could be considered to be unreasonable and unrealistic for school/academy to achieve. For example, many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a mobile phone and many staff and visitors use mobile phones to stay in touch with family. Contractors require mobile technologies for legitimate business reasons.

Potential benefits of mobile technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

For further reading, please refer to the " NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. Schools should consider the following statements and remove those that do not apply to their planned implementation approach.

- **The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**
- **The school has provided technical solutions for the safe use of mobile technology for school devices and for personal devices**
- **For all mobile technologies, filtering will be applied to the school internet connection and attempts to bypass this are not permitted**
- **Where mobile broadband (e.g. 3G and 4G) use is allowed in the school, users are required to follow the same acceptable use requirements as they would if using school owned devices.**
- **Mobile technologies must only be used in accordance with the law**
- **Mobile technologies are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.**
- **Learners will be educated in the safe and appropriate use of mobile technologies as part of the online safety curriculum**
- The school Acceptable Use Agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies

- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	Schoolowned and allocated to a single user	School owned for use by multiple users	Authorised device[9]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes / No[10]	Yes / No[10]	Yes / No[10]
Full network access	*Yes*	*Yes*	*Yes*			
Internet only						
No network access						

School devices

- **All school devices are controlled though the use of mobile device management (MDM) software**
- **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g internet only access, network access allowed, shared folder network access)**
- **All school devices must be suitably protected via a passcode/password/pin (and encryption where relevant). Those devices allocated to members of staff must only be accessed and used by members of staff**
- **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user**. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- **The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps**
- **The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain their property and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs**
- **The school is responsible for keeping devices up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network. Where user intervention or support for this process is required, this will be made clear to the user**
- **School devices are provided to support learning. It is expected that learners will bring devices to school as required**
- **The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended is not permitted**

[9] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

[10] The school should add below any specific requirements about the use of personal devices in school, e.g. storing in a secure location, use during the school day, liability, taking images etc

- *All school devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity* (details should be added here)

Personal devices

It is for the school to decide whether/or/not personal devices are permitted on school/academy premises and should clearly communicate this in their policies and acceptable use agreements.

Where the school is located in a position with a good 3G/4G signal, the school should provide guidance on the usage of this internet connectivity given that devices using these connections will not be covered by the normal school filtering. Schools should be aware that it is illegal to block (without an appropriate Ofcom licence) telephone/wireless signals.

When personal devices are permitted:

- *all personal devices are restricted through the implementation of technical solutions that provide appropriate levels of filtered network access*
- *personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in the school*
- *staff personal devices should not be used to contact learners or their families, nor should they be used to take images of learners*
- *the school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
- *the school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
- *the school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
- *the school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
- *personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day*

User behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- **the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy**
- **guidance is made available by the school to users concerning where and when mobile devices may be used** (the school will need to decide this**)**
- **devices may not be used in tests or exams**
- **users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
- **users are responsible for charging their own devices and for protecting and looking after their devices while in the school**

- **devices must be in silent mode on the school site and on school buses**
- **users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
- **learners must only photograph people with their permission and must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
- *devices may be used in lessons in accordance with teacher direction*
- *staff owned devices should not be used for personal purposes during teaching sessions, except in emergency situations*
- *printing from personal devices will not be possible*

Visitors

Visitors should be provided with information about how, where and when they are permitted to use mobile technology on the site, in line with local safeguarding arrangements. They should also be informed about the school policy on taking images.

Residential settings

Where a school has residential provision it should consider how they might balance the needs of keeping young people safe when using digital technologies and protecting the school with the importance of young people being able to communicate with friends and family and engage in appropriate online activities in a similar way to their peers in non-residential settings. The school should provide suitable statements within this policy and/or in acceptable use agreements

Similar consideration should be given to how and when learners may access digital technologies if engaged in residential activities away from the site.

Insurance

Schools that have implemented an authorised device approach (1:1 deployment) may wish to consider how they will insure these devices and should include details of the claims process in this policy.

B4 Social Media Template Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents and carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school its staff, parents and carers and learners.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- applies to all staff and to all online communications which directly or indirectly, represent the school
- applies to such online communications posted at any time and from anywhere
- encourages the safe and responsible use of social media through training and education
- *defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with learners are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- Senior Leadership Team (SLT)
    - facilitating training and guidance on Social Media use
    - developing and implementing the Social Media policy
    - taking a lead role in investigating any reported incidents
    - making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
    - receive completed applications for Social Media accounts
    - approve account creation

- Administrator / Moderator
    - create the account following SLT approval
    - store account details, including passwords securely
    - be involved in monitoring and contributing to the account

    - control the process for managing an account after the lead staff member has left the school (closing or transferring)
- Staff
    - know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - attending appropriate training
    - regularly monitoring, updating and managing content he/she has posted via school accounts
    - adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- Process for creating new accounts
  The school community is encouraged to consider if a social media account will help them in their work, eg a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the school Senior Leadership Team which covers the following points:-
    - the aim of the account
    - the intended audience
    - how the account will be promoted
    - who will run the account (at least two staff members should be named)
    - will the account be open or private/closed

  Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*

- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
- engaging
- conversational
- informative
- friendly (on certain platforms, eg. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.
- **permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected
- **under no circumstances should staff share or upload learner pictures online other than via school owned social media accounts**
- staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published
- if a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

Staff

- personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in the school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the school permits reasonable and appropriate access to private social media sites.*

Pupil/Students

- staff are not permitted to follow or engage with current or prior learners of the school on any personal social media network account
- the school's education programme should enable the learners to be safe and responsible users of social media
- learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- if parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use
- the school has an active parent and carer education programme which supports the safe and positive use of social media. This includes information on the website
- parents and carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- as part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "nothing" on social media is truly private
- social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- check your settings regularly and test your privacy
- keep an eye on your digital footprint
- keep your personal information private
- regularly review your connections – keep them to those you want to be connected to
- when posting online consider; Scale, Audience and Permanency of what you post
- if you want to criticise, do it politely
- take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- use a disclaimer when expressing personal views
- make it clear who is posting content
- use an appropriate and professional tone
- be respectful to all parties
- ensure you have permission to 'share' other peoples' materials and acknowledge the author
- express opinions but do so in a balanced and measured manner
- think before responding to comments and, when in doubt, get a second opinion
- seek advice and report any mistakes using the school's reporting process

- consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- don't publish confidential or commercially sensitive material
- don't breach copyright, data protection or other relevant legislation
- consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- don't post derogatory, defamatory, offensive, harassing or discriminatory content
- don't use social media to air internal grievances

B5 School policy template - Online safety group terms of reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the full governing body.

2. MEMBERSHIP

2.1 The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (n.b. in small schools one member of staff may hold more than one of these posts): [add/delete where appropriate]

- Senior Leadership Team (SLT) member/s
- safeguarding officer
- teaching staff member
- support staff member
- online safety co-ordinator (not ICT coordinator by default)
- governor
- parent/carer
- technical support staff (where possible)
- community users (where appropriate)
- *learner representation* – for advice and feedback. *Learner voice is essential in the make up of the online safety group, but learners would only be expected to take part in meetings where deemed relevant.*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the group to provide advice and assistance where necessary

2.3 Group members must declare a conflict of interest if any incidents being discussed directly involve

themselves or members of their families.

2.4 Group members must be aware that many issues discussed by this group could be of a sensitive or

confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave

the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The group should select a suitable chairperson from within the group. Their responsibilities include:

- scheduling meetings and notifying group members
- inviting other people to attend meetings when required by the group
- guiding the meeting according to the agenda and time available
- ensuring all discussion items end with a decision, action or definite outcome
- making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the online safety co-ordinator (or other relevant person) with the following: [add/delete where relevant]

- to keep up to date with new developments in the area of online safety
- to (at least) annually review and develop the online safety policy in line with new technologies and incidents
- to monitor the delivery and impact of the online safety policy
- to monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- to co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through[add/delete as relevant]:
    - staff meetings
    - learner forums (for advice and feedback)
    - governors meetings
    - surveys/questionnaires for learners, parents/carers and staff
    - parents evenings
    - website/learning platform/newsletters
    - online safety events
    - Internet Safety Day (annually held on the second Tuesday in February)
    - other methods
- to ensure that monitoring is carried out of Internet sites used across the school (if possible)
- to monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- to monitor the safe use of data across the [school]
- to monitor incidents involving online bullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all group members, by agreement of the majority

The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT): .....

Date: .....

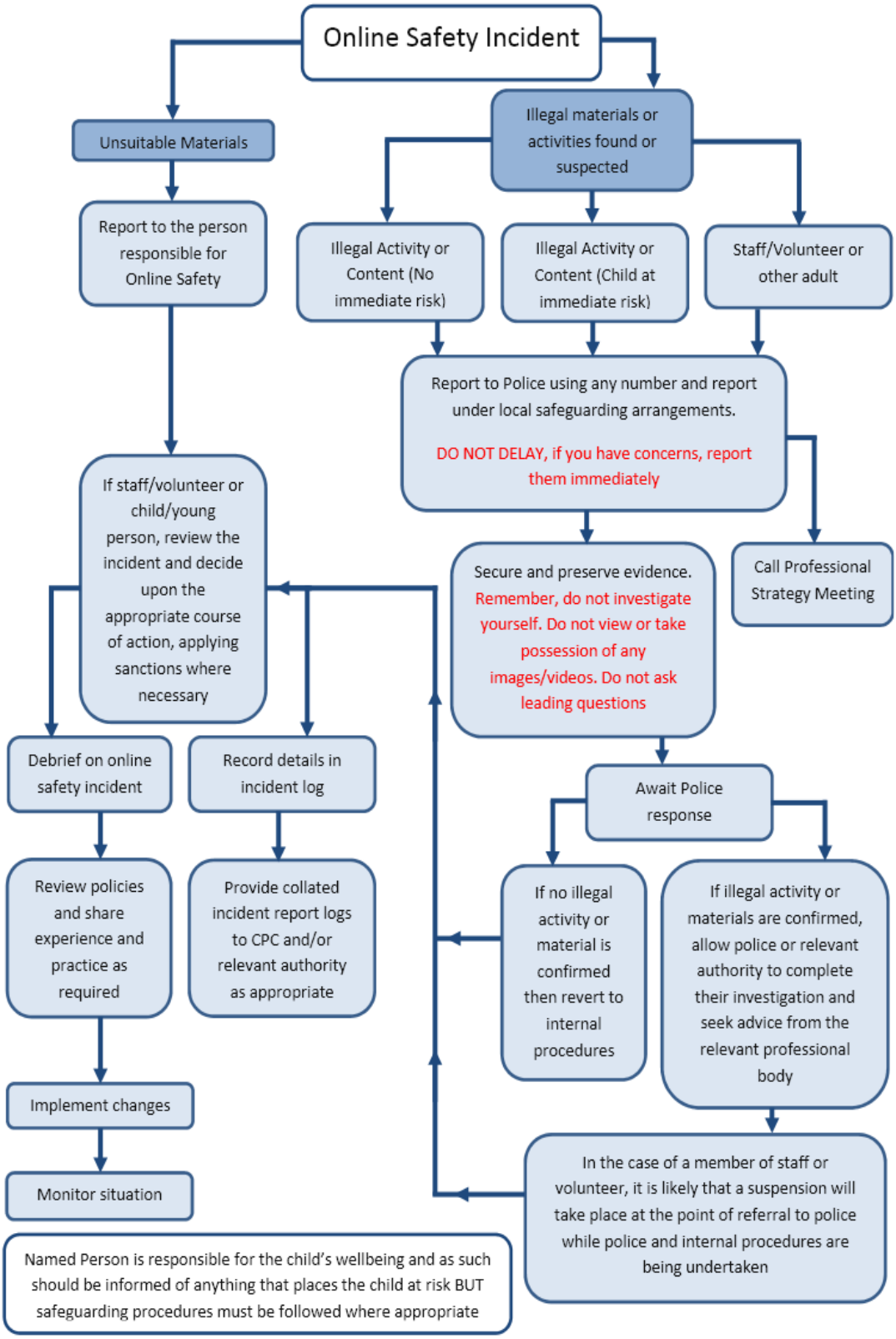
Date for review: .....

Online safety policy template
for schools

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council

C1 Responding to incidents of misuse – flow chart



C2 Record of reviewing devices/internet sites

(responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address/device	Reason for concern

Conclusion and action proposed or taken

C3 Reporting Log Template

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

C4 Training Needs Audit Log Template

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date		

C5 Summary of Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- erase or amend data or programs without authority;
- obtain unauthorised access to a computer;
- "eavesdrop" on a computer;
- make unauthorised use of computer time or facilities;
- maliciously corrupt or erase data or programs;
- deny access to authorised users.

Data Protection Act 2018

Controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- establish the facts
- ascertain compliance with regulatory or self-regulatory practices or procedures
- demonstrate standards, which are or ought to be achieved by persons using the system
- investigate or detect unauthorised use of the communications system
- prevent or detect crime or in the interests of national security
- ensure the effective operation of the system
- monitoring but not recording is also permissible in order to
- ascertain whether the communication is business or personal
- protect or support help line staff

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. You Tube).

Criminal Justice & Public Order Act 1994/Public Order Act 1986

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006/Public Order Act 1986

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18.. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly

- prohibition of discrimination
- the right to education
- the right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The Counter-Terrorism and Security Act 2015

Places a responsibility on schools to participate in work to prevent people from being drawn into terrorism, and challenge extremist ideas that support or are shared by terrorist groups.

C6 Links to other organisations or documents

These may help those who are developing or reviewing an online safety policy.

Welsh Government

- National Online Safety Plan for children and young people in Wales – July 2018
- Welsh Government - Respect and Resilience - Community Cohesion - Guidance and associated tool to support the development of community cohesion and prevent extremism in schools and other educational settings in Wales.

UK Safer Internet Centre

- Safer Internet Centre
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline
- Internet Watch Foundation

CEOP

- http://ceop.police.uk/
- ThinkUKnow

Others

- INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
- Netsmartz - http://www.netsmartz.org/

Cyberbullying

- Welsh Government – Anti Bullying Guidance
- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships, better learning, better behaviour
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/

- Enable – EU funded anti-bullying project - http://enable.eun.org/

Sexting

- UKCCIS - Sexting in schools (available in English and Welsh)
- UKSIC – Responding to and managing sexting incidents

Social Networking

- Digizen – Social Networking
- Connectsafely Parents Guide to Facebook
- UKSIC – Social Media Guides

Curriculum

- Welsh Government – Digital Competence Framework
- DCF Professional Learning Needs Tool
- SWGfL Online Safety Resource (accessed through Hwb)
- UKCCIS – Education for a Connected World- Framework
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources

Mobile Devices/BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Welsh Government - Information, guidance and templates to support schools in the implementation of our information management strategy (IMS) and to ensure biometric data is properly collected and processed.

- Information Commissioners Office:
  - ICO Guide for Organisations (general information about Data Protection)
  - ICO Guides for Education (wide range of sector specific guides)
  - DfE advice on Cloud software services and the Data Protection Act
  - ICO Guidance on Bring Your Own Device
  - ICO Guidance on Cloud Computing
  - ICO - Guidance we gave to schools - September 2012
  - IRMS - Records Management Toolkit for Schools
  - NHS - Caldicott Principles (information that must be released)
  - ICO Guidance on taking photos in schools
  - Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

- **General Teaching Council for Wales - The Code of Professional Conduct and Practice**
- Kent - Safer Practice with Technology

- Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Notes

Working with parents and carers

- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops/education
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- Internetmatters.org

C7 Glossary of terms

AUA	Acceptable use agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational Online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP	Wireless Application Protocol

This page is intentionally left blank

Executive Committee and Council only

Date signed off by the Monitoring Officer: N/A

Date signed off by the Section 151 Officer: N/A

Committee:	**Joint Education and Learning and Social Services Scrutiny Committee (Safeguarding)**
Date of meeting:	**8th October 2020**
Report Subject:	**Local Government Education Services Safeguarding Policy**
Portfolio Holder:	**Cllr J Collins, Executive Member Education**
Report Submitted by:	**Lynn Phillips, Interim Corporate Director Education Sarah Dixon, Safeguarding in Education Manager**

Reporting Pathway								
Directorate Management Team	**Corporate Leadership Team**	**Portfolio Holder / Chair**	**Audit Committee**	**Democratic Services Committee**	**Scrutiny Committee**	**Executive Committee**	**Council**	**Other (please state)**
27.08.20	X	23.09.20			08.10.20	09.12.20		

1. Purpose of the Report

The purpose of the report is to provide Scrutiny Members with the opportunity to scrutinise the Local Government Education Services Safeguarding Policy following its annual review.

2. Scope and Background

The Education Directorate Safeguarding/Child Protection Policy was originally adopted in April 2015 and has been reviewed on an annual basis. The attached draft policy has been reviewed and updated for the 2020-2021 academic year and now encompasses arrangements for all educational settings.

In order to fulfil its safeguarding responsibilities, the Council is required to provide model policies and procedures for maintained schools on all aspects of child protection. The policies and procedures must be consistent with Welsh Government guidance and local arrangements. The attached draft policy covers all employees and volunteers in Blaenau Gwent's Education Directorate and educational settings. Employees of commissioned services are required to follow their organisation's safeguarding policies e.g. Education Achievement Service, Gwent Ethnic Minority Service, Youth Offending Service and Shared Resources Service (SRS). These policies are quality assured on an annual basis by the Safeguarding in Education Manager prior to the commencement of each academic year.

All education and training providers in Wales are inspected by Estyn and a new framework was introduced in the Autumn term 2017. Safeguarding will

be inspected under inspection area four, ‘Care, Support and Guidance’ and as such the model policy is cognisant of the Local Government Education Services (LGES) framework.

The inspection of local authority education services for children and young people covers the statutory functions of the local authority, including the local authority youth service.

Children in Wales (CIW) and Estyn jointly inspect care and education in regulated non-school settings eligible for funding for part-time education These joint inspections evaluate the care provided for all children up to the age of twelve and the education of three and four year old children that do not receive education in a maintained setting for children aged three and four years old.

3. Options for Recommendation

Scrutiny Members are asked to consider the reviewed Safeguarding Policy in order to inform the development of the report that is to be submitted to the Executive Committee. The options for Scrutiny Members to consider are to:

- accept the draft policy as presented in appendix 1; or,
- make amendments to the draft policy.

4. Evidence of how does this topic supports the achievement of the Corporate Plan / Statutory Responsibilities / Blaenau Gwent Well-being Plan

4.1 Statutory Responsibilities

All schools have statutory duties to operate in a way that takes into account the need to safeguard and promote the welfare of children. This is a statutory duty under section 175 of the Education Act 2002.
The Social Services and Well-being (Wales) Act 2014 sets out the responsibilities in terms of the promotion of well-being, places a duty on local authorities to arrange or provide for services which contribute to the prevention of abuse or neglect and ensures all agencies give sufficient priority to safeguarding.

The Wales Safeguarding Procedures (2019) are national procedures which guide safeguarding practice. They are applicable for all practitioners and managers working in Wales.

4.2 Blaenau Gwent Wellbeing Plan

This report is in line with the following objectives as set out in the Blaenau Gwent Wellbeing Plan of:

- Blaenau Gwent wants everyone to have the best start in life; and,
- Blaenau Gwent wants safe and friendly communities.

5. Implications Against Each Option

5.1 **Impact on Budget (short and long term impact)**

There are no direct financial implications.

5.2 **Risk including Mitigating Actions**

Failure of educational establishments to adopt rigorous arrangements for safeguarding poses significant potential risk to children and other education users. Settings are required to have safeguarding policies and procedures in place, reviewed annually, in accordance with local and national guidance. Providing a safeguarding policy for adoption by all education settings ensures that an appropriate policy is available to mitigate risk.

5.3 **Legal**

Under Section 175 of the Education Act 2002, Local Authorities, governing bodies of maintained schools and FE institutions must have regard to Welsh Government Circular 158/2015, 'Keeping Learners Safe', for the purpose of meeting their duties, and should exercise their functions in a way that takes into account the need to safeguard and promote the welfare of children.

The Social Services and Well-being (Wales) Act 2014 sets out the responsibilities in terms of the promotion of well-being, places a duty on local authorities to arrange or provide for services which contribute to the prevention of abuse or neglect and ensures all agencies give sufficient priority to safeguarding.

5.4 **Human Resources**

There are no direct staffing or workforce implications arising from this report.

6. **Supporting Evidence**

6.1 **Performance Information and Data**

The Local Government Education Services Safeguarding Policy has been reviewed. Updates have been made to the following areas of the policy:

- Reference to Wales Safeguarding Procedures 2019, replacing previous reference to All Wales Child Protection Procedures 2008;
- Inclusion of the Blaenau Gwent Youth Service safeguarding policy in appendix 3 of the policy;
- Inclusion of the safeguarding data collection protocol; and,
- Inclusion of a COVID-19 annex to reflect the current situation and reinforce the procedures for reporting concerns. This appendix can be updated regularly as the emergency situation develops and changes.

Adoption of the policy is monitored through the safeguarding matrix, which is overseen by the Safeguarding in Education Manager.

6.2 **Expected outcome for the public**

Learners are provided with a safe learning environment, with the policy supporting settings to respond appropriately to concerns.

6.3 **Involvement (consultation, engagement, participation)**
This policy has been consulted upon with Education DMT, Social Services, Youth Service, Early Years, Organisational Development and Community Safety.

6.4 **Thinking for the Long term (forward planning)**
Ensuring that the Council and its education settings operate robust safeguarding practices, informed by policy, is essential to the wellbeing of all learners in Blaenau Gwent.

6.5 **Preventative focus**
Having an effective policy in place supports educational establishments to adopt practice to keep learners safe and identify concerns early.

6.6 **Collaboration / partnership working**
Gwent Safeguarding is the statutory multi-agency partnership Board responsible for making sure safeguarding is at the core of all services provided across the region.

Education forms part of this multi-agency partnership.

6.7 **Integration(across service areas)**
Within the context of the legal framework and associated guidance, it is important that education settings, schools and governing bodies ensure that appropriate safeguarding procedures are in place and arrangements regarding safer recruitment are rigorously followed in order to safeguard children.

6.8 **EqIA(screening and identifying if full impact assessment is needed)**
An equality impact assessment has been completed and there are no positive or adverse impacts in relation to the revised safeguarding policy.

7. **Monitoring Arrangements**

7.1 The adoption of this policy will be monitored by the safeguarding in education manager through the safeguarding matrix.

Background Documents /Electronic Links

- *Appendix 1 – Education Directorate Local Government Education Services Safeguarding Policy – June 2020*

Keeping Learners Safe
http://learning.gov.wales/docs/learningwales/publications/150114-keeping-learners-safe-en.pdf

(Former) Governors Wales

http://www.governorswales.org.uk/

Disclosure and Barring Service
https://www.gov.uk/government/organisations/disclosure-and-barring-service

This page is intentionally left blank

Education Directorate
Local Government Education Services
Safeguarding Policy

June 2020

Cyngor Bwrdeistref Sirol
Blaenau Gwent
County Borough Council

Contact Information

Safeguarding Manager – Leanne Tetley	01495 355584	Leanne.Tetley@blaenau-gwent.gov.uk
Safeguarding in Education Manager – Sarah Dixon	01495 356016 07815 005241	Sarah.Dixon@blaenau-gwent.gov.uk
Information, advice and assistance – Social services	01495 315700	dutyteam@blaenau-gwent.gov.uk
Families First team manager – Rachel Price	01495 355584	familiesfirstduty@blaenau-gwent.gov.uk
Brynmawr locality team manager – Pam Smith	01495 356093	Pam.Smith@blaenau-gwent.gov.uk
Abertillery locality team manager – Hannah Harwood	01495 356099	Hannah.Harwood@blaenau-gwent.gov.uk
Tredegar locality team manager – Claire Evans	01495 355099	Claire.Evans@blaenau-gwent.gov.uk
Ebbw Vale locality team manager – Tanya Coad	01495 255773	Tanya.Coad@blaenau-gwent.gov.uk
14+ team manager – Beth Thomas	01495 356027	Beth.Thomas@blaenau-gwent.gov.uk
Disabilities team manager – Sarah Savage	01495 355321	Sarah.Savage@blaenau-gwent.gov.uk
Children Looked After Education Coordinator	01495 357712	Catherine.Edwards@blaenau-gwent.gov.uk
PREVENT Lead	07791 875737	Helena.hunt@blaenau-gwent.gov.uk
Youth Service Manager – Joanne Sims	01495 357866	Joanne.Sims@blaenau-gwent.gov.uk
Sarah Jones – Protection of Adults at risk (POVA) Coordinator	01495 354613	Sarah.Jones@blaenau-gwent.gov.uk
Strategic Safeguarding Lead for Education Directorate SSL – Michelle Jones Deputy –Claire Gardner	01495 355823 01495 355603	Michelle.Jones@blaenau-gwent.gov.uk Claire.Gardner@blaenau-gwent.gov.uk
South East Wales Emergency Duty Team (SEWEDT) - after 5pm, weekends and Bank Holidays.	0800 328 4432.	N/A
Domestic Abuse	01495 291202	info@pheonixdas.co.uk
Modern Day Slavery/Trafficking – Training and Victim Support (BAWSO)	0800 731 8147 01633 213213	www.bawso.org.uk
Gwent Safeguarding	N/A	www.gwentsafeguarding.org.uk
Executive Member – John Mason		

With regard to Safeguarding across the Council as a whole The Local Authority Designated Officer is the Safeguarding and Quality Assurance Manager in Social Services. Sarah Dixon, the Safeguarding in Education Manager, covers the responsibilities laid out in WG circular no 009/2014, 'Safeguarding children in Education: - Handling allegations of abuse against teachers and other staff'. Sarah Dixon is the first point of contact with schools, education settings and education directorate staff for advice regarding safeguarding and child protection issues arising in education settings in relation to adults who work with children."

Document version	**Author**	**Date of issue**	**Changes made**
1.0	Sarah Dixon	April 2015	Updated to reflect changes in WG Guidance, Keeping Learners Safe 158/2015
2.0	Sarah Dixon	May 2016	Update to reflect changes in legislation: Counter Terrorism and security Act 2015
3.0	Sarah Dixon	May 2017	Annual review and updated to reflect changes in contact details and the change to Information, Advice and Assistance team.
4.0	Sarah Dixon	Aug 2018	Annual review. Updated to reflect changes in contact details and Local Government Education Services (LGES) framework
5.0	Sarah Dixon	June 2019	Annual review. Updated to reflect changes in contact details.
6.0	Sarah Dixon	June 2020	Annual review. Updated with reference to the Wales Safeguarding Procedures and to include details of safeguarding data collection, BG Youth Service policy and COVID 19 procedures

CONTENTS

INTRODUCTION

Safeguarding children and adults at risk of abuse is everybody's responsibility.

Blaenau Gwent County Borough Council is committed to ensuring that everyone living within the County Borough is safe and protected and that our statutory responsibilities to safeguard and protect children, young people and adults at risk are effectively met. This is reflected in the wellbeing plan. Objectives include Blaenau Gwent having safe and friendly communities and everyone having the best start in life.

Children are defined as anyone who has not yet reached their 18th birthday. Education services provide support to young people up to the age of 25 years. This policy covers all children and adults at risk.

All Local Government Education Services (LGES) are required to have safeguarding policies and procedures in place. The Council seeks assurance from its commissioned services that these policies and procedure are in place and this is validated by the Safeguarding in Education manager on an annual basis. Settings will need to assure themselves that commissioned services and those activities which extend beyond the school day (and not in the direct control of the setting) have appropriate safeguarding arrangements in place.

It is recommended that the policy format recorded in Keeping Learners Safe (Welsh Government circular 158/2015) is used as the basis for all establishments, organisations and services linked to Education. This format can be adapted to meet the needs and requirements of those linked to Education and can be used as the starting point for specifically constructed policies to suit their roles and responsibilities in working with and supporting children and young people.

Other information for children, parents, staff, volunteers and governors could be added as appendices to the main policy. This could include methods of internal recording of concerns and guidance and advice to children, staff and parents in raising concerns.

The policy should be dated and also notification when the next formal review is intended. Where appropriate the date of approval by the Governing Body or Management would be important to be recorded on the policy.

Basic items from the policy could be included in school/ education setting and or organisation's publications for parents and children. A full copy of the policy must be made available to parents on request, but a nominal cost may be incurred.

SCOPE

For the purposes of this policy, 'workforce' is defined as those engaged by the Council, including permanent and temporary employees, students, volunteers, workers employed by employment agencies, contractors and consultants. Where the term 'practitioner' is used, it describes anyone in paid employment and unpaid volunteers.

This policy covers all education settings within Blaenau Gwent.

While practitioners and contractors are likely to have varied levels of contact with children, young people and adults at risk as part of their duties, everyone should be aware of the potential indicators of abuse and neglect and be clear about what to do if they have concerns.

All education settings must have their own safeguarding policies and procedures which are in keeping with this document and local, regional and national procedures and guidance. An example policy template can be found at appendix 1.

RELEVANT LEGISLATION

- Section 175 of the Education Act 2002 requiring local authorities and non-maintained settings to have arrangements in place to safeguard and promote the well-being and welfare of the children on their care.
- Children Act 1989/2004
- Social Services and Wellbeing Act (Wales) 2014
- The Rights of Children and Young Persons (Wales) Measure 2011
- The Equality Act 2010
- Violence Against Women, Domestic Abuse and Sexual Violence (Wales) Act 2015
- Wales Safeguarding Procedures https://safeguarding.wales/

WHAT IS SAFEGUARDING?

Safeguarding means preventing and protecting children and adults from abuse or neglect and educating those around them to recognise the signs and dangers.

The Social Services and Well Being (Wales) Act 2014 defines abuse and neglect:

'Abuse' means physical, sexual, psychological, emotional or financial abuse and includes abuse taking place in any setting, whether in a private dwelling, an institution or any other place. 'Financial abuse' includes:

- Having money or other property stolen;
- Being defrauded;
- Being put under pressure in relation to money or property;
- Having money or other property misused.

'Neglect' means a failure to meet a person's basic physical, emotional, social or psychological needs which is likely to result in an impairment of the person's well-being for example, impairment of the person's health

A full glossary of terms can be found in the Wales Safeguarding Procedures https://safeguarding.wales/glossary.html

PREVENTATIVE APPROACH

Blaenau Gwent County Borough Council wants safe and friendly communities. With regard to this, the council is committed to the development of approaches to ensure organisations meet the same Council objective. Local Government Education Services will be expected to respond to the needs of children/adults at risk, understand how to establish a positive culture of safeguarding and adhere to the principles of partnership working, promoting prevention and early intervention.

RESPONSIBILITIES FOR SAFEGUARDING IN EDUCATION

Overview

Blaenau Gwent County Borough Council has a duty to safeguard and promote the welfare of children and adults who may be at risk of harm.

All practitioners working for or on behalf of the Council have a "**duty to report"** any concerns they may have for the welfare and/or protection of children and adults at risk. The process to follow to make reports is contained in Appendix 5.

The Council promotes safer recruitment policy and practice. Safe recruitment procedures will be implemented in accordance with local, regional and national guidance. Education settings will implement the relevant Recruitment and Selection Policy and the Manager's Guide to Volunteers in the Workplace.

Practitioners working with children and young people are required to undergo a DBS check, at the appropriate level, which is updated on a three year rolling programme. Education settings must maintain a record of DBS checks, recording the certificate number and date of issue. To ensure compliance with GDPR, original/photocopied certificates should not be retained. All school governors should undergo a DBS check at the appropriate level, upon appointment and renewed at the start of each term of office.

Where practitioners have safeguarding concerns or suspicions about other practitioners or contractors these should be reported through safeguarding procedures. Practitioners should also be aware of the statutory protection provided by the Public Interest Disclosure Act 1998 ("PIDA") that protects employees against victimisation if they speak

about concerns about conduct or practice within a school which is potentially illegal, corrupt, improper, unsafe or unethical, or which amounts to malpractice.

All practitioners will be made aware of their safeguarding responsibilities as part of their induction to their employment. Additional training will be undertaken appropriate to the practitioner's role and responsibilities.

Any person responsible for, or working with, children or adults at risk in any capacity, whether paid or unpaid, is considered both legally and morally, to owe them a duty of care. This includes a duty to behave in a manner that does not threaten, harm or put people at risk of harm from others.

All practitioners have a responsibility to conduct themselves in their private lives in a manner that does not compromise their position in the workplace or call into question their suitability to work with children or adults at risk.

Each local government education setting/school is responsible for nominating a Designated Senior Person (DSP) and deputy DSP with responsibility for safeguarding. All DSP's will be invited to termly DSP meetings with the Safeguarding in Education Manager.

The Role of the Governing Body in Schools

The Council's agreed statutory partnership agreement sets out the responsibilities of school's governing bodies, which are summarised below:

Governing Bodies of schools are accountable for ensuring effective policies and procedures are in place to safeguard and promote the welfare of children, and monitoring its compliance with them

Governing Bodies should ensure that their schools:

- Have effective child protection policies and procedures in place that are:
    - In accordance with local authority guidance and locally agreed interagency procedures
    - Inclusive of services that extend beyond the school day (e.g. community activities on school premises)
    - Reviewed at least annually
    - Made available to parents/carers upon request
    - Provided in a format appropriate to the understanding of children, particularly where schools cater for children with additional needs

- Operate safe recruitment procedures in line with Local Authority policy and 'Keeping Learners Safe' guidance. Safe recruitment procedures must take account of the need to safeguard children and young people, including arrangements to ensure that all appropriate checks are carried out on new staff

and volunteers who will work with children, including relevant DBS checks and professional registration (if required).

- Ensure that the head teacher/principal and all other practitioners who work with children undertake appropriate training to equip them with the knowledge and skills that are necessary to carry out their responsibilities for child protection effectively, which is kept up to date with refresher training
- Ensure that any agency staff who work with children have the relevant pre-employment checks and DBS checks in place
- Give clear guidance to volunteers/temporary staff providing cover during short-term absences and who will be working with children and young people on the organisation's arrangements for child protection and their responsibilities.
- Ensure that the governing body remedies, without delay, any deficiencies or weaknesses in regard to child protection arrangements that are brought to its attention.
- Ensure that the designated senior person (DSP) for child protection, the designated governor and the chair of governors undertakes training in inter-agency working that is provided by, or to standards agreed by, the Safeguarding Children Board and refresher training to keep their knowledge and skills up to date, in addition to basic child protection training.
- Provide a copy of the school's safeguarding self-evaluation to the Safeguarding in Education Manager during the first half of the autumn term
- Ensure that data for the safeguarding matrix is provided twice a year to the Safeguarding in Education Manager

The Governing Body of a school controls the use of the school premises both during and outside school hours, except where a trust deed allows a person other than the governing body to control the use of the premises, or a transfer of control agreement has been made. Governors can enter into transfer of control agreements in order to share control of the school premises with another body, or transfer control to it. The other body, known as the 'controlling body', will control the occupation and use of the premises during the times specified in the agreement.

Transferring control of the premises to local community groups, sports association and service providers can enable school facilities to be used without needing ongoing management or administrative time from school staff.

Where the governing body provides services or activities directly under the supervision or management of school staff, the school's arrangements for child protection will apply. Where services or activities are provided separately by another body, the governing body must confirm that the body concerned has appropriate policies and procedures in place in regard to safeguarding children and child protection and there are arrangements to liaise with the school on these matters where appropriate.

Responsibilities of Head Teachers/ Managers

Head teachers and Principals of schools / Managers should ensure that all practitioners (including supply staff and volunteers):

- Are aware of child protection policies and procedures, as adopted, are fully implemented and followed by all practitioners
- Ensure understanding and compliance with pre-employment, DBS and Professional Registration requirements
- Can access sufficient resources and time to enable them to discharge their responsibilities, including taking part in strategy discussions and other inter-agency meetings, and contributing to the assessment of children.
- Understand the procedures for safeguarding children, and feel able to raise concerns about poor or unsafe practice and that such concerns are addressed sensitively and effectively in a timely manner in accordance with Welsh Government Procedures for Whistleblowing in Schools (Model Policy).
- As part of their induction, are given a written statement about the school's policy and procedure, and the name and contact details of the DSP for child protection.

Head teachers/ Managers should also:

- Provide timely updates to the Safeguarding in Education Manager in line with the safeguarding data protocol (Appendix 11)
- Participate in the Quality Assurance processes in a timely manner
- Ensure that the safeguarding processes are reviewed annually and shared with staff, and, in schools, the governing body

Role of the Designated Person in schools and educational settings

The Designated Senior Person (DSP) for safeguarding fulfills an essential role in developing and implementing policies that help to safeguard adults and children from all forms of abuse and create a safe environment.

Each setting should identify a DSP with lead responsibility for safeguarding matters.

The DSP should know how to recognise and identify the signs of abuse and neglect and know when it is appropriate to make a report to the relevant investigating agency.

The role involves providing advice and support to other practitioners, making reports to and liaising and working with other agencies as necessary. The DSP role is not to investigate allegations, but they must keep the head teacher/ Manager informed of all adult/child protection issues in the establishment.

The DSP must be a senior member of the leadership team with the status and authority within the organisation to carry out the duties of the post, including committing resources to child protection matters, and where appropriate, directing other staff.

Dealing with individual cases may be a responsibility of other staff members, but it is important that a senior member of staff takes responsibility for this area of work.

In many schools and settings, a single DSP will be sufficient, but a deputy should be available to act in their absence. In establishments which are organised on different sites or with separate management structures, there should be a DSP for each part of the site. In large organisations, or those with a large number of adult/child protection concerns, it may be necessary to have a number of deputies to deal with the responsibilities.

The establishment must also make arrangements to cover the role of DSP when that person is unavailable. In many cases, there will be a deputy DSP in place and larger settings may have a team of staff working together.

The DSP will take responsibility for the establishment's safegaurding practice, policy, procedures and professional development, working with other agencies as necessary. The head teacher/ Manager should ensure that the DSP:

- Is given sufficient time and resources to carry out the role effectively, which should be explicitly defined in the post holder's job description.
- Has access to required levels of training and support to undertake the role, including ongoing professional development and regular participation at DSP meetings.
- Has time to attend and provide reports and advice to case conferences and other interagency meetings as required

Reporting Concerns

The DSP should act as a point of contact and a source of support, advice and guidance to staff within the setting/ establishment when deciding whether to make a report by liaising with relevant agencies.

The DSP is responsible for making reports about allegations of suspected abuse to the relevant investigating agencies.

In the event of a DSP and deputy being unavailable, the person holding the concern has a duty to report to the relevant agency.

Where allegations relate to cases of suspected abuse or allegations of abuse against practitioners, the relevant process is set out in the example template policy (appendix 1, under the heading, 'What to do if a child tells you they have been abused by a practitioner (including volunteers)'.

All practitioners and contractors have a responsibility to share their concerns in accordance with this policy and to undertake relevant training.

Children - Further guidance and the relevant Multi Agency Referral Form to make a report can be found through the Gwent Safeguarding website, at https://www.gwentsafeguarding.org.uk/en/Children/Report/Report-a-child-at-risk.aspx

Adults - Further guidance and the appropriate referral form for reporting an adult at risk can be found through the Gwent Safeguarding website https://www.gwentsafeguarding.org.uk/en/Adults/Report/Report-an-adult-at-risk.aspx

Training

All staff must have safeguarding training that equips them to carry out their role. This training should be refreshed at intervals not exceeding three years.

In addition to the safeguarding Children and/or adults training, all staff must complete Group 1 training on Violence Against Women, Domestic Abuse and Sexual Violence (VAWDASV) as outlined in the National Training Framework and training on Preventing Extremism. Links to online PREVENT training are contained in Appendix 8.

APPENDIX 1

Example policy template for schools/education settings

Child Protection Policy for (Name of School /Setting)

1. Introduction

The school/setting fully recognises the contribution it makes to safeguarding.

There are three main elements to our policy: -

- Prevention through the teaching and pastoral support offered to children/adults at risk
- Procedures for identifying and reporting cases, or suspected cases of abuse. Because of our contact with children and adults at risk, school and education staff are well placed to observe the outward signs of abuse; and
- Support to those pupils and adults at risk who may have been abused.

This policy applies to all practitioners, (staff and volunteers) working in the school/education setting. In the case of schools, it is the Governing Body's policy. It is recognised by this school/setting that all practitioners that come into contact with children and adults at risk can often be the first point of disclosure. This first point of contact is an important part of the safeguarding process, and it is essential that all practitioners are aware of and implement the school's/ setting's procedures as noted in this policy.

2. Prevention

This school/setting recognises that high self-esteem, confidence, supportive friends and good lines of communication with a trusted adult helps to safeguard children and adults at risk at our school /education setting.

The school/setting will therefore: -

- Establish and maintain an ethos where children and adults at risk feel secure, are encouraged to talk and share their concerns and will be listened to;
- Ensure that children and adults at risk know that all adults in this school/setting can be approached if they are worried or concerned about matters that concern them or their siblings or friends.
- Include in the activities and in the curriculum, opportunities which equip children and adults at risk with the skills they need to stay safe from abuse and to know to whom to turn for help; and

- Include in the activities and in the curriculum, material which will help children and adults at risk develop realistic attitudes to the responsibilities of adult life, particularly with regard to childcare and parenting skills.

3. Procedures

At this school/setting we will follow the Wales Safeguarding Procedures 2019, https://safeguarding.wales/ and other guidance and protocols that have been endorsed and agreed by the South East Wales Safeguarding Children Board. (SEWSCB), and the Gwent Wide Adult Safeguarding Board (GWASB) accessed via www.gwentsafeguarding.org.uk .

The school/ setting will: -

A. Ensure it has a designated senior person (DSP) and deputy for safeguarding, who have undertaken the appropriate training.
B. Recognise the role of the designated senior person and arrange support and training. The school/setting will look to Council's Safeguarding in Education Manager and Gwent Safegaurding for guidance and support in assisting the school's designated senior person.
C. Ensure that all practitioners, along with every governor, know: -

    - the name, contact details and role of the designated senior person (DSP), the deputy DSP and, in schools, the designated governor responsible for safeguarding;
    - in schools, that it is the lead person and/or their deputy who have the responsibility for making reports within timescales, by completing the agreed multi-agency referral form. In other settings, the reporting process will follow procedures agreed for that setting
    - that they have an individual responsibility for sharing concerns using the proper channels and within the timescales agreed.
    - how to take forward those concerns where the DSP is unavailable
    - that the DSP and deputy will seek advice from the Social Services Information, Advice and Assistance (IAA), and /or the Safeguarding in Education Manager if necessary when a report is being considered. When out of hours, advice will be sought from the South East Wales Emergency Duty Team (SEWEDT) Team; **if in doubt a report must be sent**.

D. Ensure that all practitioners are aware of the need to be alert to signs of abuse and know how to respond to a person who may disclose abuse.
E. Ensure that all practitioners will be offered and expected to attend appropriate training and updates as arranged/directed by the school/setting.
F. Ensure that parents have a clear understanding of the responsibility placed on the setting and its staff for safeguarding by setting out their obligations in the school prospectus and/or other forms of communications. In particular, there is a clear obligation that 'the welfare of the child is paramount' and in some

circumstances this may mean that the parents are not initially informed of a report made by the setting about a child.

G. Provide training for all practitioners so that they: -

- Understand their personal responsibility;
- Are cognisant of agreed local procedures
- Understand the need to be vigilant in identifying suspected cases of abuse; and
- Know how to support a person who discloses abuse, particularly the do's and don'ts

H. For schools, notify Social Services if: -
   - a pupil on the child protection register is excluded either for a fixed term or permanently; and
   - there is an unexplained absence of a pupil on the child protection register of more than two days' duration from school (or one day following a weekend).

I. Work to develop effective links with relevant agencies and co-operate as required with their enquiries regarding safeguarding matters including attendance at initial and review child protection conferences and core groups and support these with the submission of written reports.

J. Keep written records of concerns about children and adults at risk (noting date, event and action taken), even where there is no need to report the matter to agencies immediately.

K. Ensure that all records and files are kept secure and in locked locations. The DSP is responsible for the security, compilation and storage or all records and should be able to access and produce them in times of need. It is the responsibility of the DSP to ensure that any transfer of records is conducted via the Authority's agreed protocol and procedures for the 'Transfer of Sensitive Information' (Appendix7)

L. Adhere to the procedures set out in the Welsh Government guidance circular 002/2013 'Disciplinary and Dismissal Procedures for School Staff'.

M. Ensure that all recruitment and selection procedures follow national and local guidance and the Council's Recruitment and Selection policy. Schools will seek advice and guidance from the Council's Organisational Development Department on recruitment and selection.

N. In schools, designate a governor for safeguarding who will oversee the school's policy and practice. This governor will feed back to the Governing Body on safeguarding matters as and when required, and will be required to write an annual report to the Governing Body on the school's safeguarding activities.

4. Supporting the person at Risk

At this education setting/school we recognise that children/adults at risk who are at risk, suffer abuse, or witness violence may be deeply affected by this.

At this education setting/school we will endeavour to be patient and supportive to the person at risk.

This education setting/school will endeavour to support people through: -

- The content of the activities and the curriculum to encourage self-esteem and self-motivation (see section 2 of this policy on Prevention);
- The ethos of the school/setting which: -
    - promotes a positive, supportive and secure environment; and
    - Gives pupils/adults at risk a sense of being valued (see section 2 on Prevention);

- The setting/school's behaviour policy which is aimed at supporting vulnerable pupils in the setting. All practitioners will agree a consistent approach which focuses on the behaviour of the offence but does not damage the pupil's sense of self-worth. The school will endeavour to ensure that the pupil knows that some behaviour is unacceptable, but that each individual is valued and not to be blamed for any abuse which has occurred
- Liaison with other agencies who support the student such as Social Services, Child and Adolescent Mental Health services, the Educational Psychology Service, Education Welfare Service and advocacy services; and
- Keeping records and notifying Social Services if there is a recurrence of a concern with the individual.

When a pupil/child on the child protection register leaves, we will transfer the sensitive information to the new school /setting immediately (Using the procedure outlined in appendix 7, Safeguarding File – Transfer of Records). The DSP will be central to this process, and if not already done, will inform Social Services of the move.

5. Behaviour

This setting/school has a behaviour policy which clearly states our values and expectations. This is a separate policy which is reviewed on a regular basis by the Governing Body and can be located (State where)

6. Bullying

The setting/school's policy on Bullying has been set out in (a separate document/ the behaviour policy etc.) (It would be useful to note any guidance from the Authority within any documentation.) This policy/information is reviewed annually by Governors and can be located (State where)

7. Physical Intervention

The setting/school's policy on physical intervention has been set out in (a separate document/ the school's behaviour policy etc.) (It would be useful to note any guidance, support and training provided by the Authority within any documentation.) It is reviewed annually by the governing body and is consistent with the Welsh Government guidance on Safe and Effective intervention – use of reasonable force and searching for weapons 097/2013 This policy/information can be located (State where).

8. Keeping Safe Online

The school/setting's policy on Online Safety has been set out in (a separate document/ the setting/school IT policy etc.) It would be useful to note any guidance, support and training provided by the Authority within any documentation. This policy/information can be located. (State where)

9. Children with Special Educational Needs (SEN)

This school/setting recognises that statistically children and young people with behavioural difficulties and disabilities are most vulnerable to abuse. Practitioners who deal with children with profound and multiple disabilities, sensory impairment and or emotional and behaviour problems need to be particularly sensitive to signs of abuse. The school's policy on SEN has been set out in (A separate document). This policy/information can be located. (State where)

10. Care Experienced Children

This school/setting recognises that Children Looked After (CLA) are often the most vulnerable. Advice and guidance can be sought from the Local Authority's Education Coordinator for Children Looked After.

11. Community Cohesion – Preventing Extremism

This school/setting is committed to providing a safe environment for all of our students and practitioners. There is no place for extremist views of any kind in our setting. Where we become aware of information involving identification of potential instances of extremism and radicalisation, we will refer to Children's/Adult Services in the same way as for all safeguarding concerns. The Local Authority has 'Secure and Shelter' (Lockdown) procedures that may be activated in response to any number of situations and includes the requirement to carry out practice procedures (appendix 9).

Our policy statement for community cohesion is attached as appendix 8: Community Cohesion – Preventing Extremism.

12. Violence Against Women, Domestic Abuse and Sexual Violence (VAWDA&SV)

The Violence Against Women, Domestic Abuse and Sexual Violence (Wales) Act 2015 aims to improve arrangements for the prevention of gender based violence, abuse and sexual violence.

The protection of victims and support for people affected is underpinned by the 'Ask and Act' duty placed on public service staff to ask potential victims about the possibility that they may be experiencing VAWDASV and act so as to reduce suffering and harm.

The regional VAWDASV board has also prioritised a 'whole school approach' to training and support in order to continue a preventative agenda to domestic abuse. This approach is relevant for all education settings.

The school/setting's policy on VAWDASV has been set out in (a separate document/ the schools VAWDASV policy etc.). This policy/information can be located. (State where)

The school participates in Operation Encompass. The purpose of Operation Encompass is to safeguard and support these children and young people who have witnessed and/or been present at the time of a domestic abuse incident. Operation Encompass aims to ensure that appropriate practitioners are made aware at the earliest possible stage in order to provide relevant and tailored support to children and young people in a way that means they feel safe and included.

13. Modern Slavery

Modern slavery describes forced labour practices with the perpetrator – the slave master- trapping and controlling the victim. The most common form of modern slavery is sexual exploitation. Labour exploitation is the second most common form of slavery occurring most frequently in the agricultural, food, hospitality and construction sectors. Victims may be vulnerable UK or foreigner citizens. Police, Local Authorities, the National Crime Agency and the Gangmasters Labour and Abuse Authority who encounter a potential victim of modern slavery or human trafficking have a duty to notify the Home Office under Section 52 of the Modern Slavery Act 2015.

Modern slavery is a hidden, pervasive crim targeted towards those individuals most vulnerable. The Council and BAWSO are first responding orgnaisations to cases of slavery. Training and victim support regarding Modern Slavery can be found at BAWSO, www.bawso.org.uk

14. Safer Schools' Partnership

The Safer Schools' partnership allows the safe and legal sharing of information that will ensure children can be safeguarded where they are identified as being at risk of or involved in crime and anti-social behavior. This is a multi-agency risk assessment

approach. Specific advice on this can be sought from the Safeguarding in Education Manager.

15. Transfer of school records

Where children are transferred to or from this school, we will ensure appropriate record keeping of the transfer of child protection records through the use of the Safeguarding File – Transfer of records proforma. (See appendix 7).

16. Out of Hours

After 5pm and on weekends and bank holidays, the South East Wales Emergency Duty Team can be contacted on 0800 328 4432

17. Information for staff/volunteers

a) What to do if a person tells you they have been abused or harmed:

A person may confide in any practitioner. Practitioners to whom an allegation is made should remember: -

- Yours is a listening role, do not interrupt the when they are freely recalling events. Limit any questions to clarifying your understanding of what is being said. Any questions should be framed in an open manner so not to lead;
- In schools, you must report orally to the **Designated Senior Person (DSP) for safeguarding** immediately (or in their absence, their Deputy), to inform them of what has been disclosed. In the unlikelihood of both being absent, seek out the most senior person in the school;
- For other education settings, the process outlined in the setting's own procedures must be followed.
- Make a note of the discussion, as soon as is reasonably practical (but within 24 hours) to pass on to the DSP. The note which should be clear in its use of terminology, should record the time, date, place, and people who were present and should record answers/responses in exactly the way they were said as far as possible. This note will in most cases be the only written record of what has been disclosed, and as it is the initial contact, an important one in the process. Remember, your note of the discussion may be used in any subsequent formal investigation and/or court proceedings. It is advised that you retain a copy in a safe place;
- Do not give undertakings of absolute confidentiality. You will need to express this in age/developmental related ways as soon as appropriately possible during the disclosure. This may result in the person 'clamming up' and not completing the disclosure, but you will still be required to share the fact that they have a shared a concern with you to the DSP. Often what is initially shared is the tip of an iceberg;

- That a person may be waiting for a case to go to criminal court, may have to give evidence or in the case of a child, may be awaiting care proceedings.
- You may have a future role in terms of supporting or monitoring the person, for example, contributing to an assessment or in the case of a child, implementing child protection plans. You can ask the DSP for an update on concerns shared, but they are restricted by procedures and confidentiality and may be limited in their response. The level of feedback will be on a need to know, but whatever is shared is strictly confidential and not for general consumption with others.
- When making a report about an 'adult at risk', consent is not required to make the report, but it would be helpful to know if the adult at risk consents to the adult safeguarding process.

b) What to do if a person tells you they have been abused by a practitioner (including volunteers):

If an allegation of abuse is made against a practitioner, this must be reported in accordance with the information below.

Where the allegation is made against a practitioner, reports to Children's/adult services are made in the same way as for all allegations of abuse

Where an allegation is against a practitioner you should refer to authority's guidance which takes into account the Welsh Government's guidance circular 002/2013 Disciplinary and Dismissal Procedures for School Staff and Welsh Government guidance circular 009/2014 Safeguarding Children in Education: Handling allegations of abuse against teachers and other staff. (A summary of procedures is included in appendix 6: Professional Allegations/Concerns).

If an allegation of abuse is made against a practitioner this must be reported to the Head Teacher/ manager.

If the concern is about the Head Teacher, this must be reported to the Chair of Governors and if the concern is about a manager, it must be reported to the next line manager.

The matter must also be discussed with the Safeguarding in Education Manager.
In the absence of the Safeguarding in Education Manager, do not delay, contact the Social Services Information, Advice and Assistance Team.

If there is an allegation against a Local Authority Officer then this must be communicated to the Corporate Director for Education (Interim), Lynn Phillips Tel: 01495 355603/ 07772379795 and the Strategic Safeguarding Lead (SSL) for the Education Directorate, Michelle Jones Tel: 01495 355823 mobile 07881815904

If the concern is about the SSL, then the Corporate Director for Education is to be contacted. If there is a concern about the Corporate Director for Education, then this should be referred to the Chief Officer/Head of Paid Service.

Upon receipt of an allegation/concern about a practitioner in a school, the Head teacher/ manager (or where appropriate, the Chair of Governors), will:

- obtain details of the allegation in writing, signed and dated
- Keep a record of dates, times, location and names of potential witnesses.
- Not investigate the allegation, or interview pupils, or discuss the allegation with the member of staff, but should consider, in consultation with the Senior Officer, whether the allegation requires further investigation and if so by whom.
- inform the Chair of Governors / manager
- Contact the Safeguarding in Education Manager who, together with Children's Services will give urgent consideration as to whether or not there is sufficient substance to the allegation to warrant an investigation: The outcome will either be:

  i. without foundation
  ii. internal disciplinary procedures
  iii. a report under the safeguarding procedures

- In the case of adults at risk, further advice can be sought from the Protection of Adults at risk (POVA) Coordinator, Sarah Jones (01495 354613)

Pending the outcome of this process, interim safeguarding arrangements will be necessary. This will require a risk assessment to be completed and documented by the Head teacher/Chair of Governors/manager. This should ensure that there is no contact between the person who is the subject of the allegation and the person who has been accused of the allegation. Interim safeguarding measures should also be put in place regarding the contact that takes place between any other child(ren)/adult at risk and the person against whom the allegation has been made.

The sharing of information about an allegation must be handled sensitively and must be restricted to those who have a need to know in order to safeguard.

Information about the child, adult at risk or family must not be shared with the individual against whom the allegation was made or anyone representing them.

The matter must be treated confidentially and will not be discussed with practitioners. Each establishment, organisation or service will keep and maintain records which detail allegations of abuse against any practitioner working for them, whether in a paid or

voluntary capacity, whatever the outcome. There are clear requirements of when this information is to be shared with legal or statutory organisations such as DBS and the Education Workforce Council (EWC). Advice and guidance for the sharing of this specific information **must** be sought from Organisational Development

c) Confidentiality

The school/setting and practitioners are fully aware of confidentiality issues if a person divulges that they are or have been abused. A person may only feel confident to confide in a practitioner if they feel that the information will not be divulged to anyone else. However, practitioners have a professional responsibility to share relevant information with the designated statutory agencies when a child is experiencing child welfare concerns or an adult is an 'adult at risk'.

It is important that each practitioner deals with this sensitively. When responding, practitioners should explain that they must inform the appropriate people who can help, but they will only tell those who need to know in order to be able to help. Practitioners should reassure the person and tell them that their situation will not be common knowledge within the setting. Be aware that it may well have taken significant courage to disclose the information and they may also be experiencing conflicting emotions, involving feelings of guilt, embarrassment, disloyalty (if the abuser is someone close) and hurt.

Remember the pastoral responsibility of the Education Service. Ensure that only those with a professional involvement, i.e. the DSP and Head teacher/Manager, have access to safeguarding records. At all other times, they should be kept secure and separate from the person's main file.

18. Training

The school/setting will ensure that the designated senior person and deputy will have received initial training when starting their role and continued professional updates as required. Specific updates as suggested by national and local requirements will be central to the DSP/deputy DSP development.

Designated teachers and senior members of staff responsible for safeguarding must attend training in multi-agency safeguarding procedures, and must undertake refresher training on a regular basis not exceeding three years.

All practitioners will be regularly updated during the year as appropriate from the DSP, but will receive specific awareness raising training within a 3-year period.

Members of school governing bodies must also receive awareness raising training and the Chair of governors and the nominated governor for safeguarding will be offered opportunities for more specific training.

In addition to the safeguarding Children and/or adults training, all staff must complete Group 1 training on Violence Against Women, Domestic Abuse and Sexual Violence (VAWDASV) as outlined in the National Training Framework and training on Preventing Extremism. Links to online PREVENT training are contained in Appendix 8.

All educational settings and partners working with children and adults at risk in Blaenau Gwent must keep records of training and carry out regular audits to ensure that all practitioner training for safeguarding is kept up to date. Educational establishments and partner agencies will be required to provide information on practitioner training to the Council and the Safeguarding Board upon request.

The Designated Senior Person for safeguarding at this school/setting is:-

……..

The Deputy Designated Senior Person for safeguarding at this school/setting is:-

……..

The designated governor for safeguarding at this school is:-

……..

The Council's Safeguarding in Education Manager is:-

Sarah.Dixon@blaenau-gwent.gov.uk **07815 005241; 01495 356016**

Social Services can be contacted as follows:-

Telephone- **01495-315700**
Out of hours number **0800 328 4432**

This policy was updated on _____ by _____

This policy was presented and accepted by the Governing Body on _____

This staff were made aware of this policy and or updates on _____

This policy will be reviewed on _____

APPENDIX 2

Example policy template for Early Years, Childcare and play

Safeguarding Policy for (Name of Setting)

……(setting) believes that children have the right to be completely secure from both the fear and reality of abuse, and we are committed to safeguarding all children in our care from harm. The practitioners at …… (setting) fully recognises the contribution it makes to safeguard children and complies with Wales Safeguarding Procedures 2019, Gwent Safeguarding Children's Board and Blaenau Gwent authority's safeguarding policy.

We recognise the key role that……(setting) can play in working with children and their families to seek early help to address any emerging concerns to help prevent problems from escalating, in preventing abuse by providing our children with good lines of communication with trusted adults, supportive friends and an ethos of protection. Our setting will therefore:

- establish and maintain an ethos where children feel secure, respected and valued, where children are encouraged to talk and are always listened to;
- ensure that all children know there is an adult in the setting whom they can approach
  if they are worried or in difficulty;
- encourage positive emotional health and well-being, self-esteem and self-assertiveness;
- promote a caring, safe and secure environment;
- have regard to the characteristics, culture and beliefs of the child and their family (including, for example language) whilst recognising the paramountcy of safeguarding the individual;
- liaise and work together with all other support services and those agencies involved in early intervention services and the safeguarding of children and young people;
- providing continuous support to a child about whom there have been concerns;

This policy has been drawn up on the basis of National and Gwent Children's Safeguarding Boards' guidance and protocols that seek to protect children, namely:

- Section 175 of the Education Act 2002 requiring local authorities and non-maintained settings to have arrangements in place to safeguard and promote the well-being and welfare of the children on their care.
- Children Act 1989. Children and Family (Wales) Measure 2010
- United Convention of the Rights of the Child 1991
- Data Protection Act 1998
- Sexual Offences Act 2003
- Children Act 2004
- The Equality Act 2010
- Protection of Freedoms Act 2012

- Social Services and Well Being (Wales) Act 2014
- Domestic abuse (Violence against Women, Domestic Abuse and Sexual Violence (Wales) Act 2015)
- Female Genital Mutilation (FGM)
- Modern Slavery Act 2015
- Wales Safeguarding Procedures 2019
- The UNCRC seven core aims for children and young people in Wales
- Relevant Welsh Government guidance on safeguarding children

This policy applies to all staff and volunteers working at ……. (setting).

We aim to:-

- Ensure that all children are never placed at risk while in the care of ……..(setting);
- Support child's health and development in ways that foster security, confidence and independence;
- Ensure that the child's best interests are paramount and as far as reasonably practicable, have regard to the child's views, wishes and feelings, so that they receive the care and support they need before a problem escalates;
- Ensure that confidentiality is maintained at all times;
- Ensure parents are fully aware of our safeguarding/child protection policies and procedures when they register with the setting and are kept informed of all updates when they occur;
- Practitioners should always seek to be transparent with people they are working with about circumstances where they may need to share information with social services and/or the police;
- Regularly review and update this policy with staff and parents;
- Ensure that all staff have regard to this guidance when fulfilling their responsibilities in identifying and reporting possible cases of abuse - safeguarding and promoting the welfare, health and well-being of children in their care;
- Ensure that all staff regularly revise Safeguarding issues and procedures and sign a declaration that they have understood and will adhere to the setting's policies and procedures;
- That practitioners understand their duty to seek early help to address any emerging concerns to help avoid problems escalating;
- To provide a systematic means of monitoring children known or thought to be at risk of harm;
- To emphasise the need for good levels of communication between all members of staff;
- To develop a structured procedure within ……..(setting) which will be followed by all members of staff;

- To develop and promote effective working relationships with other agencies and co-operate as required with their enquiries regarding safeguarding matters including attendance at initial and review child protection conferences and core groups and support with the submission of written reports.
- To ensure that all adults within the setting, who have access to the children, have been checked as to their suitability (including visitors);
- Care Inspectorate Wales (CIW) CIW will be notified of any allegations made against staff, managers, any volunteers, students and/or outside agencies in the setting.

Safe recruitment

…….. (the setting) operate safe recruitment procedures and ensure that all appropriate checks are carried out on new practitioners and volunteers who will work with children, including disclosure and barring checks (DBS) in line with current guidance. We abide by CIW requirements in respect of references and suitability checks for practitioners and volunteers, to ensure that no disqualified person or unfit person works at the nursery or has access to the children. All practitioners and temporary practitioners/volunteers providing cover during short-term absences and who will be working with children are given clear guidance of the setting's arrangements for child protection and their responsibilities during induction.

Children with additional learning needs

We recognise that statistically children and young people with behavioural difficulties and disabilities have an increased risk of being abused compared with their non-disabled/non sensory impaired peers. We also recognise that adults who support children and young people with profound and multiple disabilities, sensory impairment and or emotional and behaviour problems will need to be particularly sensitive to signs of abuse.

Appointed Designated Safeguarding Person (DSP) and their responsibilities.

The setting's Designated Safeguarding Person is …… who will be responsible for supporting practitioners in liaising with Social Services, Gwent Safeguarding Children's Board and CIW regarding any child protection matter.

The setting's Deputy Designated Safeguarding Person is ……who will be responsible for supporting practitioners in the absence of the Designated Safeguarding Officer.

The Designated Safeguarding Person and their Deputy will:

- act as a source of advice and support within …… (the setting) and provide a point of contact for practitioners who have concerns or information that child or young person may be suffering abuse;
- co-ordinate any necessary reports to Social Services, **however** individual practitioners have a duty to report and the responsibility for raising concerns, completing report information, informing Social Services and involvement in any safeguarding processes that follow after a report is made. (e.g. requests for information, attending case conferences etc.)
- support those practitioners in our setting who have been involved with a child who has suffered, or was at risk of suffering harm, who may find the situation stressful and upsetting.
- ensure that ……(the setting) contributes fully to the safeguarding processes e.g. by providing reports, attending meetings or conferences when needed;
- ensure that all practitioners and parents/carers are aware of and have access to our setting's safeguarding policy and procedures and the Wales Safeguarding Procedures;
- disseminate safeguarding information gained from training and other sources to all practitioners in our setting and ensure that newly appointed practitioners are aware of their child protection/safeguarding responsibilities;
- inform CIW of any allegations that have been made against managers, practitioners and volunteers.

Practitioner commitment

The ……(setting) is committed to fulfilling its responsibilities in respect of child protection and safeguarding through the provision of support and training to practitioners. Therefore, ……(setting) will ensure that:-

- all practitioners have up to date safeguarding training so that they understand their roles and responsibilities to safeguard and promote the welfare of children at risk of harm, abuse and neglect
- implement safe recruitment practices for all practitioners, students and volunteers, including verified references and full and up to date enhanced DBS checks
- all practitioners and volunteers are given a copy of the Safeguarding policy during their induction, and have its implications explained to them.
- all practitioners are alert to children's needs including any potential or suspected risk of abuse or harm and understand what action they should take
- any practitioner, student or volunteer under investigation for the alleged abuse of a child, will be subject to the provisions of the setting's Disciplinary Policy
- all practitioners and volunteers receive regular staff meetings and supervision where opportunities to discuss Safeguarding/Child Protection issues will be made and further support provided if necessary;

- all practitioners are aware of any early intervention services that could help prevent any problems escalating;
- All practitioners should familiarise themselves with the culture and beliefs of those families they work with. Practitioners should not be afraid to ask about particular behaviours and the reasons for them in a sensitive manner and should never overlook potential harmful practices on the basis of cultural sensitivity;
- all practitioners are aware of their statutory requirements in respect of the disclosure or discovery of child abuse and the procedure for doing so. All students and volunteers are instructed to report the disclosure or discovery of abuse to the DSP or setting's manager.
- All visitors/contract/external workers will sign a visitor's book and be formally identified before accessing the setting. They will be accompanied whilst on the premises, especially when in the areas the children use.

Supporting Practitioners

We recognise that all practitioners working in the setting who has been involved with a child who has suffered, or is at risk of suffering harm, may find the situation stressful and upsetting. We will support the practitioner by providing opportunity to talk through their anxieties with the Designated Safeguarding Person and to seek further support if needed.

Recognising Child Abuse

Child abuse can manifest itself in a variety of different ways, some overt and others much less so. A person may abuse or neglect a child by inflicting harm, or by failing to act to prevent harm. Children may be abused in a family, an institution or community setting; by those known to them or, more rarely by a stranger.

Indicators of abuse (although this is by no means an exhaustive list)

- Failure to thrive and meet developmental milestones
- Fearful or withdrawn tendencies
- Aggressive behaviour
- Unexplained injuries to a child or conflicting reports from parents or staff
- Repeated injuries
- Unaddressed illnesses or injuries
- Inappropriately clothed

Types of Harm

- **Physical abuse** - hitting, slapping, over or misuse of medication, undue restraint, or inappropriate sanctions;

- **emotional/psychological abuse** - threats of harm or abandonment, coercive control, humiliation, verbal or racial abuse, isolation or withdrawal from services or supportive networks, witnessing abuse of others**;**
- **sexual abuse** - forcing or enticing a child or young person to take part in sexual activities, whether or not the child is aware of what is happening, including: physical contact, including penetrative or non-penetrative acts; non-contact activities, such as involving children in looking at, or in the production of, pornographic material or watching sexual activities or encouraging children to behave in sexually inappropriate ways;
- **financial abuse** - this category will be less prevalent for a child but indicators could be: not meeting their needs for care and support which are provided through direct payments; or complaints that personal property is missing.
- **neglect** - failure to meet basic physical, emotional or psychological needs which is likely to result in impairment of health or development.
- **Identity Neglect** – not recognising or addressing the child or young person's needs in terms of (for example) culture, religion, gender and sexuality.
- **Emotional Neglect** – It also includes not saying anything kind, expressing positive feelings or congratulating a child's successes, not showing any emotions in interactions with a child

A full glossary of terms can be found in the Wales Safeguarding Procedures: https://safeguarding.wales/glossary.html

What to do if a practitioner has a concern

The action that …… (the setting) take to safeguard children will be in line with the Wales Safeguarding Procedures.

It is not the role of any practitioner in our setting to investigate and attempt to seek out evidence on matters relating to safeguarding concerns and they must not attempt to do so. Practitioners in our setting all have a role in assisting social services and/or the police and/or CIW by providing information for safeguarding/child protection enquiries. They recognise that sharing information for the purposes of safeguarding is essential and that safeguarding the individual overrides the need to keep information confidential.

Practitioners in our setting will inform the Designated Safeguarding Person of:

- any concerns that a child or young person is suffering or is likely to be suffering some form of abuse;
- any allegations of abuse against a practitioner;
- any disclosures of abuse.

Any child currently on the Child Protection Register who is absent without explanation for two days will be referred to the social services team.

Not all child protection information results in a report to Social Services, but small

pieces of information may be significant on their own to create a wider picture.

The practitioner who is making the report should seek to obtain consent from parent or carer. This supports positive working relationships between children/young persons and their families. The child and parent/s wish not to report may be over-ridden if it is considered by practitioners that there is still a need for a report.

It may not be appropriate to seek parent consent:

- ❖ the possibility that the child would be put at further risk;
- ❖ the possibility that a child would be threatened or otherwise coerced into silence;
- ❖ a strong likelihood that important evidence would be destroyed/lost;
- ❖ the parent identified as the alleged abuser
- ❖ the child in question not wishing the parent to be involved at that stage and is competent to take that decision;
- ❖ it is in the public interest.

Practitioners should discuss whether it is appropriate to seek consent from the child and parents with their agency's designated safeguarding person (DSP). If the decision is made not to seek consent this decision must be recorded.

Information that should be included in a report:

- Date of disclosure/concern
- Date and time of the record being made
- Name, address and date of birth of the child/children
- Details about the **cause for concern** regarding risk of harm
- A factual report of what happened, what was witnessed or said – use the child's own words!
- Detailed description of any injuries sustained and any allegations, for example sexual abuse, their sources, timing and location
- A note of any other people involved, family circumstances
- Whether the child is safe currently or is in need of immediate protection and actions taken so far
- Whether consent has been obtained and if not, why not
- Any discussions held with the parent/s (where deemed appropriate)
- Name of the person making the report and their job title
- Signature

The Designated Safeguarding Person (DSP) should be informed and given the record. The member of staff should contact Social Services via telephone, to express their concern and Social Services will advise if a report should be made.

- Note the time of the telephone call to Social Services;
- Note the name of the person that is dealing with the telephone call;
- Note the actions to be taken;

If a report is to be made the DSP will support the practitioner (report maker) in completing the Multi Agency Referral Form (MARF) and processing the report.

Further guidance and the relevant Multi Agency Referral Form to make a referral can be found through the Gwent Safeguarding website, at

https://www.gwentsafeguarding.org.uk/en/Children/Report/Report-a-child-at-risk.aspx

*__Remember to create the Picture__ so that the person reading the report gets a clear understanding of why you have concerns about a child or children. Make it factual – how you are involved, what did you see, what did you hear, what happened, where did it happen, when did it happen, who else is involved and why you are reporting.

Third Party Information

Practitioners 'must not leave it to the member of public to contact social services or just advise the person to contact social services directly'. The practitioner has a Duty To Report concerns raised by a member of the public. Practitioners have a responsibility to report any concerns they are alerted to by the general public – both in their work and private lives. When making a report that comes from a third party or the public Practitioners must:

- Record exactly what has been said by the member of public
- Give the information provided to them
- Establish what evidence the member of public has regarding the risk of harm. For example - have they witnessed the abuse, spoken to the individual who is at risk of harm, or heard something?
- Explain that whilst respecting any wish to remain anonymous this may not always be possible, for example if a crime is suspected.

Where possible, members of the public should be encouraged to provide contact details.

The Prevent Duty

As a registered childcare provider we are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, and have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

As a childcare provider, we as a setting, understand our role in identifying the possible risk to children in our care who may be vulnerable to radicalisation by others, whether in their own family or outside.

……(setting) is committed to:

- Taking appropriate action when observing concerning behaviour
- Training practitioners so that they are able to identify families and children who may be vulnerable to radicalisation
- Build children's resilience to radicalisation by promoting fundamental British values.
    1. Democracy
    2. Rule of law
    3. Independent liberty
    4. Mutual respect and tolerance
- Assist in promoting children's learning in their personal, social and emotional development and understanding of the world
- Report any concerns following our setting's safeguarding procedures

Allegations against a practitioner

If an allegation of any form of child abuse is made against a practitioner, the following procedure will be adhered to:-

- All allegations of abuse of children by a professional or practitioner must be taken seriously and treated accordingly
- All practitioners are made aware and understand that they can approach social services or the police, independently, to discuss any worries they have about abuse, neglect or harm and that they should always do so if;
    - ❖ They have concerns that their manager, designated practitioners or proprietors may be implicated;
    - ❖ They have concerns that the manager, designated practitioners or proprietor will not take the matter seriously and/or act appropriately to protect the child; or
    - ❖ They fear intimidation and/or have immediate concerns for their own or for the service user's safety
- All allegations and suspicions of professional abuse must be referred to Social Services, CIW or to the Police. The setting will follow their safegaurding procedures and submit a report.
- All allegations and concerns must be recorded, dated and signed.
- The setting will have high regard to;
    - ❖ Any concerns about a practitioner's behaviour towards their own children/family members;

- ❖ If there are concerns about the practitioner's behaviour towards children unrelated to their employment or voluntary work;
- ❖ When an allegation is made about historical abuse;

- A responsible senior manager from Social Services will meet with the setting's manager for an initial discussion and establish if further action is to be taken. Social Services will provide guidance and inform the setting's manager on how to proceed.
- If further action is to be taken, the responsible senior manager will arrange a strategy discussion with the police to consider any immediate action to be taken to protect the child, and to arrange a strategy meeting.
- At any point after an allegation is made the setting's manager may decide to suspend the practitioner.
- The practitioner should be informed that an allegation has been made at the earliest opportunity. Details of what can be shared will be discussed during the strategy discussion.
- The child's parents/carers will be informed of details of the allegations and the procedures to be followed.
- On no account should the allegation be discussed and direct questioning should be avoided if the police wish to interview the practitioner
- During the strategy discussion, a decision will be made regarding a Professional Strategy Meeting (PSM). If a PSM is to be held, this will be convened by Children's Services. The PSM should develop an action plan with time scales in order to avoid any necessary delay.
- The practitioner will be informed that the child protection enquiry will be carried out in accordance with child protection procedures. The practitioner will be reassured that every effort will be made to preserve confidentiality, however information gained which is relevant to disciplinary or criminal proceedings may be disclosed for this purpose.
- If the practitioner is a member of a trade union or other professional association they should be advised to contact that organisation. They can request copies of the minutes of the Professional Strategy Meeting if they so wish.
- At the conclusion of the investigation the member of staff must be informed, in writing, within 5 working days about the allegation that was made, the procedures followed and the outcome.
- Arrangements should be made to keep the child and their parents/carers informed of the outcomes.
- Where a practitioner is dissatisfied with the enquiries/investigation, or the outcome reached, they should be informed of grievance, complaints or appeals procedures which may by applicable.

Record Keeping

Children's records are freely accessible to parents. However, a written request must be made for personal files on the children as we must take into account data protection rules when disclosing records that refer to third parties.

The designated safeguarding person will ensure that:

• a chronological record of concerns about a child is maintained even if there is no need to make an immediate report;
• all such records are kept confidentially and secure.
• A file is maintained with copies of safeguarding reports, child protection conference minutes, observations, feedback from Social Services, record of injuries, reasons of absence, copies of emails are headed with the child's name, Social Workers name and contact, Health Visitors name and contact and kept within the child's file.

Safe Caring

All practitioners will make:-

- Every effort will be made to avoid or minimise time when practitioners, students or volunteers are left alone with a child. If practitioners are left alone with a child, the door of the room should be kept open and another practitioner should be informed
- If a child makes inappropriate physical contact with a practitioner this will be recorded fully in the Incident Record Book
- Practitioners will never carry out a personal task for children that they can do for themselves. Where this is essential, a practitioner will help a child whilst being accompanied by a colleague. Unless a child has a particular need, a practitioner should not accompany children into the toilet. Practitioners are aware that this and other similar activities could be misconstrued.
- Practitioners will be mindful of how and where they touch children, given their age and emotional understanding. Unnecessary or potentially inappropriate physical contact will be avoided at all times.

Confidentiality

Practitioners cannot keep confidential a disclosure or allegation of abuse and must refer the matter to the Designated Safeguarding Person and/or other senior member of staff. It is important that each practitioner deals with this sensitively. When responding, the practitioner should explain that they must inform the appropriate people who can help, but they will only tell those who need to know in order to be able to help. Practitioners should reassure the child/young person and tell them that their situation will not be common knowledge within the setting. Be aware that it may well have taken significant courage to disclose the information and they may also be experiencing conflicting emotions, involving feelings of guilt, embarrassment, disloyalty (if the abuser is someone close) and hurt.

All reports should be made with the knowledge that during any subsequent investigation, the source (i.e. the setting) will be made known to the family.

All suspicions, enquiries and external investigations are kept confidential and shared only with those who need to know.

Other practitioners may need to be alerted to concerns about a child or young person, possibly in order to monitor the concern or to gather further evidence prior to a report being made, or to assist in providing appropriate support to a child or young person once a report has been made. Information should only be shared on a strict need to know basis.

Relevant Telephone Numbers

Social Services IAA Team	**01495 315700**
Social Services out of hours service	**0800 328 4432**
Gwent Police	**01633 838111**
Care Inspectorate Wales	**0300 7900 126**

This policy was updated on _____ by _____

Staff were made aware of this policy and or updates on _____

This policy will be reviewed on _____

APPENDIX 3

Policy template for Blaenau Gwent Youth Service

Safeguarding/Child Protection Policy

Blaenau Gwent Youth Service is committed to safeguarding the welfare of the young people who engage with us through creating and maintaining an environment where young people are listened to and are able to talk safely about any concerns that they may have.

Legislation

Article 19 of the United Nations Convention on the rights of the child states that children have:

> *'the right to be protected from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation including sexual abuse by those looking after them.'*

It further states that protective measures should, as appropriate, include:

> *'effective procedures for prevention, identification, reporting, referral, investigation, treatment and follow up of instances of child maltreatment.'*

The Children Act 1989 (updated in 2004 following the Victoria Climbie Inquiry) legislates for Children in England & Wales. The principles of the Act are to ensure that the welfare and developmental needs of children and young people under the age of 18 are met. This also includes the need to be protected from harm.

Part V of the Act relates to this and states that in addition to **Social Services** only the **Police** and the **NSPCC** have the legal right and responsibility to investigate concerns about child abuse.

However, when working with children and young people **you have a duty of care** and should report any concerns that you may have. If any person has knowledge, concerns or suspicions that a child or young person is suffering, has suffered or is likely to be at risk of harm, it is their responsibility to ensure that the concerns are referred to one of the agencies that have a statutory duty to make enquiries and intervene when necessary.

The Wales Safeguarding Procedures 2019, takes into account the above legislation and should be used as the main basis for all child protection in Wales. **A copy of this document is available via https://safeguarding.wales/ and the South East Wales Safeguarding Board (https://www.gwentsafeguarding.org.uk/en/Home.aspx) and can be downloaded as an App. It is the responsibility of all staff to familiarise yourself with the documents and it's location.** This policy does not replace this document but provides you with the necessary information and guidance needed to assist you with your duty of care to safeguard young people. This policy sits underneath the **Corporate Child Protection Policy,** which is available via your line manager.

Definitions of Abuse and Neglect

All practitioners should be aware of the definitions of abuse and neglect in the Social Services and Well-being Act (Wales) 2014, as well as the signs and indicators of abuse and neglect. This is essential in order to communicate concerns about harm in a meaningful way.

S.130 (4) of the Social Services and Well-being (Wales) Act 2014 defines a **child at risk** as a child who:

1. Is experiencing or is at risk of abuse, neglect or other kinds of harm;
2. Has needs for care and support (whether or not the authority is meeting any of those needs).

The Social Services and Well Being (Wales) Act 2014 defines abuse and neglect:

'Abuse' means physical, sexual, psychological, emotional or financial abuse and includes abuse taking place in any setting, whether in a private dwelling, an institution or any other place. 'Financial abuse' includes:

- Having money or other property stolen;
- Being defrauded;
- Being put under pressure in relation to money or property;
- Having money or other property misused.

'Neglect' means a failure to meet a person's basic physical, emotional, social or psychological needs which is likely to result in an impairment of the person's well-being for example, impairment of the person's health

'Harm' means abuse or the impairment of (a) physical or mental health, or (b) physical, intellectual, emotional, social, or behavioural development, (including that suffered from seeing or hearing another person suffer ill treatment)

Types of Harm

- **Physical abuse** - hitting, slapping, over or misuse of medication, undue restraint, or inappropriate sanctions;
- **emotional/psychological abuse** - threats of harm or abandonment, coercive control, humiliation, verbal or racial abuse, isolation or withdrawal from services or supportive networks, witnessing abuse of others**;**
- **sexual abuse** - forcing or enticing a child or young person to take part in sexual activities, whether or not the child is aware of what is happening, including: physical contact, including penetrative or non-penetrative acts; non-contact activities, such as involving children in looking at, or in the production of, pornographic material or watching sexual activities or encouraging children to behave in sexually inappropriate ways;
- **financial abuse** - this category will be less prevalent for a child but indicators could be: not meeting their needs for care and support which are provided through direct payments; or complaints that personal property is missing.
- **neglect** - failure to meet basic physical, emotional or psychological needs which is likely to result in impairment of health or development.

Pointers for Practice: Signs and Indicators of Possible Abuse, Neglect and Harm In a Child https://safeguarding.wales/chi/cp/c1p.p2.html?highlight=pointers

A full glossary of terms can be found in the Wales Safeguarding Procedures: https://safeguarding.wales/glossary.html

Safeguarding

If you have a concern that a young person may be at risk of harm (e.g their safety or welfare), but are not in immediate danger or at significant risk then this has to be noted and passed onto your line manager. This may be something that you have heard, seen or had disclosed to you. These cases can be difficult to judge and therefore should be discussed with your line manager, as soon as possible, with action to be taken within the next 24 hours.

Child Protection

If you have a concern, or a young person has made a disclosure that makes you believe that an individual may be at risk of significant or immediate harm you must respond urgently to secure their safety and inform your line manager as soon as possible to inform them of your course of action.

Safeguarding Young People and Staff

(*taken from the Wales Safeguarding Procedures 2019)*

The Social Services and Well-being (Wales Act 2014, specifies the duty to report both adults and children at risk or where there is reasonable cause to suspect are at risk of harm. You have a duty to report concerns, suspicions, observations or disclosures made to you regarding safeguarding/child protection which involves a member of staff. Note the date, time, location and who was present and report to your line manager. Notes should also be kept of meetings/discussions with clear agreement about what action is to be taken and by whom. If the decision is made that no further action is to be taken, this should also be recorded with the reasons for the decision. These notes should be kept in a confidential file should they be required at a later date. Should there be serious concerns, agencies must not make their own internal decisions about whether it is a disciplinary issue or a child protection matter. These complex considerations should only take place with the involvement of social services and the police. The police have the statutory powers and responsibility for determining whether a criminal investigation is to be undertaken.

Informing Young People

As a youth worker it is important to let young people know, where possible before they make a disclosure, that if you have concerns for their wellbeing that you may need to pass that information on to ensure that they are kept safe from harm. Should a concern need to be referred on, be open and honest with the young person, keeping them informed, as much as possible, of the process and steps taken to secure their safety and/or wellbeing.

Informing Parents/Carers

Where possible parents should be informed that a report to Social Services is being made. Consent should be given by the parent/carer for this to happen. If the parent does not consent, yet the concern is still of enough significant for a report to Social Services then a report should still be submitted. It should be made clear on the form the reasons for consent not being given or reasons that parents could not be contacted to inform them of the report.

Sharing Information Among Professionals

A failure to share information is a common finding of practice reviews.

Effective sharing and exchange of information between professionals is essential in order to safeguard children and young people.

The law is rarely a barrier to disclosure of information. There is no restriction in the Data Protection Act or any other legislation that prevents concerns regarding individuals being

highlighted and shared between agencies for the purpose of protecting children. The Bichard and Carlile reports both confirm the need to be aware that concerns from a number of sources, which individually may not be of any significance, can build up a picture which may suggest a child is suffering or at risk of suffering significant harm and therefore requires professionals to act to protect them.

Whenever possible, consent should be obtained before sharing personal information with third parties, but in the public interest in child protection always overrides the public interest in maintaining confidentiality or obtaining consent from families. A child's safety is the paramount consideration in weighing these interests.

Any discussion relating to a young person's welfare should be noted. Note the date, time and who was present at the meeting/discussion. At the end of the meeting/discussion there should be a clear agreement about what action is to be taken and by whom. If the decision is made that no further action is to be taken, this should also be recorded with the reasons for the decision. All concerns about a child or young person's welfare should be documented whether or not further action is taken. These notes should be kept in a confidential file should they be required at a later date.
Pointers for Practice: Seven Golden Rules for Information-Sharing
https://safeguarding.wales/chi/cp/c3p.p5.html?highlight=information-sharing
https://safeguarding.wales/adu/ap/a3pt1p.p7.html?highlight=information-sharing

Supervision

In addition to regular supervision for staff, where there is a safeguarding/child protection concern, line managers should make additional provision for staff to ensure that procedures have been followed and that support and guidance is given to the referring member/s of staff.

Training

All staff will be expected to keep up to date with child protection policies and procedures. Where this necessitates training then staff will be required to attend. Training in respect of safeguarding and child protection will be ongoing and identified by the youth service. Staff will be informed of when this will take place and will be expected to treat this as a diary priority.

Youth Work Staff Located Offsite

All staff should adhere to the Child Protection/Safeguarding procedures of the youth service. Where a youth provision is based within another setting e.g. schools, then staff should obtain and familiarise themselves with the child protection procedures of that setting and have available the name and contact details of the designated safeguarding person. Should a safeguarding/child protection issue be raised, staff should firstly seek

advice from their line manager. Following this, the designated safeguarding person at the setting should be informed of the concern and any action taken.

Youth Work Staff Working in Out of Hours Provision

Staff working out of hours should adhere to the Child Protection/safeguarding procedures of the youth service. Where concerns are raised then the procedures for Out of Hours Service should be followed.

Protection of Adults at risk (PoVA)

As youth workers we provide services to young people aged 11-25 years. This means that we may come into contact with adults who may need intervention from Social Services. Just as with safeguarding/child protection, we have the same duty of care for adults at risk. This means that staff should act if they:-

- Witness abuse;
- Receive information about abuse, suspected abuse or concerns about the care or treatment of a vulnerable adult;
- Have concerns or suspicions about possible abuse or inappropriate care

As with younger aged young people, adults at risk have the same rights to be fully informed and involved in the safeguarding process and make decisions about their safety and welfare. Adults at risk, if they have the mental capacity, should also have their wishes respected if they seem able to make an informed decision about action and/or intervention unless:

- There is a statutory duty to intervene e.g. a crime has been committed or may well be
- It is in the public interest e.g. another person/s are being put at risk
- It is suspected that they are under the undue influence or someone else

Who are Adults at Risk?

The Social Services and Well-being (Wales) Act states that an 'adult at risk' is an adult who:

- is experiencing or is at risk of abuse or neglect;
- has needs for care and support (whether or not the authority is meeting any of those needs;
- as a result of those needs, is unable to protect him/herself against the abuse or neglect or the risk of it.

This definition may include a person who:

- Has learning disabilities

- Has mental health problems
- Is an older person with support/care needs
- Is physically frail or has a chronic illness
- Has a physical or sensory disability
- Misuses drugs or alcohol
- Has social or emotional problems
- Has an autistic spectrum disorder

Abuse can be physical, sexual, psychological, emotional or financial (includes theft, fraud, pressure about money, misuse of money. It can take place in any setting, whether in a private dwelling, an institution or any other place.

Neglect describes a failure to meet a person's basic needs which is likely to result in an impairment of the person well-being. It can take place in a range of settings, such as private dwelling, residential or day care provision.

The following behaviours could place the adult at risk of abuse or neglect (this list is **not** exhaustive):

- Violence against women, domestic abuse and sexual violence (VAWDASV)
- Modern Slavery
- Domestic abuse and violence against men
- Criminal exploitation
- Financial abuse
- Institutional abuse
- Discrimination and hate crime e.g. racial, homophobic, disability
- Forced marriage
- Abuse by another vulnerable adult
- Abuse by children

Pointers for Practice: Signs and Indicators of Possible Abuse and Neglect in an Adult at risk https://safeguarding.wales/adu/ap/a1p.p2.html?highlight=pointers

When making the decision to report an adult at risk, you should apply the same procedures as safeguarding/child protection and may need to refer to **the Wales Safeguarding Procedures**. **It is the responsibility of all staff to familiarise yourself with these procedures and how to access them, https://safeguarding.wales/**

The referral numbers for adults at risk are the same as Child Protection. Links to the relevant forms are found here:
https://www.gwentsafeguarding.org.uk/en/Children/Report/Report-a-child-at-risk.aspx
https://www.gwentsafeguarding.org.uk/en/Adults/Report/Report-an-adult-at-risk.aspx

Full time provision - Safeguarding/Child Protection Procedures

Flow chart

You have a concern about the safety or welfare of a young person (this maybe something you have seen, heard or had disclosed to you) You need to inform the young person (ideally before they disclose) that you may need to pass on any information they disclose regarding their safety.

↓

Note exactly what you have seen, or heard recording as much information as possible. If it is a disclosure – always use the young person's own words, never try to interpret what is being said, only ask questions for clarification. Never ask leading or probing questions.

↓

Contact your line manager, or next appropriate manager to inform them of your concerns

↓

Safeguarding concern

↓

ACT WITHIN 24 HOURS
Complete the appropriate referral form (Appendices 1 & 2) and send to your line manage/other manager for forwarding to Duty Team. Keep a log of times and who you contacted with your notes. A copy should be sent to your designated safeguarding person for information.

↓

Child Protection/PoVA Issue

↓

ACT IMMEDIATELY
Contact Social Services out of hours service or Police. Keep a log of times and who you contacted with your notes. This should be followed with a referral to Social Service as soon as possible via your line manager/other manager with a copy sent to the designated safeguarding person for information

Useful Numbers

Joanne Sims	Youth Service Manager	01495 357866 07772 755435
Claire Madden	Youth Service Development Officer/ Designated Child Protection Officer	01495 357863 07581 628601
Ben Arnold	NEETS Projects Manager	01495 357864 07791 443612
Greg Morgan	Detached Youth Development Officer	01495 355674 07970 208727
Julia Swallow-Edwards	Inspire 2 Achieve Team Lead	01495 355690 07817 760771

Liam Thomas	Engagement and Progression Coordinator	01495 355690 07854 937489

Social Service Referral Telephone Number	01495 315700
Out of Hours Social Services Telephone Numbers	0800 3284432 01495 767045
Police	01633 838111
NSPCC Helpline (for professional advice)	0808 800 5000

Blaenau Gwent Youth Service

Full time Provision located Offsite – Child Protection/Safeguarding Procedures

Flow chart

You have a concern about the safety or welfare of a young person (this maybe something you have seen, heard or had disclosed to you) You need to inform the young person (ideally before they disclose) that you may need to pass on any information they disclose regarding their safety.

↓

Note exactly what you have seen, or heard recording as much information as possible. If it is a disclosure – always use the young person's own words, never try to interpret what is being said, only ask questions for clarification. Never ask leading or probing questions.

↓

Contact your line manager and inform them of concerns and take advice and action if necessary. Contact the designated safeguarding person to inform them of the course of action taken.

↓

Safeguarding concern

↓

ACT WITHIN 24 HOURS

Complete the appropriate referral form (Appendices 1 & 2) and send to your line manager/other manager for forwarding to Duty Team. Keep a log of times and who you contacted with your notes. A copy should be sent to your designated safeguarding person for information.

↓

Child Protection/PoVA Issue

↓

ACT IMMEDIATELY

Contact Social Services out of hours service or Police. Keep a log of times and who you contacted with your notes. This should be followed with a referral to Social Service as soon as possible via your line manager/other manager with a copy sent to the designated safeguarding person for information

Useful Numbers

Joanne Sims	Youth Service Manager	01495 357866 07772 755435
Claire Madden	Youth Service Development Officer/ Designated Child Protection Officer	01495 357863 07581 628601
Ben Arnold	NEETS Projects Manager	01495 357864 07791 443612
Greg Morgan	Detached Youth Development Officer	01495 355674 07970 208727
Julia Swallow-Edwards	Inspire 2 Achieve Team Lead	01495 355690 07817 760771

Liam Thomas	Engagement and Progression Coordinator	01495 355690 07854 937489

Social Service Referral Telephone Number	01495 315700
Out of Hours Social Services Telephone Numbers	0800 3284432 01495 767045
Police	01633 838111
NSPCC Helpline (for professional advice)	0808 800 5000

Blaenau Gwent Youth Service

Out of Hours Provision – Child Protection/Safeguarding Procedures

Flow chart

You have a concern about the safety or welfare of a young person (this maybe something you have seen, heard or had disclosed to you) You need to inform the young person (ideally before they disclose) that you may need to pass on any information they disclose regarding their safety.

↓

Note exactly what you have seen, or heard recording as much information as possible. If it is a disclosure – always use the young person's own words, never try to interpret what is being said, only ask questions for clarification. Never ask leading or probing questions.

↓

Contact your line manager, or next appropriate person to inform them of your concerns.

↓

Safeguarding concern

↓

ACT WITHIN 24 HOURS
Complete the appropriate referral form (Appendices 1 & 2) and send to your line manager/other manager for forwarding to Duty Team. Keep a log of times and who you contacted with your notes. A copy should be sent to your designated safeguarding person for information.

↓

Child Protection/PoVa Issue

↓

ACT IMMEDIATELY
Contact Social Services out of hours service or Police. Keep a log of times and who you contacted with your notes. This should be followed with a referral to Social Service as soon as possible via your line manager/other manager with a copy sent to the designated safeguarding person for information

Useful Numbers

Joanne Sims	Youth Service Manager	01495 357866 07772 755435
Claire Madden	Youth Service Development Officer/ Designated Child Protection Officer	01495 357863 07581 628601
Ben Arnold	NEETS Projects Manager	01495 357864 07791 443612
Greg Morgan	Detached Youth Development Officer	01495 355674

		07970 208727
Julia Swallow-Edwards	Inspire 2 Achieve Team Lead	01495 355690 07817 760771
Liam Thomas	Engagement and Progression Coordinator	01495 355690 07854 937489

Social Service Referral Telephone Number	01495 315700
Out of Hours Social Services Telephone Numbers	0800 3284432 01495 767045
Police	01633 838111
NSPCC Helpline (for professional advice)	0808 800 5000

Types of Harm

All practitioners should be aware of the definitions of abuse and neglect in the Social Services and Well-being Act (Wales) 2014, as well as the signs and indicators of abuse and neglect. This is essential in order to communicate concerns about harm in a meaningful way.

A full glossary of terms can be found in the Wales Safeguarding Procedures https://safeguarding.wales/glossary.html

S.130 (4) of the Social Services and Well-being (Wales) Act 2014 defines a **child at risk** as a child who:

3. Is experiencing or is at risk of abuse, neglect or other kinds of harm;
4. Has needs for care and support (whether or not the authority is meeting any of those needs).

The Social Services and Well-being (Wales) Act states that an 'adult at risk' is an adult who:

- is experiencing or is at risk of abuse or neglect;
- has needs for care and support (whether or not the authority is meeting any of those needs;
- as a result of those needs, is unable to protect him/herself against the abuse or neglect or the risk of it.

Types of Harm

- **Physical abuse** - hitting, slapping, over or misuse of medication, undue restraint, or inappropriate sanctions;
- **emotional/psychological abuse** - threats of harm or abandonment, coercive control, humiliation, verbal or racial abuse, isolation or withdrawal from services or supportive networks, witnessing abuse of others**;**
- **sexual abuse** - forcing or enticing a child or young person to take part in sexual activities, whether or not the child is aware of what is happening, including: physical contact, including penetrative or non-penetrative acts; non-contact activities, such as involving children in looking at, or in the production of, pornographic material or watching sexual activities or encouraging children to behave in sexually inappropriate ways;
- **financial abuse** - this category will be less prevalent for a child but indicators could be: not meeting their needs for care and support which are provided through direct payments; or complaints that personal property is missing.
- **neglect** - failure to meet basic physical, emotional or psychological needs which is likely to result in impairment of health or development.

A full glossary of terms can be found in the Wales Safeguarding Procedures: https://safeguarding.wales/glossary.html

APPENDIX 5

How to make a Report

LISTEN

If you are concerned because of something a child or adult at risk is saying, you should not attempt to take any action directly but **you should**:

- Stay calm
- Listen carefully, do not directly question him or her, instead use open questions; what, where, when, who?
- Never stop them talking if they are freely recalling significant events
- Tell them what you will do next and who you will inform (see below)
- Never promise to keep what you have been told secret or confidential
- Make a note of the discussion, taking care to record what was said, when and where it happened and who else was present

SHARE

Any safeguarding concerns should be discussed with the Designated Safeguarding Person in the respective service area. With the support of the Designated Safeguarding Person the decision to report a concern to Social Services will be made and responsibility for reporting will be agreed i.e. the staff member or the Designated Safeguarding Person will make the report.

Should the concerns relate to a professional, the same procedure will apply. Educational settings must also contact the safeguarding in education manager

Reports in relation to a concern about a child, young person or adult should be made to Social Services as soon as possible and certainly **within 24 hours.**

Social Services Information, Advice and Assistance Service can be contacted on:

01495 315700

Outside office hours, reports should be made to the South East Wales Emergency Duty Team or if there is immediate risk, to the Police.

The Emergency Duty Team can be contacted on: **0800 328 4432**

Practitioners and providers should be aware that they **cannot remain anonymous** when making a report.

The Duty Worker taking the report should be given as much information as possible if it is available to the reporter. This will include the following:

- Full name of the subject of the concern
- Their date of birth or age
- Their address
- The nature of the concern
- Who may be responsible
- Their name and relationship (if any)
- What happened
- When and where
- What has been done in response
- Whether or not the Police have been informed
- The names and relationship of those with caring responsibility
- The names and ages of any other adults living in the household
- The names of any professionals known to be involved e.g. school, GP
- Any information affecting the potential safety of staff
- The allocated social worker or team if known/if applicable

RECORD

All telephone reports should be confirmed in writing within two working days.

- For Children, a Multi-Agency Referral Form (MARF) should be used:

https://www.gwentsafeguarding.org.uk/en/Children/Report/Report-a-child-at-risk.aspx

- For an Adult, a Duty to Report form should be used.

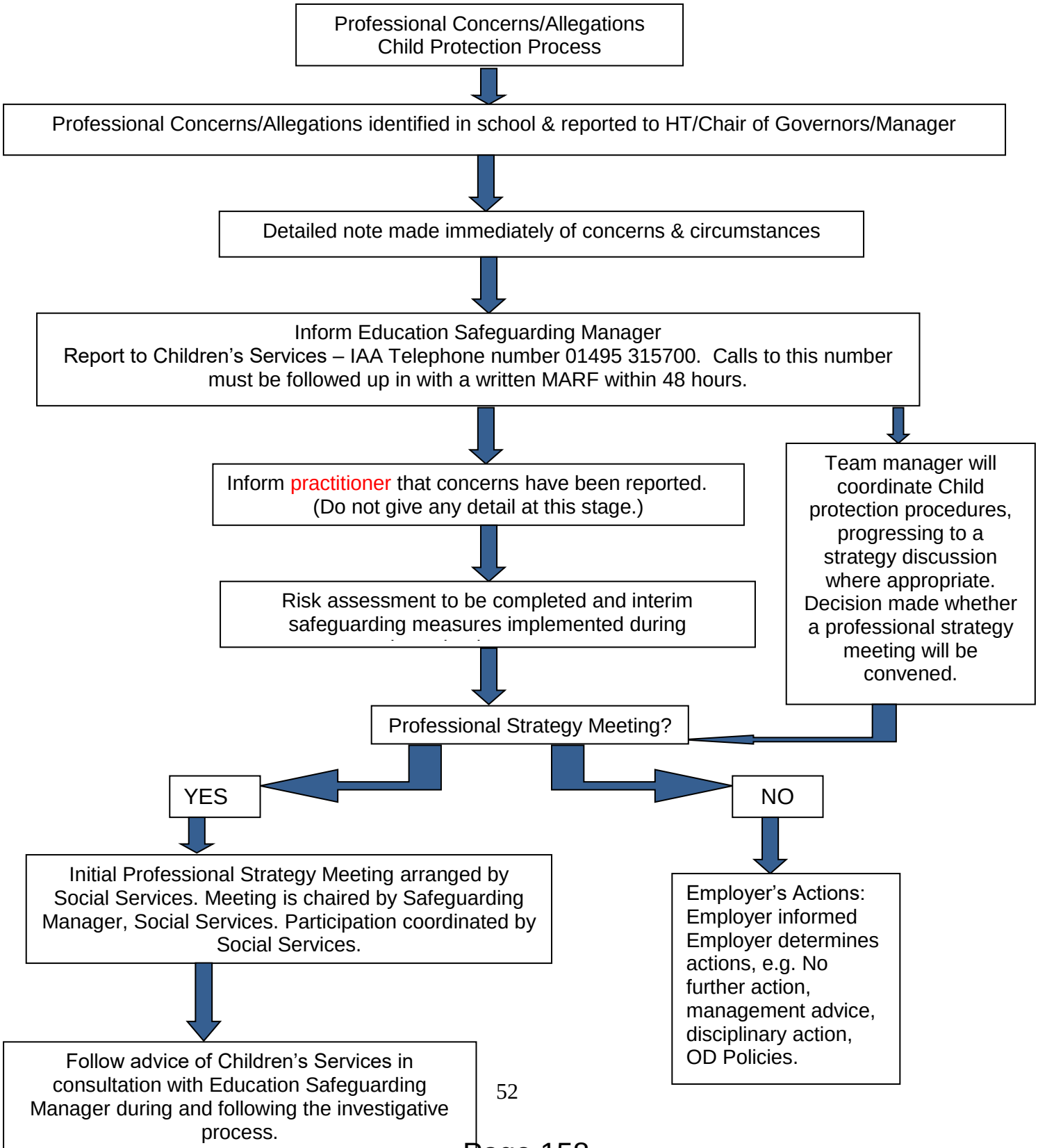
https://www.gwentsafeguarding.org.uk/en/Adults/Report/Report-an-adult-at-risk.aspx

LISTEN, SHARE, RECORD

APPENDIX 6

PROFESSIONAL CONCERNS/ALLEGATIONS

This Flowchart should be used as a brief checklist of procedure for professional concerns/allegations
Detailed procedures are outlined in Wales Safeguarding Procedures, section 5
Also refer to Safeguarding Children in Education: Handling Allegations of abuse against teachers and other staff 009/2014



APPENDIX 7

Safeguarding File - Transfer of Records

A receiving school must be made aware of the existence of a Child's Safeguarding file prior to the child transferring from their original school.

The confidential Safeguarding File must be securely transferred to the new school either in Person, or via secure mail that requires a signature of receipt. This Transfer of Records form should be completed and forwarded with the file to the new school. Either the Head teacher or the Designated Senior Person for safeguarding should sign receipt for the file.

Sending Schools should retain a copy of the signed` Transfer of Records forms as evidence of the transfer, and ensure appropriate signatures are obtained.

Child Name	
DOB	

Name of sending school/setting:		
Date record ended at this school/setting (pupil end date):		
Name of receiving school/setting:		
Date of contact with new school/setting		
Has sensitive and urgent information been shared with new school/setting?	**Yes / No**	**If No, why not?**

Name of DSP sending records	
Date file sent	
File passed to (name):	

This section to be completed by the receiving school if file delivered by hand.

Receiving School/setting	
Signed	
Print name and position	
Date	

This section to be completed by the sending school with the postage receipt reference if file sent via secure post as proof of sending.

Reference number of postage receipt	
Name and address of recipient	
Date of postage	

APPENDIX 8

Community Cohesion – Preventing Extremism

Our school/setting is committed to providing a safe environment for all of our children, staff and any visitors. There is no place for extremist views of any kind in our school/setting.

Community cohesion is the term used to describe how everyone in a geographical area lives alongside each other with mutual understanding and respect. A cohesive community is where a person has a strong sense of belonging. It is safe, vibrant and able to be resilient and strong when tensions occur.

Those involved in supporting terrorism look to exploit and radicalise vulnerable people, including children and young people. Since July 2015, the Counter Terrorism and Security Act 2015 introduced a statutory duty on us 'to have due regard to the need to prevent people from being drawn into terrorism'

We are aware that young people can be exposed to extremist influences or prejudiced views from an early age which spring from a variety of sources including the internet. At times students, visitors or parents may themselves reflect or display views that may be considered as discriminatory, prejudiced or extremist, including using derogatory language; this will always be challenged and where appropriate dealt with.

Education is a powerful deterrent against this and we will strive to equip young people with the knowledge, skills and resilience to challenge and discuss such issues in a facilitated and informed way. This way our students are enriched, understand and become tolerant of difference and diversity where they can thrive, feel valued and not marginalised.

We have a clear safeguarding framework on how to manage and respond to issues where a pupil develops or expresses extreme views and ideologies, which are considered inflammatory and against the community cohesion ethos of our school.
Where such cases are identified a Multi-Agency Referral Form is to be completed and submitted to Children's Services. The Local Authority Lead Officer for PREVENT should also be contacted.

Safeguarding Channel Panel

Safeguarding and promoting the welfare of children, young people and adults is everyone's responsibility. We are committed to working with our partners to protect and support our students, and where a Multi-Agency Referral Form leads to one of our Students needing safeguarding, we will support the Channel programme.

Channel is a multi-agency approach to protect vulnerable people by identifying individuals at risk; assessing the nature and extent of that risk; and developing the most appropriate support plan for the individuals concerned.

Channel is about ensuring that vulnerable children and adults of any faith, ethnicity or background receive support before their vulnerabilities are exploited by those that would want them to embrace terrorism, and before they become involved in criminal terrorist related activity.

Training

We are committed to ensuring that all staff in our school have access to the Workshop to Raise Awareness of Prevent (WRAP) and are encouraged to make use of other counter-terrorism related training modules and the reference material below.

Key Points of Contact

…… School's/Setting's Safeguarding Lead

Helena Hunt
Prevent Lead for Blaenau Gwent County Borough Council
Email: Helena.hunt@blaenau-gwent.gov.uk Tel: 07791 875737

Reference Material

Respect and Resilience – Developing Community Cohesion
https://gov.wales/sites/default/files/publications/2018-03/respect-and-resilience-developing-community-cohesion.pdf

Respect and Resilience – Developing Community Cohesion: Assessment tool:
https://gov.wales/respect-and-resilience-self-assessment-tool-schools

Prevent Duty Guidance: https://www.gov.uk/government/publications/prevent-duty-guidance

Channel Guidance: https://www.gov.uk/government/publications/channel-guidance

E-learning training on:
PREVENT Awareness:
https://www.elearning.prevent.homeoffice.gov.uk/edu/screen1.html

PREVENT Referrals:
https://www.elearning.prevent.homeoffice.gov.uk/preventreferrals

Channel Awareness:
https://www.elearning.prevent.homeoffice.gov.uk/channelawareness

Website: http://educateagainsthate.com Resources for parents and teachers

APPENDIX 9

Secure and Shelter Procedure *(example)*

Secure and Shelter (Lockdown) procedures may be activated in response to any number of situations, but some of the more typical might be:

- A reported incident / civil disturbance in the local community (with the potential to pose a risk to staff and pupils in the school)
- An intruder on the school site (with the potential to pose a risk to staff and pupils)
- A warning being received regarding a risk locally of air pollution (smoke plume, gas cloud etc.)
- A major fire in the vicinity of the school
- The close proximity of a dangerous dog roaming loose

The school's secure and shelter plan is as follows:

Signal for secure and shelter	
Signal for all clear	

Actions - dependent upon the cause of the activation of Safe and Secure *(amend as required)*

- *Who sounds the alarm / other form of notification (specify)*
- **Pupils who are outside of the school buildings** are brought inside as quickly as possible and return to their *classroom / other location (specify)* (outside staff will be informed by a senior member of staff)
- **Those inside the school** should remain in their classrooms and check corridors and toilets for pupils or staff
- All external doors and, as necessary, windows are closed (depending on the circumstances, internal classroom doors must also be closed).
- If the cause of the secure and shelter is air pollution, close air vents and switch off extractor fans / air conditioning.
- Blinds should be drawn and pupils sit quietly
- Once in lockdown mode, staff should notify the office immediately of any pupils not accounted for via the internal telephone system and instigate an immediate search for anyone missing
- Staff should encourage the pupils to keep calm

- The school office will establish communication with the Emergency Services
- If it is necessary to evacuate the building, the fire alarm will be sounded and the usual fire evacuation procedure will then take place
- Parents will be notified as soon as it is practicable via Parentmail and the website (only when appropriate via guidance from Emergency Services)
- Pupils will not be released to parents during a safe and secure situation.

All situations are different, once all staff and pupils are safely inside, senior staff will conduct an on-going risk assessment based on advice from the Emergency Services.

This can then be communicated to staff and pupils. Emergency Services will advise as to the best course of action in respect of the prevailing threat.

All Clear

Once the incident has been assessed as safe all classrooms will be either visited by a senior member of staff or via classroom telephone and told the situation is under control and the class can resume activities as normal.

Emergency Services

It is important to keep lines of communication open with Emergency Services as they are best placed to offer advice as a situation unfolds. The school site may or may not be cordoned off by Emergency Services depending on the severity of the incident that has triggered the Lockdown.

Emergency Services and Corporate Communications will support the decision of the Headteacher with regarding the timing of communication to parents.

Safe and Secure Drill

It is of vital importance that the school's Safe and Secure procedures are familiar to all members of the school staff. To achieve this, a drill should be undertaken at least once a year.

Staff will ALWAYS have advance notice of a Safe and Secure drill, therefore if the signal occurs without warning staff must assume it is NOT A DRILL.

Parents will be notified as soon as it is practicable of the drill via Parentmail and the website

Associated Policies, Guidance and Advice

- Wales Safeguarding Procedures – 2019
  https://safeguarding.wales/
- Keeping Learners Safe: The role of local authorities, governing bodies and proprietors of independent schools under the Education Act 2002. (January 2015)
- https://gov.wales/keeping-learners-safe
- Recruitment and selection policy
  http://intranet/organisational-development-(hr)/schools-hr/recruitment.aspx
- Violence against Women, Domestic Abuse and Sexual Violence (VAWDASV) education toolkit
  https://gov.wales/violence-against-women-domestic-abuse-and-sexual-violence-vawdasv-educational-toolkit
  https://gov.wales/violence-against-women-domestic-abuse-and-sexual-violence-guidance-governors-0
- Safeguarding in Education: handling allegations of abuse against teachers and other staff – circular 009/2014 (April 2014)
- https://gov.wales/handling-allegations-abuse-against-teachers-and-staff
- Disciplinary and dismissal procedures for school staff- circular 002/2013 (replaces circular 007/2001)
  https://gov.wales/disciplinary-and-dismissal-procedures-school-staff
- Blaenau Gwent Corporate Safeguarding Policy
  http://intranet/media/130044/Corporate_Safeguarding_Policy_May_2017docxv3.pdf
- Procedures for Whistle blowing in Schools and Model policy- circular 036/2007
  https://gov.wales/whistleblowing-schools-guidance-governors
  Blaenau Gwent Whistleblowing policy
  http://intranet/media/92682/Whistleblowing-Policy-for-School-based-staff.pdf
- Safeguarding Children: Working Together Under the Children Act 2004
  https://www.basw.co.uk/system/files/resources/basw_14350-5_0.pdf
- Procedures for reporting misconduct and incompetence in the education workforce in Wales-Welsh Government 168/2015 (replaces 018/2009)
  http://dera.ioe.ac.uk/23182/1/150608-reporting-misconduct-en.pdf
- Safe and effective intervention-use of reasonable force and searching for weapons, Welsh Government circular 097/2013 (replaces 041/2010).
  https://gov.wales/sites/default/files/publications/2018-03/safe-and-effective-intervention-use-of-reasonable-force-and-searching-for-weapons.pdf
- Children Missing from Education WG circular 002/2017 (replaces circular 006/2010)
  https://gov.wales/children-missing-education
- Education Records, School Reports and the Common Transfer System - Circular 18/2006
  https://gov.wales/sites/default/files/publications/2018-03/educational-records-school-reports-and-the-common-transfer-system-the-keeping-disposal-disclosure-and-transfer-of-pupil-information.pdf

- Teaching Drama: guidance on Safeguarding Children and Child protection for managers and drama teachers- National Assembly for Wales circular 23/2006 http://dera.ioe.ac.uk/7299/1/clwych-drama-guidance-e.pdf%3Flang%3Den
- The Control of School Premises (Wales) Regulations 2008 http://www.legislation.gov.uk/wsi/2008/136/made http://www.legislation.gov.uk/wsi/2008/136/note/made

Gwent Safeguarding:

https://www.gwentsafeguarding.org.uk/en/Home.aspx

Services for people from Black and Ethnic Minority (BME) backgrounds:

- BAWSO http://www.bawso.org.uk/

Domestic Abuse:

- https://gov.wales/live-fear-free
- https://www.gwentsafeguarding.org.uk/en/VAWDASV/VAWDASV.aspx
- info@phoenixdas.co.uk

Modern Slavery
https://gov.wales/live-fear-free/slavery

Keeping Safe Online
https://hwb.gov.wales/zones/online-safety/key-information/

APPENDIX 11

Blaenau Gwent County Borough Council
Safeguarding Data Protocol

Introduction

The governing body of a maintained school is responsible for the conduct and standards of the school; the Council shares the responsibility for standards in schools and discharges these responsibilities for the overall provision of education services in Blaenau Gwent.

The Council provides governing bodies with support through strategic support services that help to create a level of common policy planning and practices that schools share. As part of this, support is provided through the commissioned service known as the South East Wales Education Achievement Service (SEWEAS).

In order to manage the improvement process, there is a need to share information on a timely basis to ensure that appropriate monitoring, evaluation and reporting occurs and where appropriate timely intervention takes place.

The Council and its schools take their safeguarding responsibilities seriously and the purpose of this protocol is to articulate the timeframes in which the data will be shared

Background

This protocol sets out good practice for the exchange of safeguarding information between schools and the local authority in the discharge of statutory functions.

Principles

The Council has a dedicated Safeguarding in Education Manager who will manage the information and the return of the data from schools. Data is to be returned twice a year and a timetable will be established and shared with schools at the start of the Autumn term.

Protocol

The information required is detailed below. The request for information will be generated by a member of Business Support and all information will be sent to the Business Support officer using the return email address Timothy.Griffiths@blaenau-gwent.gov.uk by the dates specified.

The Safeguarding in Education Manager will maintain effective oversight of the information and use it to inform training and support programmes.

Any identified trend which requires immediate intervention will be managed by the Safeguarding in Education Manager.

Training:	*Dates of safeguarding training that have taken place since the previous data submission for the following:* • Whole school staff training – individual staff names to be confirmed • Designated and Deputy Designated Senior Person, including title of course • Chair of governors and lead governor for safeguarding • Individual governors *Date of PREVENT training and who received this training.* *Date of VAWDASV training and who received this training*
Policy adoption:	*Policy adoption dates will be required only where polices have been reviewed and distributed to schools since the previous adoption date:* Safeguarding policy Online Safety Policy Internet and Social Networking policy Appropriate use of the internet Anti-bullying policy Physical Intervention Safer recruitment policy Volunteer Guidance Whistle Blowing Policy Time-out policy Strategic Equity Plan Partnership Agreement
Governors	*Confirmation of DBS certificate number and issue date* *Date of safeguarding training*
Volunteers:	*Confirmation of DBS certificate number and issue date* *Reference details* *Date of safeguarding training*

Training

Any training requirements for reporting of the data should be made to the Safeguarding in Education Manager.

Safeguarding Data Reporting Timeframe for 2020/2021 academic year

Date	Start	Half Term Starts	Half Term Ends	Term Ends	Data returned by
Autumn	01/09/2020	26/10/2020	30/10/2020	18/12/2020	**13/11/2021**
Spring	04/01/2021	15/02/2021	19/02/2021	26/03/2021	N/A
Summer	12/04/2021	31/05/2021	04/06/2021	20/07/2021	**26/4/2021**

APPENDIX 12

Example: Covid 19 Child Protection Policy Annex: to be read in conjunction with the school's safeguarding/child protection policy.

Introduction

At this time when the landscape is changing day to day, we must all remember we still have a duty to safeguard children.

The purpose of this policy annex is to reflect the different ways in which we are working and to reinforce the procedures that remain in place to safeguard children.

Whilst acknowledging the pressure that schools and colleges are under during the lockdown period, it remains essential that they continue to be safe places for children. The '**Keeping learners safe**' guidance continues to apply to school or college settings.

- the best interests of children must always continue to come first
- if anyone in the school has a safeguarding concern about any child they should continue to act immediately
- a designated safeguarding person (DSP) should be available and easily identified
- unsuitable people must not enter the children's workforce and/or gain access to children
- children should continue to be protected when they are online
- schools should, as far as possible, take a whole setting approach to safeguarding. This will ensure that any new policies and processes in response to coronavirus are not weakening their approach to safeguarding or undermining their child protection policy.

Procedures

During the **COVID 19** outbreak the Information, Advice and Assistance Team (IAA) continue to be fully operational, the office hours remain as 9am - 5pm Monday – Friday.

The IAA Team will be able to offer advice if you have concerns for a child. They can be contacted on:

- **01495 315700**

Referrals can continue to be made to Blaenau Gwent Children's Services using a multi-agency referral form (MARF). This form can be found on the Gwent Safeguarding website: https://www.gwentsafeguarding.org.uk/en/Children/Report/Report-a-child-at-risk.aspx

The MARF should be sent to:

- **DutyTeam@blaenau-gwent.gov.uk**

After 5pm, on weekends and bank holidays, contact the South East Wales Emergency Duty Team (EDT) to report any safeguarding concerns:

- **0800 328 4432**

If you think a child or young person is in immediate danger, contact the Police on 999.

The Legal Framework

The Social Services and Well-being (Wales) Act 2014 specifies the ***duty*** placed on practitioners and partners under s.162 of the Act to report both adults and children including unborn children where they have reasonable cause to suspect the criteria regarding risk of harm is met.

A report ***must*** be made whenever a professional has concerns about a child under the age of 18 years.

If any person has knowledge, concerns or suspicions that a child is suffering has suffered or is likely to be at risk of harm, it is their responsibility to ensure that the concerns are reported to social services or the police who have statutory duties and powers to make enquiries and intervene when necessary

It is important that practitioners and partners do not ignore or dismiss suspicions as everybody has a responsibility to safeguard children.

The Social Services and Well-being (Wales) Act 2014 defines a **child at risk** as a child who:

1. Is experiencing or is at risk of abuse, neglect or other kinds of harm;

The Act provides definitions of abuse and neglect as follows:

Abuse means physical, sexual, psychological, emotional or financial abuse (and includes abuse taking place in any setting, whether in a private dwelling, an institution or any other place), and 'financial abuse' includes theft, fraud, pressure about money or misuse of money

Neglect means a failure to meet a person's basic physical, emotional, social or psychological needs, which is likely to result in an impairment of the person's well-being (for example, an impairment of the person's health).

Harm means abuse or the impairment of (a) physical or mental health, or (b) physical, intellectual, emotional, social or behavioural development, (including that suffered from seeing or hearing another person suffer ill treatment).

Identifying and reporting Concerns

During this period of lockdown and self-isolation there have been increased risks for those living at home with someone who may display abusive behaviours. It may be more difficult to report concerns.

Limited numbers of children have been attending settings during the lockdown period. As schools re-open to all learners, all staff need to be alert to the signs of abuse and know how to respond to a person who may disclose abuse. Practitioners may identify new safeguarding concerns about individual children as they start to see them in person.

Whether safeguarding concerns are identified regarding a pupil attending the school site or through continued contact arrangements by school staff with students, the school continues to have a legal duty to report all safeguarding concerns.

Whether a child is attending the setting or accessing learning from home, school continues to be a support to pupils and parent/carers who are concerned about harm or abuse. Any pupils, parents/carers who are concerned about harm or abuse, should contact their class or form teacher or another adult in the school to share their concerns.

During the COVID restrictions, multi-agency meetings have been held using remote ways of working. Education Staff will continue to work with children's social workers and contribute to safeguarding meetings in this way.

Safeguarding and supporting children during the COVID 19 period continues to be a priority. To report concerns, follow the procedures set out in this annex.

Concerns about a staff member/volunteer who may pose a safeguarding risk to children**:** any concerns within the setting must be reporting to the Headteacher. If the concern relates to the Headteacher, contact the Safeguarding in Education Manager. Safeguarding concerns about a member of staff/volunteer must be reported to the IAA

The Safeguarding in Education Manager must be contacted for all concerns about a member of staff/volunteer. Sarah.Dixon@blaenau-gwent.gov.uk 07815 005241. If not available, contact the IAA

Designated Safeguarding Person (DSP)

The Designated Safeguarding Person (DSP) for the setting is:

The Deputy DSP is:

Contact arrangements for the DSP/Deputy DSP will be displayed around the building and communicated to all staff/volunteers. If the DPS/deputy is off site, then they will be available via remote means, for example, by telephone or video conference, or an alternative named member of staff will be designated for contact for safeguarding matters. This information will also be communicated to staff who are working in any alternative buildings, if the school uses any off-site buildings.

Any changes to these arrangements will be communicated to all staff/volunteers.


WG
designated-safegua


WG
practitioner-handou

The Safeguarding in Education Manager for Blaenau Gwent is Sarah.Dixon@blaenau.gwent.gov.uk

Operation Encompass

Operation Encompass continues to operate during the lockdown period.

The purpose of Operation Encompass is to safeguard and support these children and young people who have witnessed and/or been present at the time of a domestic abuse incident.

The Live Fear Free helpline is available 24 hours a day, 7 days a week, for free advice and support or to talk through options:
0808 80 10 800 info@livefearfreehelpline.wales
https://gov.wales/live-fear-free/staying-safe-during-coronavirus-emergency

Keeping Safe Online

During the COVID restrictions, children and young people are likely to spend more time online, whether for entertainment, to stay in touch with friends and family or to support their home learning. There are clearly many benefits to staying connected, however, increased time online may also increase the risk of encountering online safety issues.

Useful links for staying safe online:

Keeping safe online guidance from Welsh Government https://hwb.gov.wales/zones/online-safety/key-information/

Live streaming guidance https://hwb.gov.wales/zones/online-safety/live-streaming-safeguarding-principles-and-practice-for-education-practitioners/

Reporting harmful content found online https://reportharmfulcontent.com/

Online safety playlist for parents https://hwb.gov.wales/zones/online-safety/news/articles/21e491a7-e417-4570-92dd-12bd7ba05747

Wales Safeguarding Procedures

This setting follows the Wales Safeguarding Procedures 2019 and also policies, protocols and guidance documents that have been endorsed by Gwent Safeguarding

Detailed information on safeguarding procedures, a glossary of terms and All Wales Practice Guides can be found in these procedures https://safeguarding.wales/

Gwent Safeguarding links

https://www.gwentsafeguarding.org.uk/en/Children/Protocols-and-Procedures/Protocols-and-Procedures.aspx.

https://www.gwentsafeguarding.org.uk/en/Children/Professionals/Professionals.aspx

https://www.gwentsafeguarding.org.uk/en/Children/Parents-and-Carers/Parents-and-Carers.aspx

https://www.gwentsafeguarding.org.uk/en/Children/Children-and-Young-People/Children-and-Young-People.aspx

Communication protocol for contacting families during lockdown

During the school re-purposing period, schools continued to contact families. A protocol for communication was implemented and can continue to be used during the school re-opening phase.

Communication_protocol_V4_-_4.5.20.c

Welsh Government Guidance:

This guide aims to assist practitioners in accessing information and advice on identifying abuse and/or supporting disclosure and reporting concerns

https://gov.wales/keeping-children-and-young-people-safe-non-statutory-guide-practitioners

This page is intentionally left blank

Executive Committee and Council only

Date signed off by the Monitoring Officer: N/A

Date signed off by the Section 151 Officer: N/A

Committee:	**Joint Social Services & Education and Learning (Safeguarding) Scrutiny Committee**
Date of meeting:	**8th October 2020**
Report Subject:	**Safeguarding Performance Information for Social Services – 1st April 2019 to 31st March 2020**
Portfolio Holder:	**Cllr John Mason, Executive Member Social Services**
Report Submitted by:	**Damien McCann, Corporate Director of Social Services**
	Alison Ramshaw, Service Manager, Children's Services

Reporting Pathway								
Directorate Management Team	**Corporate Leadership Team**	**Portfolio Holder / Chair**	**Audit Committee**	**Democratic Services Committee**	**Scrutiny Committee**	**Executive Committee**	**Council**	**Other (please state)**
22.09.20	24.09.20	24.09.20			08.10.20	14.10.20		

1. Purpose of the Report

1.1 The purpose of this report is to provide scrutiny members with safeguarding performance information and analysis from children's social services from 1st April 2019 to the 31st March 2020. Monitoring and reporting systems are well developed to ensure the department is able to track information and evidences that the safeguarding agenda remains a priority for the local authority.

1.2 The information provided will enable members to identify safeguarding trends and areas within the authority that require further development to improve safeguarding practice in order to meet the safeguarding needs of children and young people within Blaenau Gwent.

2. Scope and Background

2.1 The report contains safeguarding information from social services from 1st April 2019 – 31st March 2020 (Q's 1, 2, 3 & 4)

2.2 This report is written in order to provide a greater focus on the safeguarding agenda. The Corporate Leadership Team and Elected Members agreed for safeguarding information to be reported to a Joint Social Services /Education and Learning Scrutiny Committee.

2.3 Members will be aware that a separate briefing note has been provided to this committee in respect of the educational element of this report in relation to the period January to March 2020 in the light of the pandemic

3. **Options for Recommendation**

3.1 The Safeguarding Performance Information has been approved by CLT at their meeting on 24th September 2020.

Having scrutinised the information members can:

3.2 **Option1**
Accept the approach and information detailed in the report provided

3.3 **Option 2**
Consider the information provided and provide comments on where improvement can be made to the current monitoring processes.

4. **Evidence of how does this topic supports the achievement of the Corporate Plan / Statutory Responsibilities / Blaenau Gwent Well-being Plan**

4.1 The Safeguarding agenda is considered as part of the Council's Corporate Strategies that includes:

- Corporate Plan
- Well-Being Plan
- Corporate Risk Register
- Safe Reduction of CLA Strategy
- Early Intervention and Prevention Strategy

4.2 Social Services work to a number of regional and national safeguarding procedures which can be located on the South East Wales Safeguarding Children's Board website: **http:/sewsc.org.uk**

5. **Implications Against Each Option**

5.1 ***Impact on Budget (short and long term impact)***

Q's 1, 2, 3 & 4 has seen the number of children on the child protection register vary from 61 at the lowest and 72 being the highest. The numbers of children looked after remained stable with the overall trend showing a decrease in numbers. This along with the lower numbers of court applications continuing a positive impact on the budget

The safeguarding team experienced some staffing challenges in the first 3 quarters of the reporting period however this has since changed with the safeguarding team operating at full capacity, which has negated the need to seek staffing support from the independent sector.

5.2 ***Risk including Mitigating Actions***

The Directorate Risk register identifies the highest risks for the Social Services Department. These are monitored as part of the quarterly report of the Director of Social Services.

6. **Supporting Evidence**

6.1 **Performance Information and Data (see Appendix 1)**
Social Services

6.1.1 **Referrals to Social Services**

6.1.2 **Figure 1:1** Shows the number of referrals made to social services within the four reporting quarters. The chart demonstrates a slight increase in referrals during Q2 (*1,192*) with a slight dip then in Q3 (*1,031*) with a second slight rise in Q4 (1189). The overall data evidences consistency in referral rates and despite Q's2 & 4 sowing an increase this increase is not significant enough to raise safeguarding concerns.

6.1.3 **Figure 1.2:** Shows the source of the referrals, again the data provides a consistent picture in that police remain the highest referring agency (1,434 for all four quarters) followed by Education (771) and then closely followed by Health (626)

6.1.4 **Figure 1.3:** shows the numbers of referrals received into the department on open cases. During Q2 the number increased to 1,029 from 806 in Q1 this number increased again slightly in Q3 to 1.036. In Q4 this had risen to 1888.
The rise in additional referrals on open cases was analysed and it would appear that referrals for those cases open to the 14+ team were high in all four quarters. Further analysis evidenced that of these numbers a high percentage of children were being managed under the exploitation risk management processes and the 115 (contextualised safeguarding) meeting. This would account for the high percentage of referrals for this cohort of children.
For those children aged 0 -13 years the numbers of additional referrals on open cases are on average similar to previous quarters.

It is noteworthy to mention that whilst the numbers of referrals on open case can appear high, duplication and for information only MARF's are also captured under a re referral

6.1.5 **Youth Services**

Figure 1.4: Shows the numbers of youth service referrals during tis reporting period and the data shows a fluctuation in the numbers of referral throughout the year. Whilst the numbers of referrals are low, I can confirm that those young people attending youth service provision also attend an education provision and the likelihood is that their needs are picked up through education referrals. Young people are also referred into the preventative

service provisions where needs are assessed and met in accordance with that assessed need.

The Youth Service is an active partner on the Space Wellbeing Panel, they sit on the Steering Group as part of the Families First model and they actively participate in the South East Wales Safeguarding Local Network meetings. Multi agency working and close partnership arrangements with the youth service ensure that safeguarding is prioritised.

6.1.6 **Child Protection**

6.1.7 **Figure 2.2:** Gives a summary of the number of children on the child protection register the numbers of registrations and deregistration is also included. There were a total of 61 children on the child protection register in Q2 to 32 families. This accounted for an additional 17 children being registered in this quarter. The numbers of children on the child protection register decreased by 9 in Q2.
Q3 saw a slight rise in registrations with 72 children on the child protection register to 35 families. During Q4 the numbers of children on the child protection register decreased to 61 The numbers throughout the four quarters indicates an overall trend as the numbers in previous quarters demonstrates similar numbers

70 in Q1 (2019)
61 in Q2 (2019)
72 in Q3 (2019)
61 in Q4 (2020)

6.1.8 **Figure 2.5:** shows the average time a child is on the CPR. The social services senior management team review all those children on the CPR for 12 months or longer to ensure there is no unnecessary drift. It is pleasing to see that over the last 4 quarters these numbers continue to reduce, with no children being recorded as being on the child protection register for more than 24 months. Significant reduction in time spent on the child protection register for periods of 6 – 12 months and 12 – 24 months can also be see in Q4

6.1.9 **Figure 2.6:** gives the breakdown on both initial and review conferences. They show the numbers of conferences held the number of families involved and the outcomes in terms of registered or not.

The numbers of initial conferences remained consistent averaging between 25/39 throughout this reporting period. (108 in total)

201 review conferences were held in the four Q's with 96 continued registrations and 105 reaching an outcome of deregistration

Of the numbers of initial conferences held throughout the four reporting quarters 94 children were registered 11 were not and 3 registrations were agreed pre-birth.

6.1.10 **Figure 2.7:** shows the number of initial conferences held within timescales. There has been consistence practice in this area throughout Q's 1, 2, & 3 (100%) with a dip Q4 showing at 86%

6.1.11 **Figure 2.8:** relates to review conferences and the graph shows excellent performance with just slight dips in the 100% target.

- **Q1 – 100%**
- **Q2 – 91%**
- **Q3 – 100%**
- **Q4 – 98.5%**

6.2 **Expected outcome for the public**

Those children who are assessed to be at risk of harm are protected and safeguarded, and that the Local Authority adheres to legislation regarding statutory intervention.

6.3 **Involvement (consultation, engagement, participation)**

6.3.1 The development of the Corporate Safeguarding Policy and the Departmental Safeguarding Leads help ensure all departments within the Authority are aware of their responsibilities for safeguarding and are kept undated with any emerging issues or trends within safeguarding.

6.3.2 Termly meetings also take place with the Safeguarding Leads from all the schools and monthly meetings take place between the safeguarding team and lead education staff.

6.3.3 The SEWSCB local Safeguarding Network group also reviews the safeguarding information to ensure all partner agencies are as fully aware as possible.

6.4 **Thinking for the Long term (forward planning)**

The Annual Council Reporting Framework (ACRF) enables Social Services to plan for the future as spend, risk and performance is continuously reported on and provides a baseline of where the department is currently and where it needs to be in the future.

6.5 **Preventative focus**

6.5.1 The work undertaken by the Social Services Directorate looks to promote a preventative approach to practice through early identification and intervention. Having a proactive rather than reactive approach to service planning can also help with planning resources.

6.5.2 Providing this report and the level of detailed safeguarding information to Scrutiny Committee enables members to ensure risks are identified and acted on.

6.6 **Collaboration / partnership working**

The South East Wales Safeguarding Children's Board and its sub groups ensure a multi-agency collaborative approach to safeguarding. Blaenau Gwent fully participates in the Children's and Adults Safeguarding Boards.

6.6.1 Additionally, the Corporate Safeguarding Policy ensures each department has safeguarding leads and these meet together on a quarterly basis looking at safeguarding across the whole Authority. The Leisure Trust lead also participates in this meeting.

6.6.2 Throughout the four Q's partnership working with the police continues to progress through the Early Action Together programme. The Detective Sergeant (DS) in post continues to make positive contributions to the safeguarding process. Strategy Discussions are now being held in a timely manner (within 24hours) and information relevant to safeguarding decision making happens in a much more efficient manner.

6.6.3 Regarding the quality assurance element to the DS role, it has been reported through the Early Action Together steering group meetings that the police are feeling better supported in the completion of the PPN's and this has been evidenced with the Information Advice and Assistance service as the quality of information in the PPN's is much improved.

6.7 **Integration (across service areas)**

All local authorities and partner agencies work together on safeguarding through the South East Wales Safeguarding Children Board and Gwent wide Adult Safeguarding Board.

6.8 **EqIA**

N/A

7. **Monitoring Arrangements**

The Local Safeguarding Network Group is a sub group of the South East Wales Safeguarding Children Board and Gwent wide Adult Safeguarding Board. This group is made up of multi-agency representation from within Blaenau Gwent who monitors and reviews the safeguarding information and performance. This group has direct links with the Youth Forum to ensure the voice of the child is fully considered and heard on safeguarding issues.

Background Documents /Electronic Links

- *Append 1 – BG Safeguarding Reporting Template 2019-2020 (Q1, Q2, Q3 and Q4)*

Social Services
1st April 2019 to
31st March 2020

Safeguarding Performance Report

Cyngor Bwrdeistref Sirol
Blaenau Gwent
County Borough Council

00 Table of Contents

00 Foreword

Purpose of the report

The purpose of this report is to provide safeguarding information that is recorded by Social Services and Education.

Monitoring and reporting systems are well-developed to ensure the department is able to track information and evidences that the safeguarding agenda remains a priority for the local authority.

Performance information is collated from Social Services and Education information systems which identifies activity, demands and trends of data. This includes a number of items that are statutory requirements as part of the Welsh Government Performance Framework.

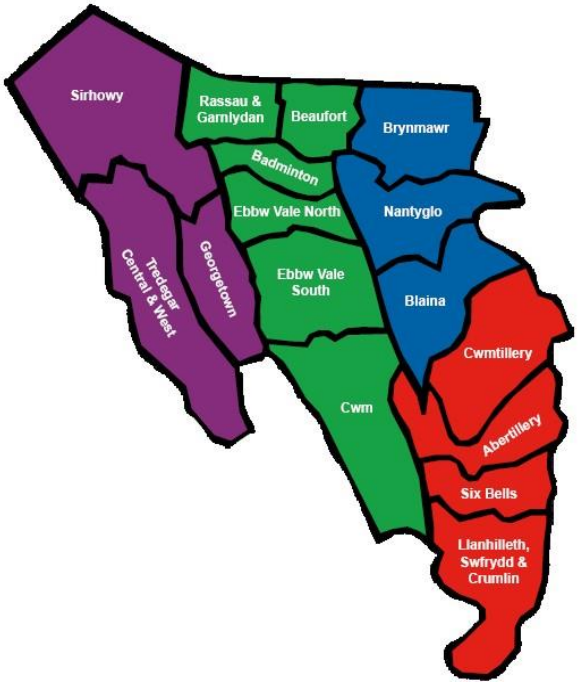
The report includes information on the following:

- Referrals received and their outcomes
- Children who are being safeguarded and analysis
- Quality assurance arrangements with education settings
- Broader issues within education that impact upon safeguarding

This report will be shared with Senior Management Teams within Social Services and Education and presented to the Safeguarding Scrutiny Committee for Social Services, Education and Active Living.

00 Community Profile - Demographics

Community Profile



- 47% of Blaenau Gwent's local areas are amongst the top 20% deprived areas in Wales. (Welsh Index of Multiple Deprivation 2014)

- The proportion of benefit claimants amongst people of working age was higher in Blaenau Gwent than the proportion across the comparable authorities (working-age client group – key benefit claimants August 2014 - 23.2% in Blaenau Gwent compared to all Wales level of 16.4%)

- The total rate of Blaenau Gwent's recorded offence levels was higher than comparative areas. For the year ending December 2014 Police recorded crimes - 76.89 crimes per thousand population in Blaenau Gwent compared to its most similar group of areas average (as defined by the Home Office) of 69.03 per thousand population.

- Total Population: 69,713 Number of 0 – 17 year olds: **13,607** (2018 Population Estimates)

- Number of Open cases to Children's Social Services as at 30th June 2019: **971**

- Number of pupils attending primary schools: **5,849**

- Number of pupils attending secondary schools: **2,962**

01 Referrals to Social Services

Fig: 1.1 Number of referrals received by Social Services

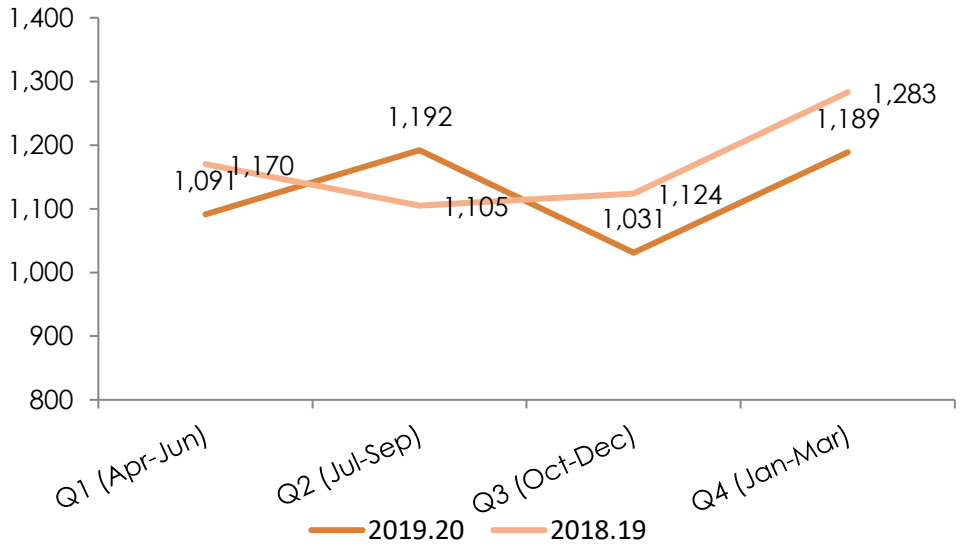


Fig: 1.2 Number and Percentage of Referrals by Source (19.20)

	Q1	Q2	Q3	Q4	Annual	%
Police	334	399	308	393	1,434	32%
Education	196	154	194	227	771	17%
Other Agency	107	141	103	137	488	11%
Health	154	170	177	125	626	14%
Social Services	114	146	108	125	493	11%
Individuals	138	125	75	138	476	11%
Housing	18	8	3	12	41	1%
Other LA	11	36	29	14	90	2%
Youth Service	18	10	18	7	53	1%
Other Departments	1	2	13	8	24	1%
YOS	0	1	3	3	7	0%
Total	1,091	1,192	1,031	1,189	4,503	100%

01 Referrals to Social Services

Graph showing the source of referrals and the percentage

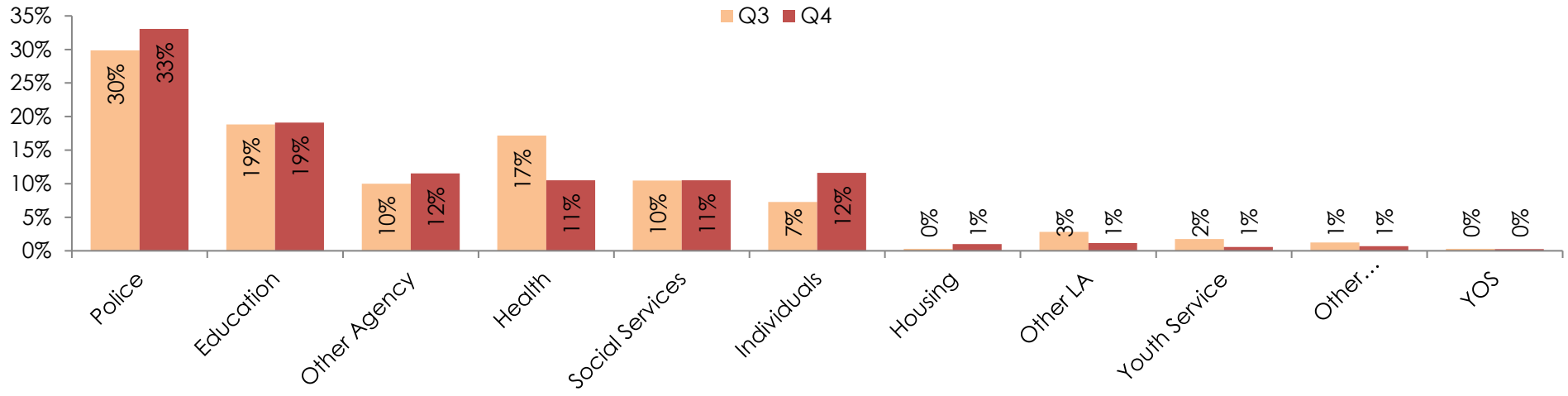


Fig: 1.3 Multi-agency referral forms (MARF's) received on open cases

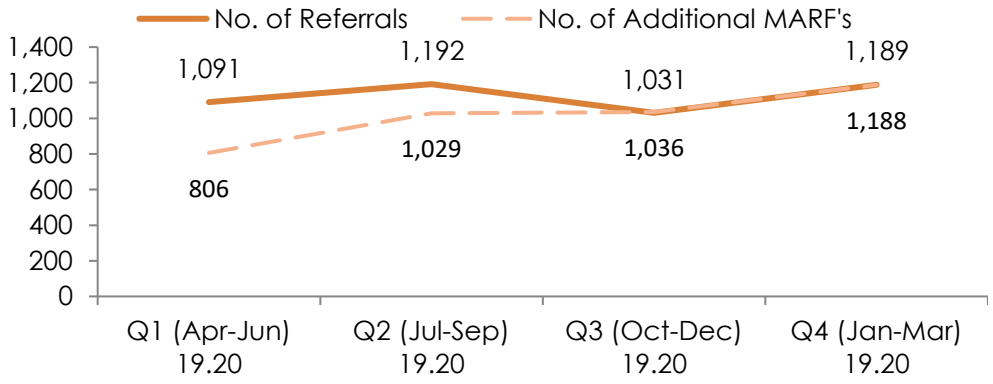
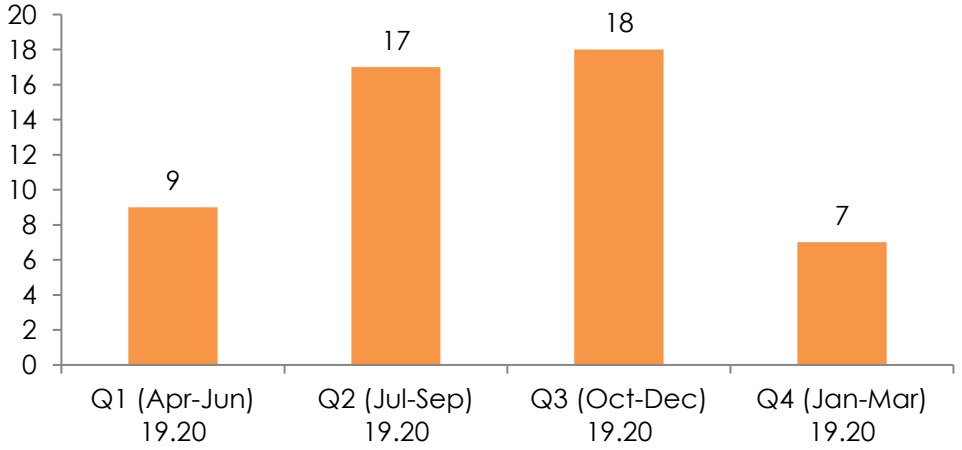


Fig: 1.4 Referrals received from Youth Services



02 Child Protection Register

Fig 2.1 Children on the Child Protection Register

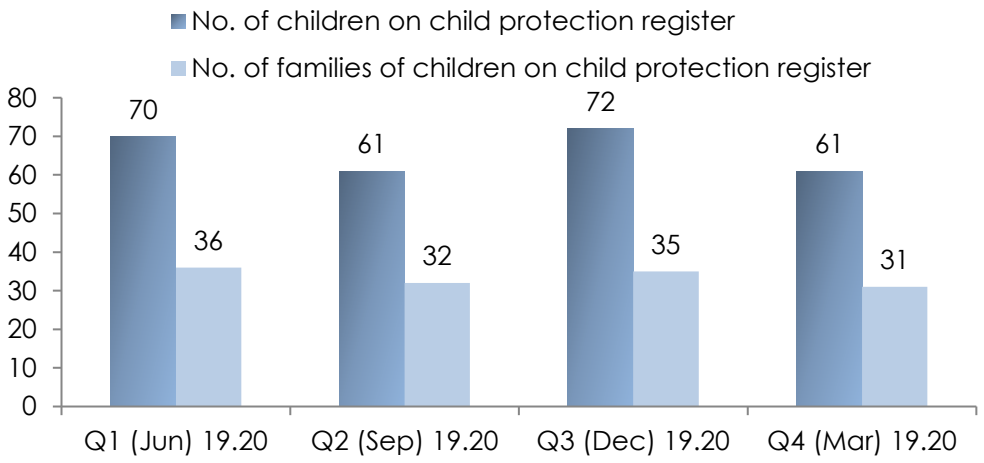


Fig 2.2 Child Protection Register Summary

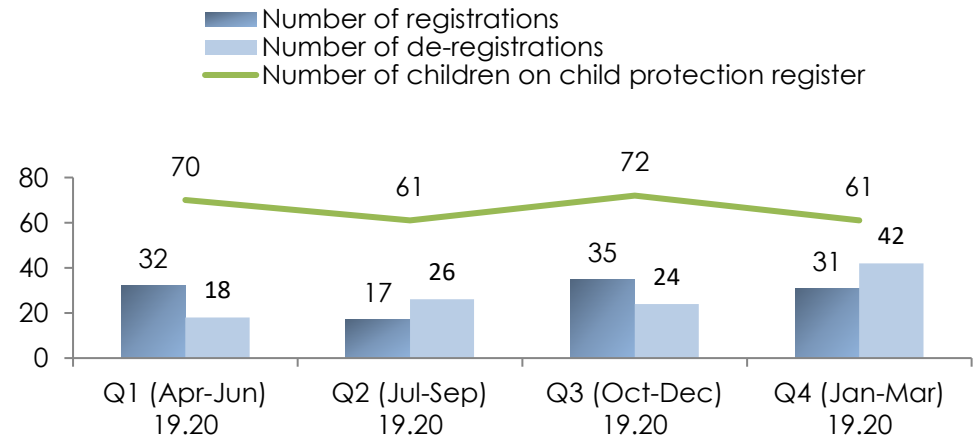


Fig 2.3 Categories of abuse

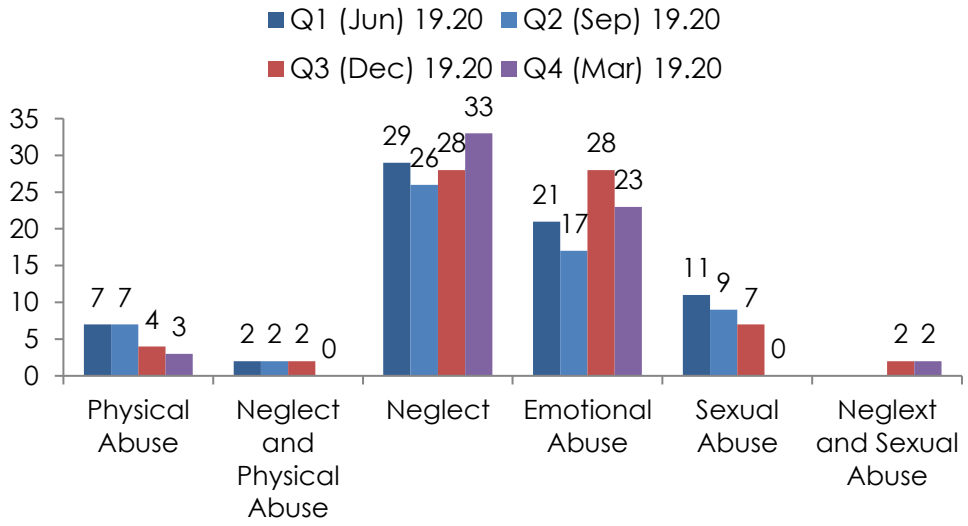


Fig 2.4 Age Breakdown of children on child protection register

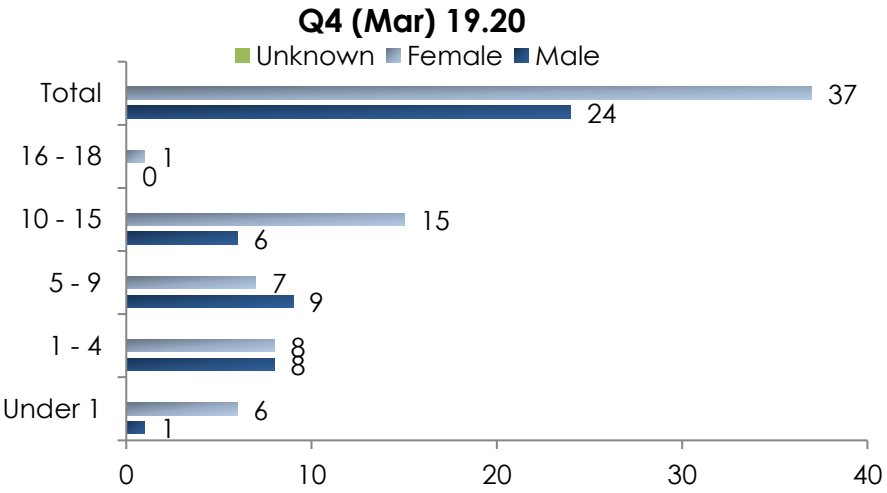


Fig 2.5 Average length of time on register

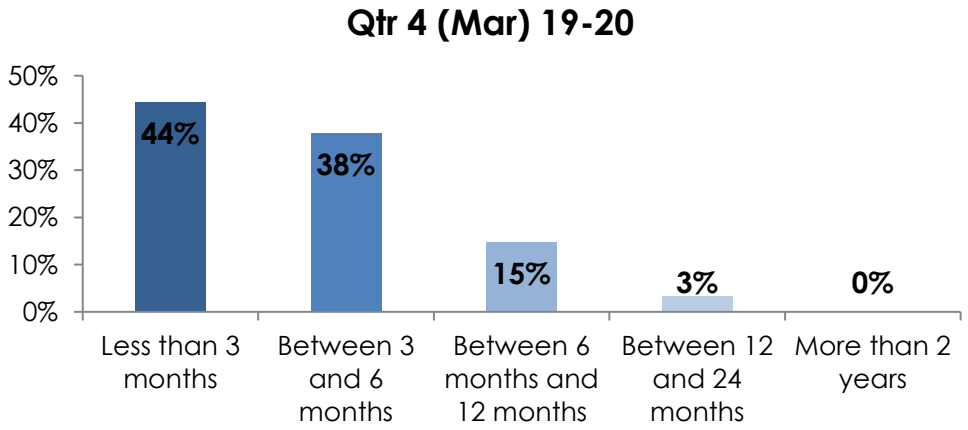


Table showing the breakdown of children on the child protection register over the last 12 months

	Q1 (Jun) 19.20	Q2 (Sep) 19.20	Q3 (Dec) 19.20	Q4 (Mar) 19.20
Less than 3 months	31	13	31	27
Between 3 and 6 months	8	26	10	23
Between 6 months and 12 months	27	15	24	9
Between 12 and 24 months	3	6	6	2
More than 2 years	1	1	0	0
	70	**61**	**71**	**61**

Fig 2.6: Child Protection Conferences

	Q1 (Jun) 19.20		Q2 (Sep) 19.20		Q3 (Dec) 19.20		Q4 (Mar) 19.20	
	No.	%	No.	%	No.	%	No.	%
Conferences Held								
Initial Conferences	30	*45%*	14	*20%*	39	*48%*	25	*27%*
No. of Families	16		8		17		15	
Review Conferences	36	*55%*	56	*80%*	43	*52%*	66	*73%*
No. of Families	23		28		24		33	
Initial Child Protection Conferences	**30**		**14**		**39**		**25**	
Outcome:								
Registered	26	*87%*	14	*100%*	32	*82%*	22	*88%*
Registered at birth	1	*3%*	0	*0%*	0	*0%*	2	*8%*
Not registered	3	*10%*	0	*0%*	7	*18%*	1	*4%*
Review Child Protection Conferences	**36**		**56**		**43**		**66**	
Outcome:								
Continue with registration	19	*53%*	32	*57%*	19	*44%*	26	*39%*
Cease registration	17	*47%*	24	*43%*	24	*56%*	40	*61%*

02 Child Protection Register

Fig 2.7 Initial Child Protection Conferences

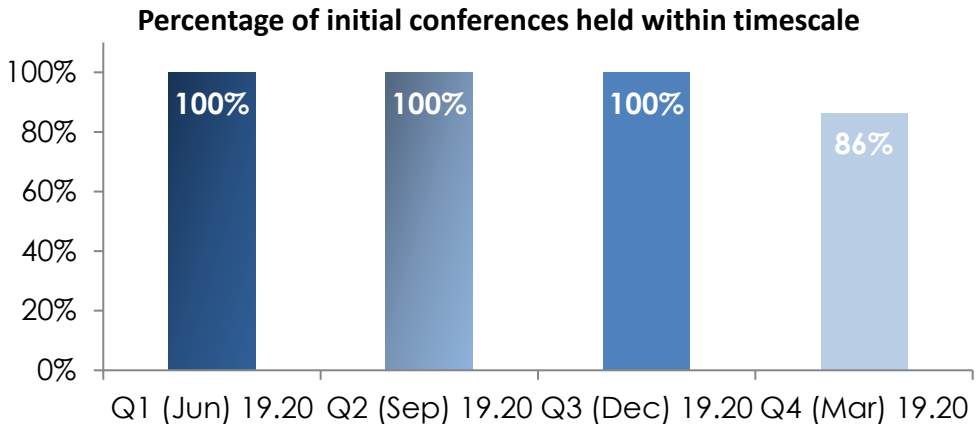
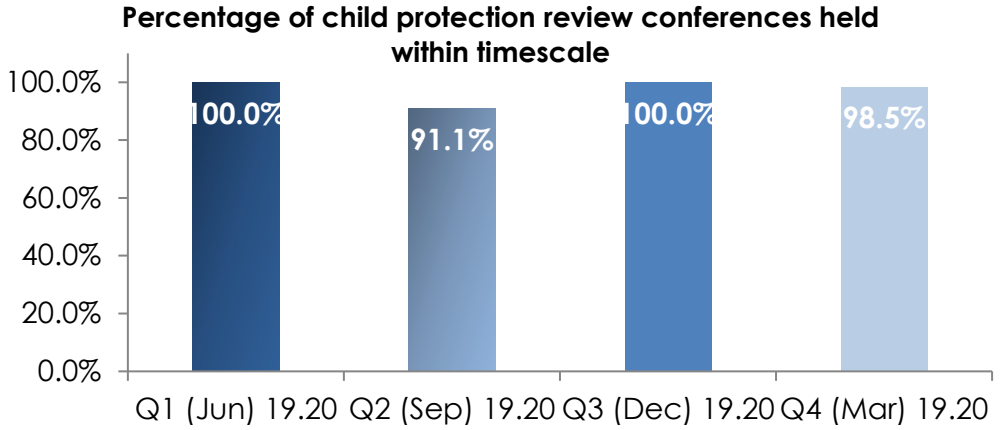


Fig: 2.8 Child Protection Review Conferences



	Q1 (Jun) 19.20	Q2 (Sep) 19.20	Q3 (Dec) 19.20	Q4 (Mar) 19.20	Annual 19.20
Number of initial conferences held	28	14	39	22	103
Number of initial conferences held within 15 working days of the strategy discussion	28	14	39	19	100
Percentage of initial conferences held within timescale	100%	100%	100%	86%	97%

	Q1 (Jun) 19.20	Q2 (Sep) 19.20	Q3 (Dec) 19.20	Q4 (Mar) 19.20	Annual 19.20
Number of Review Child Protection Conferences held	36	56	43	66	201
Number of Review Child Protection Conferences held within timescale	36	51	43	65	195
Percentage of Review Child Protection Conferences held within timescale	100.0%	91.1%	100.0%	98.5%	97%

Executive Committee and Council only

Date signed off by the Monitoring Officer: N/A

Date signed off by the Section 151 Officer: N/A

Committee:	**Joint Education and Learning and Social Services (Safeguarding) Scrutiny Committee**
Date of meeting:	**8th October 2020**
Report Subject:	**Adult Safeguarding Report 1st April 2019 to 31st March 2020**
Portfolio Holder:	**Cllr John Mason, Executive Member Social Services**
Report Submitted by:	**Damien McCann, Director of Social Services**

Directorate Management Team	Corporate Leadership Team	Portfolio Holder / Chair	Audit Committee	Democratic Services Committee	Scrutiny Committee	Executive Committee	Council	Other (please state)
x	x	23.09.20			08.10.20	Info Item 14.10.20		

1. Purpose of the Report

1.1 The purpose of this report is to provide Scrutiny Members with Safeguarding Performance information relating to Adult Services from 1st January 2020 to the 31st March 2020 for the 4th quarter of the financial year and also the information of the financial year 1st April 2019 to 31st March 2020. The information provided will enable Members to identify Safeguarding areas within the Authority which require further development to improve Safeguarding practice and procedures for Adult Services.

2. Scope and Background

2.1 In April 2016 The Gwent-wide Adult Safeguarding Board (GWASB) became a statutory Board as set out in Part 7 of the Social Services and Well Being (Wales) Act 2014. The Board's purpose is twofold; to protect adults in Gwent becoming "adults at risk" and to protect adults who have been abused or neglected or are at risk of abuse or neglect. They are supported in their work by a number of sub groups that manage core business and other more specific pieces of work which deliver on the strategic priorities set by the Board each year.

3. Options for Recommendation

3.1 The report has been considered and agreed by the Social Services Leadership team and the Corporate Leadership Team. There were no recommendations identified from the previous report presented to Members.

3.2 **Option 1**

Members are asked to consider the detail contained in the Adult Safeguarding Report and contribute to the continuous assessment of effectiveness by making appropriate recommendations for amendment to the report before consideration at Executive Committee.

Option 2
Accept the report as provided.

4. **Evidence of how does this topic supports the achievement of the Corporate Plan / Statutory Responsibilities / Blaenau Gwent Well-being Plan**

4.1 The Social Services and Well-being (Wales) Act 2014 places a statutory duty on all local authorities to produce an annual report on the discharge of its social services functions.

4.2 The Council's Corporate Plan sets out the Council's priorities for 2018-2022- This will help support the Corporate plan by implementing effective safeguarding arrangements to prevent adults becoming at risk by identifying and promoting preventative work.

5. **Implications Against Each Option**

Risk including Mitigating Actions

The Directorate Risk Register identifies safeguarding as high risk and is therefore monitored as part of the quarterly report of the Director of Social Services via the business planning process for each option. The Directorate Risk Register includes what actions have been taken to mitigate these risks and is reviewed on a regular basis.

5.1 ***Impact on Budget***

Confirmation has been received from Welsh Government and the RPB that the Integrated Care Funding (ICF) has been approved for a further 12 months from the 1st April 2021 and it is hopeful this will continue to fund the support worker post put in place.

5.2 ***Legal***

The Social Services and Well-being (Wales) Act came into force on 6 April 2016. The Act provides the legal framework for improving the well-being of people who need care and support, and carers who need support, and for transforming social services in Wales.

5.3 ***Human Resources***

There are no human resources implications attached to this report.

6. **Supporting Evidence**

6.1 ***Performance Information and Data***

Performance and data is provided within the report.

6.2 The number of reports received of an 'adult suspected of being at risk' during the given period was 136. The total number of referrals for 2019/2020 was 540. This is a significant increase on the referrals from 2018/19 where there were 491. This could be related to a particular home where the medication process was changed to an electronic system and there were some difficulties within the system and the staff using it which resulted in a number of referrals for that care home. This was addressed accordingly and is described in more detail in point 6.4

Number of reports of an adult suspected of being at risk received during the fourth quarter of 2019/2020 1st January to 31st March 2020	136
Number of reports of an adult suspected of being at risk received during 2019/2020 1st April 2019 – 31st March 2020	540

6.3 The number of referrals received within the different categories of abuse or neglect are shown below. It should be noted that concerns about more than one type of abuse can be reported within the same referral. As in previous years the most referrals are received for females over the age of 65. This is a national trend. The category of abuse most reported is one of neglect and the least reported is sexual which has been the situation for last three years.

Category of Abuse	Gender	Age 18-64 01/01/20 – 31/03/20	Age – 65 and over 01/01/20 – 31/03/20	Age 18-64 01/04/19 – 31/03/20	Age – 65 and over 01/04/19 – 31/03/20
Physical	Male	9	5	30	22
	Female	13	13	47	61
	Transgender	1	0	0	0
Sexual	Male	0	0	2	2
	Female	4	3	16	5
Emotional /Psychological	Male	7	3	20	21
	Female	10	13	39	41
	Transgender	1	0	0	0
Financial	Male	7	5	29	13
	Female	8	7	24	33
Neglect	Male	5	17	32	68
	Female	6	29	35	115
	Transgender	1	0	0	0
Total	**Male**	**18**	**28**	**89**	**109**
	Female	**31**	**59**	**115**	**226**
	Transgender	**0**	**0**	**1**	**0**
	Total	**49**	**87**	**205**	**335**

6.4 Referrals of domestic abuse are captured as part of the data return for the Welsh Government.

		Age 18-64 01/01/20 – 31/03/20	Age – 65 and over 01/01/20 – 31/03/20	Age 18-64 01/04/19 – 31/03/20	Age – 65 and over 01/04/19 – 31/03/20
Domestic	Male	3	2	7	6
	Female	11	4	37	23

6.4.1

Each of the five local authorities have different structures in place to respond to concerns about domestic violence, however GWASB partner agencies are represented on local and regional domestic abuse forums. There are strong links between practitioners in safeguarding and domestic abuse fields of practice and domestic abuse training is available and is well attended by all agencies across Gwent in a variety of formats. As discussed in previous years Blaenau Gwent have secured a seconded post, funded through ICF, from Cyfannol and the support worker is based within safeguarding and IAA.

6.4.2

The place where the alleged abuse occurred can be seen in the table below. The majority of referrals were split between the alleged abuse taking place in the persons own home The alleged perpetrators in these cases could be paid carers going into the home or friends and family or within a care setting including a health environment - this could be residential, nursing or respite care and again the alleged perpetrators could be paid carers, family and/or other service users.

Place alleged abuse or neglect occurred	**Total** 01/01/20 – 31/03/20	**Total** 01/04/19 – 31/03/20
Own Home	64	242
Community	7	38
Care Home Setting	54	222
Health Setting	5	14
Other	**6**	**24**
Total	**136**	**540**

6.4.3

Safeguarding is an important part of the commissioning function and requires a substantial resource commitment from the Commissioning Team who provide crucial information in respect of commissioned services and providers which contributes to informed decision making in relation to safeguarding cases. A member of the Commissioning Team attends every strategy meeting held for commissioned services to offer advice, guidance and perspective. The Contracts and Commissioning Team Manager and the three Contract Monitoring Officers are all fully trained non-criminal investigators and undertake investigations independently or jointly with colleagues depending on the complexity and size of the investigation, or, with health colleagues if there are nursing issues involved. Whether referrals progress to strategy meetings and/or investigation, or are closed down as inappropriate

safeguarding referrals, there is very often some preliminary investigation work and/or recommendations / performance issues with providers to be acted upon and followed up by the Commissioning Team. During the 2nd quarter we received a high volume of Care home referrals (79 in total) with one nursing home submitting 31 in relation to system errors in the ordering and recording of medication for residents. As a result of this a systems audit was undertaken by health which led to improvements being implemented by the Care home around their current operating and IT systems. Following a joint investigation of the 31 referrals received there was no significant harm to the residents and they had all received their correct medication.

6.4.4

The persons alleged responsible for the abuse are broken down in the table below. Paid employees being alleged perpetrators for 30 in quarter 4 and a total of 172 in the year. 47 being a relative or friend in quarter 4 and a total of 154 in the year. The previous year showed similar figures with 171 referrals where the alleged perpetrator was a paid employee and 128 family/friend. To progress the referral consent is needed from the alleged victim, but that consent can be overridden when a paid employee is the alleged perpetrator. In the domestic abuse cases a high proportion of alleged victims do not consent to the referral progressing through safeguarding. These referrals are submitted to the Police for further action.

Person alleged responsible	**Total** 01/01/20 – 31/03/20	**Total** 01/04/19 – 31/03/20
Paid Employee	30	172
Relative / Friend	47	154
Volunteer / Unpaid employee	0	1
Other service user	16	50
Other	1	8
Unknown – no specific individual identified on the duty to report due to the nature of the service settings i.e. unwitnessed fall by a service user	42	155
Total	**136**	**540**

6.5 The referrals received are from a variety of sources, as listed in the table below. The majority of the referrals were submitted from provider agencies. This is a trend every year.

Source of Referral	Total 01/01/20 – 31/03/20	Total 01/04/19 – 31/03/20
Self-reported	0	0
Relative / friend	0	2
Local authority	32	130
Police	3	11
Local health board	10	60
Independent hospital	0	0
Ambulance service	3	10
Care regulator	0	1
Provider agency	69	260
Probation	0	1
Third sector	15	46
Advocate	0	0
Other	4	19
Total	**136**	**540**

6.6 **Updates on the achievements and progress on the strategic development plans during 2019/2020 and beyond:**

- The All Wales New Safeguarding procedures were launched in November 2019
- Development of training resources and to revise the current documentation to support implementation of the new Safeguarding Procedures has commenced and an Independent Provider has been commissioned to deliver training in the New Year.
- In response to the follow up review of the corporate arrangements for safeguarding by Wales Audit Office (WAO) which was presented to Corporate Overview Scrutiny Committee on the 12th February 2020 a working group has been set up and an action plan developed to address the recommendations required.

Response to the Pandemic

- Gwent Safeguarding Board has produced a strategic response to ensure that safeguarding remains everybody's business whilst our partner agencies, citizens and services cope with the Covid-19 pandemic.
- Gwent Safeguarding Board continue to support partner agencies and practitioners, at this time, as they perform their safeguarding duties to ensure that the safeguarding of children, young people and adults at risk remains at the forefront of our work.
- Safeguarding has been critical through the pandemic with all safeguarding staff in Adults working from home to maintain an essential service.
- The new policy was implemented from April 6th 2020, however, due to the difficulties in these unprecedented times face to face training was put on hold until further notice, safeguarding training via eLearning is still available.

- There was no drop in referrals due to the pandemic and we haven't seen any increase in domestic abuse referrals through safeguarding.

6.7 ***Expected outcome for the public***
Quarterly reporting provides the public with the opportunity to view progress of the Directorate and ensure accountability.

6.8 ***Involvement (consultation, engagement, participation)***
The Social Services and Well-being (Wales) Act 2014 looks to build and strengthen on existing arrangements by involving service users, carers and other key partners where possible in helping shape and influence future design of services.

6.9 ***Thinking for the Long term (forward planning)***
The Gwent wide Adult Safeguarding Board has developed a new partnership agreement between local authorities and agency partners including Gwent Police, Aneurin Bevan University Health Board, Wales Probation Trust, Gwent Association of Voluntary Organisations which sets out a clear and shared vision to ensure all adults in Gwent are safeguarded effectively through partnership working and community engagement.

6.10 ***Preventative focus***
Providing this report and the level of detailed safeguarding information to the Joint Safeguarding Committee enables Members to ensure risks are identified and acted on.

6.11 ***Collaboration / partnership working***
It is a very important that GwASB does not work in isolation and having strong working relationships with the South East Wales Safeguarding Children's Board (SEWSCB) and the Domestic Violence Board will be essential.

6.12 ***Integration (across service areas)***
The development of the Corporate Safeguarding Policy and the Departmental safeguarding leads meetings helps ensure all departments within the Authority are aware of their responsibilities for safeguarding and are kept updated with any issues trends within safeguarding.

6.13 ***EqIA (screening and identifying if full impact assessment is needed)***
Not applicable.

7. **Monitoring Arrangements**

7.1 The performance of the department is monitored throughout the financial year from April to March and reported to the Social Services Scrutiny Committee.

Background Documents /Electronic Links

The following hyperlink provides further details on the governance and structure arrangements: www.gwentsafeguarding.org.uk

This page is intentionally left blank