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

13th March, 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 Council Chamber, Civic Centre, Ebbw Vale on Monday, 23rd March, 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) 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 action sheet.

6. SAFEGUARDING PERFORMANCE INFORMATION FOR SOCIAL SERVICES AND EDUCATION - 1ST JULY TO 31ST DECEMBER 2019 15 - 40

To consider the report of the Service Manager, Children's Services and the Strategic Education Improvement Manager.

7. ADULT SAFEGUARDING REPORT 1ST JULY TO 31ST DECEMBER 2019 41 - 48

To consider the report of the Head of Adult Services.

8. 360 DEGREE SAFE CYMRU ONLINE SAFETY POLICY FOR SCHOOLS 49 - 132

To consider the report of the Corporate Director Education.

9. EDUCATIONAL NEGLECT POLICY 133 - 152

To consider the report of the Corporate Director Education.

To: Councillor S. Thomas (Chair)
Councillor D. Bevan
Councillor M. Cook
Councillor G. A. Davies
Councillor M. Day
Councillor P. Edwards
Councillor L. Elias
Councillor K. Hayden
Councillor W. Hodgins
Councillor J. Holt
Councillor C. Meredith
Councillor J. Millard
Councillor M. Moore
Councillor J. C. Morgan
Councillor J. P. Morgan
Councillor G. Paulsen
Councillor K. Pritchard
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 Social Services & Education and Learning (Safeguarding) Scrutiny Committee**
Date of meeting:	**23rd March 2020**
Report Subject:	**Safeguarding Performance Information for Social Services and Education – 1st July to 31st December 2019**
Portfolio Holder:	**Cllr John Mason, Executive Member Social Services; and Cllr Joanne Collins, Executive Member Education**
Report Submitted by:	**Alison Ramshaw, Service Manager, Children's Services; and Michelle Jones, Strategic Education Improvement 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)**
20.02.20	06.03.20	09.03.20			23.03.20	22.04.20		

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 and Education from 1st July 2019 to the 31st December 2019. 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.

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 July 2019 – 31st December 2019, and Education information from 1st July – 31st December 2019

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 after each school term.

2.3 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 action plan developed to address the recommendations required. A further update will be provided at the next meeting

3. **Options for Recommendation**

3.1 Having scrutinised the information members can

Option1
Accept the approach and information detailed in the report provided.

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**

The Safeguarding agenda is considered as part of the Council's Corporate Strategies that includes:

- Corporate Plan
- Single Integrated Plan
- Corporate Risk Register
- Safe Reduction of CLA Strategy
- Early Intervention and Prevention Strategy

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)***

Quarters 2 & 3 have seen the number of children on the child protection register vary from 61 in Quarter 2 and 71 in Quarter 3. The numbers of children looked after has remained stable and the numbers of court applications continues to be stable which is having a positive impact on the budget

The safeguarding team is experiencing some staffing challenges with a full time Independent Reviewing Officer on long term sick leave. This has resulted in the service needing to source support from the independent sector which will come at a cost. The full extent of this cost implication will be known and reported on in Quarter 4's report.

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)**

6.2 ***Social Services***

6.2.1 **Referrals to Social Services**

Figure 1:1 Shows the number of referrals made to Social Services. The chart demonstrates a slight increase in referrals during Quarter 2 (*1,192*) with a slight dip then in Quarter 3 (*1,031*). The drop in referrals may be an indication that the work currently being undertaken with partner agencies regarding thresholds /assessments of risk and the availability of preventative services is having a positive impact on Children's Services.

.

Figure 1.2: Shows the source of the referrals as previous quarters, police remain the highest referring agency (33.5% in Quarter 2 & 29.9% in Quarter 3) followed by Health (14.3%) and then closely followed by Education (11.8%)

Figure 1.3: shows the numbers of referrals received into the department on open cases. During Quarter 2 the number increased to 1,029 from 806 in Quarter 1 this number increased again slightly in Quarter 3 to 1.036.

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 both quarters. Further analysis evidenced that of these numbers a high percentage of children were being managed under the exploitation risk management processes. 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.

6.2.2 **Youth Services**

Figure 1.4: Shows the numbers of youth service referrals during Quarters 2 and 3. The figure shows that a continued rise in referrals from 17 in Quarter 2 to 18 in Quarter 3.

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.

6.2.3 **Child Protection**

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 Quarter 2 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 Quarter 2.

Quarter 3 saw a slight rise in registrations with 71 children on the child protection register to 35 families, which was an increase of 10 from the previous quarter. 34 children were placed on the register during Quarter 3. The numbers indicate an overall trend as the numbers in previous quarters demonstrates similar numbers (see below):

- 56 in Quarter 4 (2018/19)
- 70 in Quarter 1 (2019/20)
- 61 in Quarter 2 (2019/20)
- 71 in Quarter 3 (2019/20)

Figure 2.5: shows the average time a child is on the Child Protection Register. The Social Services Senior Management Team review all those children on the Child Protection Register for 12 months or longer to ensure there is no unnecessary drift. It is pleasing to see that over the last 2 quarters these numbers continue to reduce.

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 decreased during Quarter 2 to 14 children to 8 families. All 14 children subject to a child protection case conference were registered.

56 review conferences were held in Quarter 2, 32 children continued registration with 24 children who ceased to be registered.

The numbers of initial conferences held in Quarter 3 increased to 39 children to 17 families. Of the 39 children subject to child protection case conference 32 were registered.

43 review conferences were held in Quarter 3, 19 children continued registration with 24 who ceased to be registered.

Figure 2.7: shows the number of initial conferences held within timescales. There has been consistence practice in this area throughout the 2 reporting period, with 100% of conferences held within timescales.

Figure 2.8: relates to review conferences and the graph shows 100% performance which is excellent.

6.3 Education Information

6.3.1 Overview

Blaenau Gwent Council and Education Directorate is committed to ensuring that Safeguarding in Education processes are robust, fit for purpose and are being consistently applied. Through this report Scrutiny Members are provided with greater clarity on the extensive work that is undertaken in ensuring that safeguarding arrangements give no cause for concern and fulfil the requirements as set out in the Estyn framework for Local Government Education Services (LGES).

6.3.2 Bullying Incidents and Restrictive Physical Interventions (RPI)

There have been processes developed between Education and the Youth Offending Service to tackle anti-social behaviour in schools and a draft policy is in the process of being adopted to look at parenting contracts with parents. This is on the Forward Work Programme of the Education and Learning Scrutiny Committee. In addition, the current RPI policy is under review and will be finalised in the summer term.

6.3.3 Numbers of restrictive physical interventions

Systems are in place within the Local Authority to gather incidents when Restrictive Physical Interventions *(Figure 4.1)* are used in school to manage pupils' behaviour. Following each incident, the school is required to record the incident in a Bound and Numbered book and complete an incident form. The incident form is sent to the Local Authority Education Directorate where it is recorded on a central recording system.

The number of RPIs in the Autumn term was 55. This is a decrease from the same period last year.

The 55 interventions are for 21 different children. A small number of these children experienced more than 2 RPIs.

Regular monitoring of incident forms is undertaken by the Safeguarding in Education Manager to ensure the use of physical intervention is appropriate.

6.3.4 Numbers of bullying incidents reported which have led to exclusions

Bullying has been identified by children and young people as a significant issue they face. An anti-bullying strategy has been developed by the Education Department and work based on the new Welsh Government guidance is also in train.

In the period 1st September to – 31st December 2019 (*Figure 4.2*) there were no exclusions from schools where bullying was recorded as the primary reason for the exclusion, or indeed as an additional reason.

It should be noted that caution is needed when considering fluctuations in such small numbers and drawing trend conclusions.

6.3.5 **Quality Assurance Visits**

The Education Directorate has developed a quality assurance process across Local Government Education settings (LGES) which has been in place since September 2017.

Members will be aware through a report to this Committee that this protocol was recently reviewed and learning from visits and broader safeguarding issues has continued to inform the focus of the Safeguarding in Education Managers work.

As such, quality assurance visits to Local Government Education Settings (LGSES) include pupil and staff voice through pupil and staff discussions, scrutiny of training, policy, safe recruitment practice, and record-keeping of concerns. A “dip test of activity” is undertaken by the Safeguarding in Education Manager to test the robustness of the safeguarding systems and to ascertain a level of assurance.

Over a two-year time period, this process has been applied to Schools, Early Years settings, the Youth Service, Leisure Trust, Home to School Transport, Catering and Organisational Development and has now been extended to cover independent school settings and after school clubs.

During the Summer term 2019 an audit of safeguarding arrangements in Blaenau Gwent Breakfast clubs took place. Information for this audit was gathered through discussion, observation, questionnaires and with reference to Welsh Government statutory guidance document no 145/2014, ‘Free Breakfast in Primary Schools’. The findings of the audit confirm that all staff in Breakfast clubs receive safeguarding training and know how to report their concerns as well as other areas where learning has been identified. Therefore, a full report on this subject matter is included in the forward work programme for this Committee and will be presented to the next Committee meeting at the end of the summer term.

During the Autumn Term, 100% (6) of the possible quality assurance visits have taken place. This has included maintained schools, independent special schools and early years. There have been no significant safeguarding issues identified during these visits which have provided reassurance that appropriate safeguarding arrangements are in place in schools and other education services.

6.3.6 **Estyn Judgements**

Scrutiny members will be aware of the Estyn framework for schools which changed in 2017 and that Inspection area 4 covers the safeguarding element. In arriving at a judgement for this Inspection area within 4.3 Inspectors will

consider whether the schools safeguarding arrangements are effective and give no cause for concerns. In coming to a judgment Inspectors will consider a multitude of evidence such as:

- whether the schools safeguarding arrangements protect all children;
- the arrangements for the safe recruitment of staff and volunteers;
- how well the school promotes safe practices and a culture of safety;
- whether the school complies with statutory guidance in discharging its safeguarding functions;
- the arrangements of the management of bullying, harassment and discrimination reporting of physical interventions;
- how well the school keeps pupils safe from radicalisation;
- arrangements for the provision of pupils educated off site; and
- the health and safety of the school buildings and site.

Figure 4.4: provides an overview of the Estyn judgements for schools inspected under the new arrangements from September 2017 up until December 2019. During the period there was 1 Estyn inspection reported.

The table evidences that care support and guidance arrangements in nearly the majority of schools (5/9) are good or better, with 4 schools receiving adequate judgements. All schools inspected during the period were assessed as having suitable arrangements for safeguarding in place that meet requirements and give no cause for concern

6.3.7 **Operation Encompass**

Figure 4.5: shows the number of domestic abuse incidents reported during the period. During the period there were 156 occurrences involving 247 children. When further analysed it is noted that the majority of the children (152 61%) affected are of primary school age.

Unfortunately, on this occasion the data regarding the number of repeat incidents on children is not available.

However, of the children affected during the period:

- 8 cases were high risk
- 56 cases were medium risk
- 183 cases were standard risk

Risk is assessed on a case by case basis by a professional against a risk tool known as the Dash checklist. The purpose of the Dash risk checklist provides a consistent and simple tool for practitioners who work with adult victims of domestic abuse in order to help them identify those who are at high risk of harm and whose cases should be referred to a MARAC meeting in order to manage their risk.

6.3.8 **Compliance Reporting**

The Police compliance target for recording the school name on the PPN is 90%. However, at the end of the current period the compliance rating remains below target at 64.8% and has also fallen from the previous period. 70.7%

During this period a member briefing session was held on this important initiative.

6.3.9 **Elected Home Educated (EHE):**

Elective home education (EHE) is when parents decide to provide home based education for their child rather than sending them to school. Home educated children are therefore not registered at mainstream or special schools.

Figure 4.6: The total number of children electively home educated as of 31st December 2019 was 77. At the same point in 2018 the number was 76.

Figure 4.7: sets out the number of secondary age pupils who have become EHE or who have returned to school from being EHE during the Spring, Summer and Autumn term. This is a decrease of 14 pupils coming out of school when compared to the data for the previous two years.

Figure 4.8: sets out the number of additional pupils who have become EHE or who have returned to school from being EHE during the Spring Summer and Autumn term. This is an increase of 2 pupils coming out of school when compared to the data for last year.

Figure 4.9: provides a breakdown by year group of EHE pupils. The numbers of pupils in KS3 is the highest which is slightly different to the pattern across Wales where KS4 is the highest.

Members should note that there are appropriate processes in place to monitor elective home education with formal visits held to check on the suitability of education. However, whilst the number of EHE pupils overall has seen a small increase the work carried out in the last academic year has ensured the rate of rise has been positively impacted.

7.1 **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.

7.2 **Involvement (consultation, engagement, participation)**

The development of the Corporate Safeguarding Policy and the Departmental Safeguarding Leads meetings which are due to be reconvened 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.

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.

The South East Wales Safeguarding Children's Board (SEWSCB) local Safeguarding Network group also reviews the safeguarding information to ensure all partner agencies are as fully aware as possible.

7.3 **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.

7.4 **Preventative focus**

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.

Providing this report and the level of detailed safeguarding information to Scrutiny Committee enables members to ensure risks are identified and acted on.

7.5 **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 Adult Safeguarding Boards.

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.

Throughout Quarters 2 and 3 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.

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.

7.6. **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.

8 **EqIA (screening and identifying if full impact assessment is needed)**
N/A

8.1 **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 (Q2 and Q3)*

Social Services
1st July 2019 to
31st December 2019

Education
2nd September 2019 to
20th December 2019

Safeguarding Performance Report

Cyngor Bwrdeistref Sirol
Blaenau Gwent
County Borough Council

00 Table of Contents

00

Foreword
Community Profile - Demographics

01 Referrals to Social Services

Number of referrals received by social services (on new and closed cases)
Percentage of referrals received by source
Additional Multi Agency Referrals (on open cases)
Referrals from Youth Services

02 Child Protection

Number of children on the Child Protection Register
Child Protection Register Summary
Categories of Abuse
Age Breakdown
Average Length of Time on Register
Child Protection Conferences
Initial Child Protection Conferences
Review Child Protection Conferences

03 Referrals to Education

Contacts by Source (Primary)
Contacts by Source (Secondary)
Contacts by Source (Other)

04 Education

RPI Incidents
Bullying Incidents leading to Exclusions
Quality Assurance
Estyn Judgements
Operation Encompass
Elected Home Education (EHE)
School Attendance
Persistently Absent
School Exclusions

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 and Education and Learning.

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

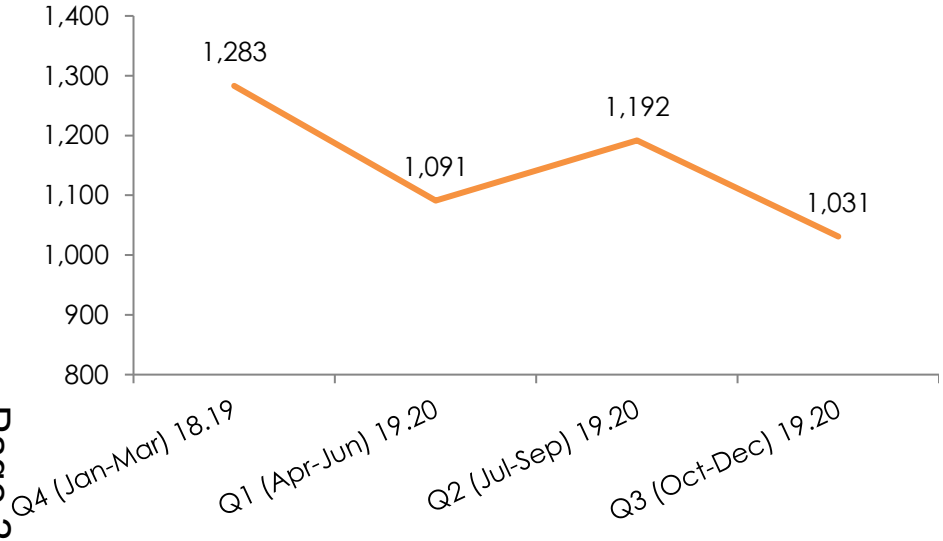


Fig: 1.2 Number and Percentage of Referrals by Source (Q2 & Q3)

	Quarter 2		Quarter 3	
	No.	**Percentage**	**No.**	**Percentage**
Police	399	33%	308	33%
Education	141	12%	181	12%
Other Agency	141	12%	103	12%
Health	170	14%	177	14%
Social Services	146	12%	108	12%
Individuals	125	10%	75	10%
Education - Post 16	2	0%	2	0%
Education - OOC	11	1%	11	1%
Housing	8	0.7%	3	0.7%
Other LA	36	3.0%	29	3.0%
Youth Service	10	0.8%	18	0.8%
Other Departments	2	0.2%	13	0.2%
YOS	1	0.1%	3	0.1%
Total	**1,192**	**100%**	**1,031**	**100%**

01 Referrals to Social Services

Graph showing the source of referrals and the percentage

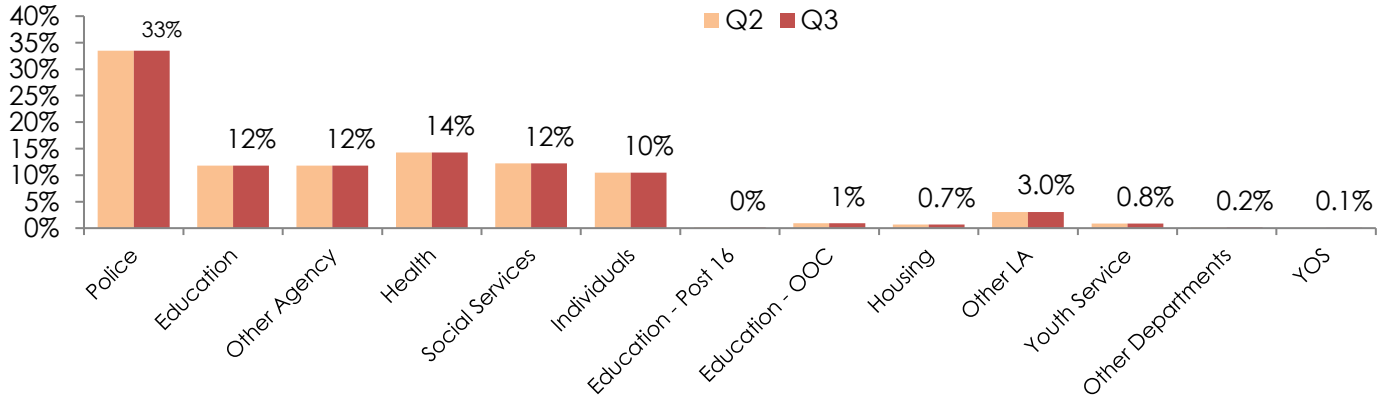


Fig: 1.3 Multi-agency referral forms (MARF's) received on open cases

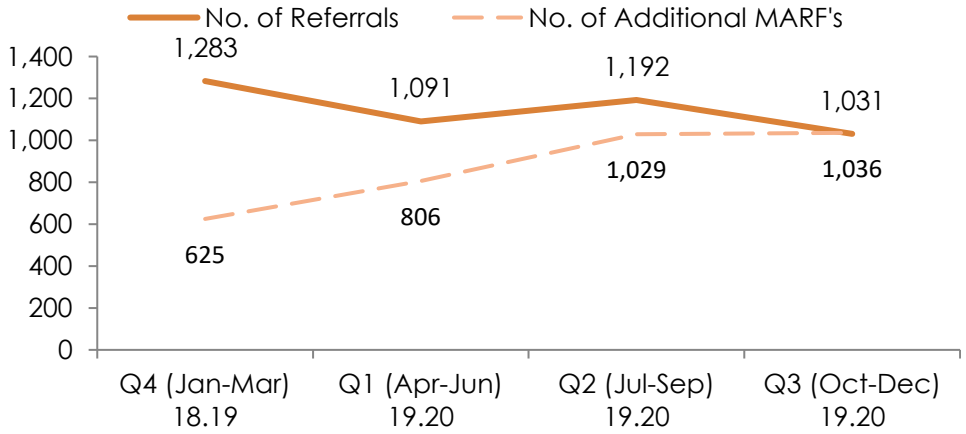
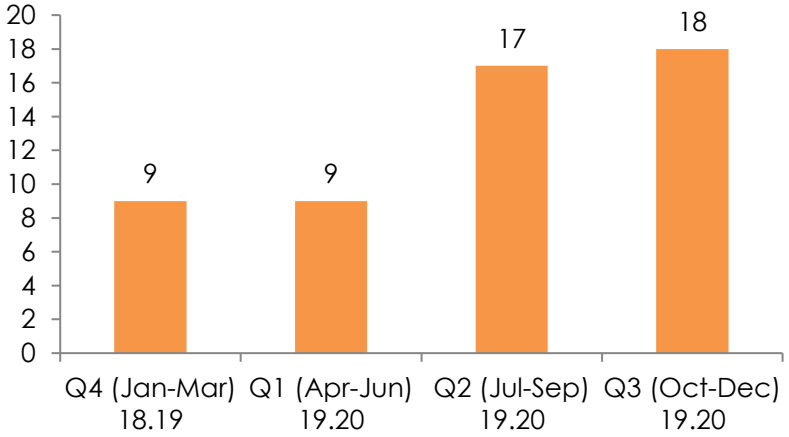


Fig: 1.4 Referrals received from Youth Services



02 Child Protection Register

Fig 2.1 Children on the Child Protection Register

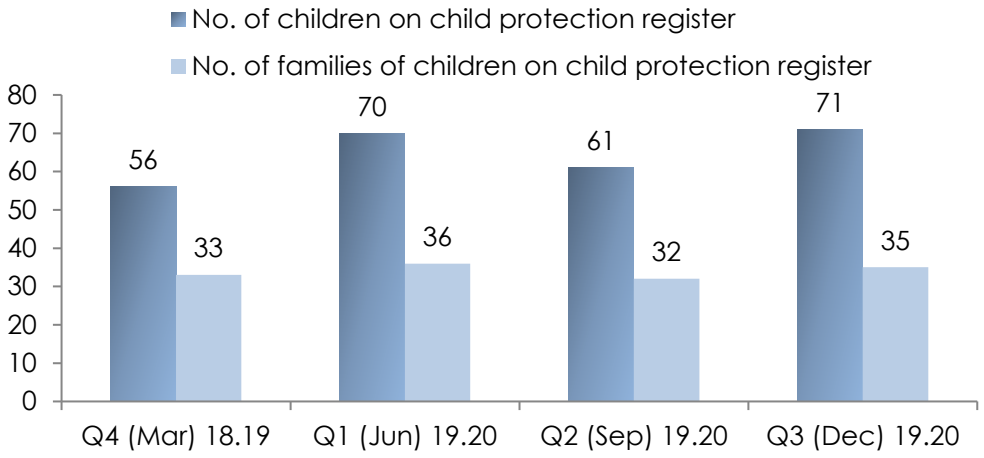


Fig 2.2 Child Protection Register Summary

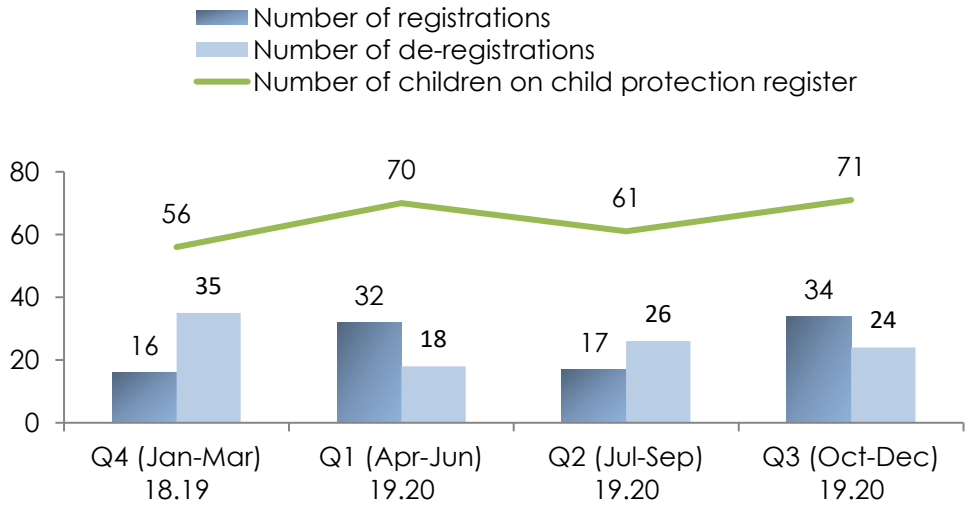


Fig 2.3 Categories of abuse

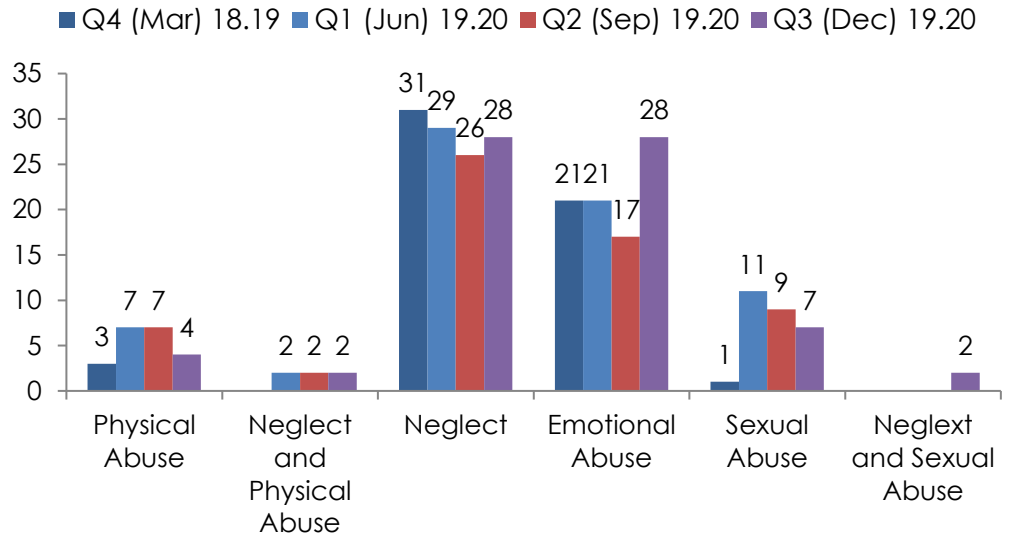


Fig 2.4 Age Breakdown of children on child protection register

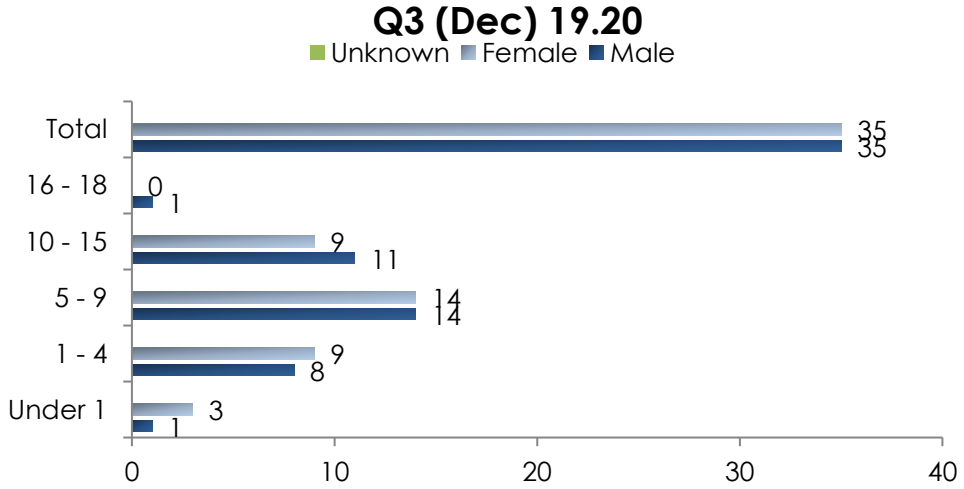


Fig 2.5 Average length of time on register

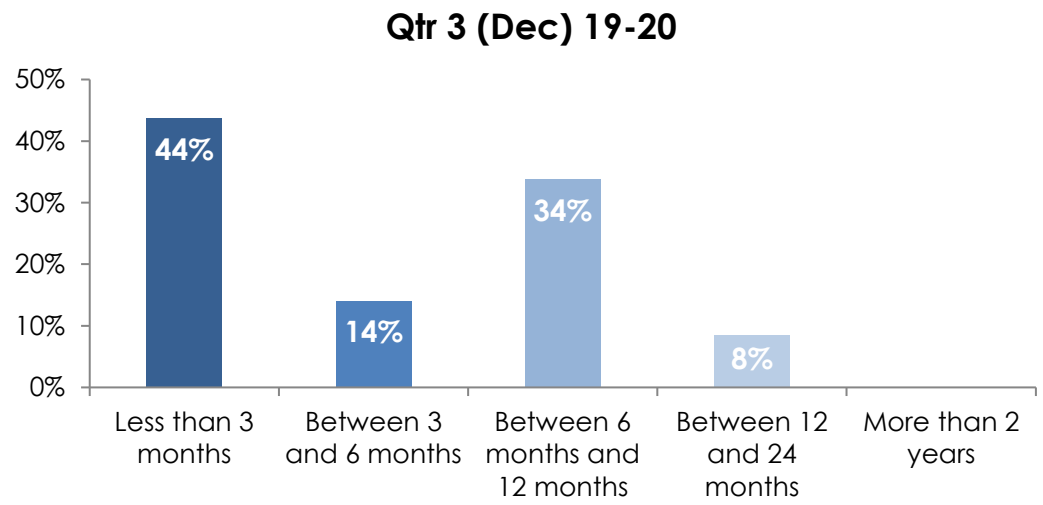


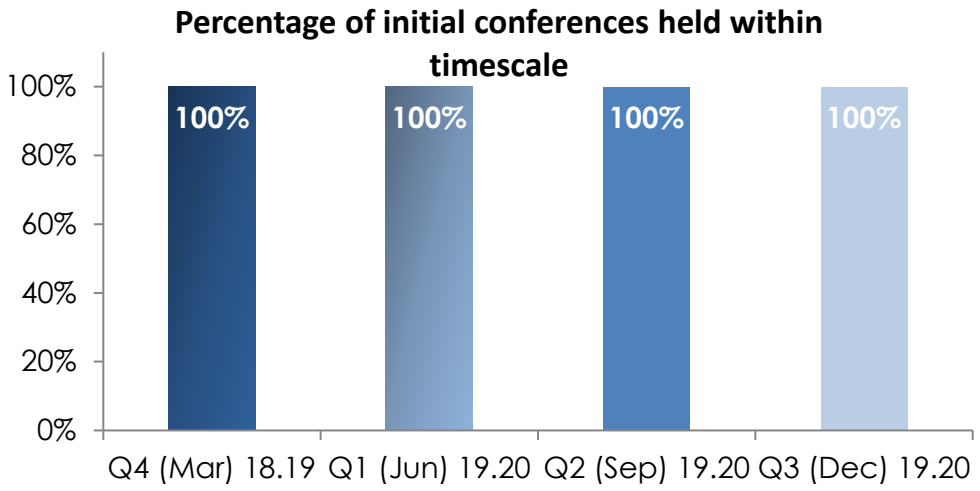
Table showing the breakdown of children on the child protection register over the last 12 months

	Q2 (Sep) 18.19	Q3 (Dec) 18.19	Q4 (Mar) 18.19	Q1 (Jun) 19.20
Less than 3 months	15	31	13	31
Between 3 and 6 months	25	8	26	10
Between 6 months and 12 months	15	27	15	24
Between 12 and 24 months	1	3	6	6
More than 2 years	0	1	1	0
	56	**70**	**61**	**71**

Fig 2.6: Child Protection Conferences

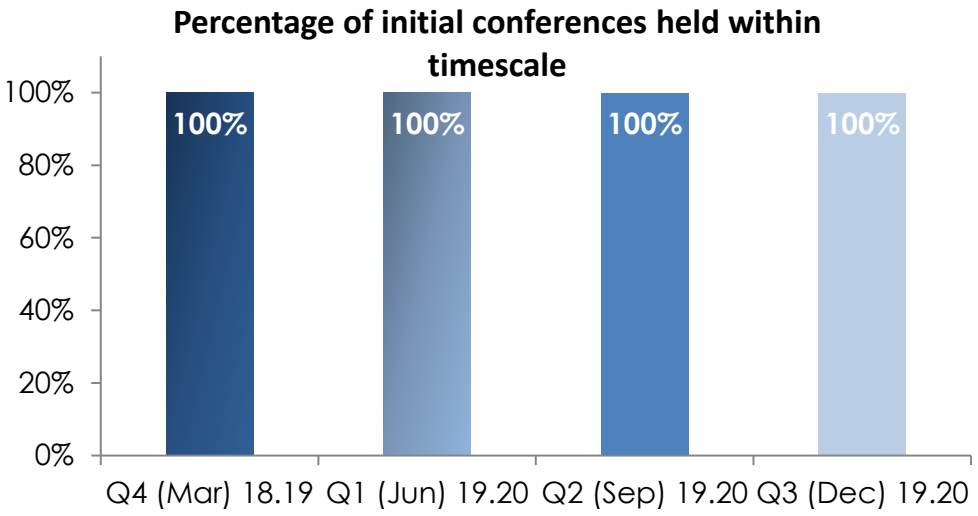
	Q4 (Mar) 18.19		Q1 (Jun) 19.20		Q2 (Sep) 19.20		Q3 (Dec) 19.20	
	No.	%	No.	%	No.	%	No.	%
Conferences Held	**83**		**66**		**70**		**82**	
Initial Conferences	20	*24%*	30	*45%*	14	*20%*	39	*48%*
No. of Families	14		16		8		17	
Review Conferences	63	*76%*	36	*55%*	56	*80%*	43	*52%*
No. of Families	38		23		28		24	
Initial Child Protection Conferences	**20**		**30**		**14**		**39**	
Outcome:								
Registered	14	*70%*	26	*87%*	14	*100%*	32	*82%*
Registered at birth	3	*15%*	1	*3%*	0	*0%*	0	*0%*
Not registered	3	*15%*	3	*10%*	0	*0%*	7	*18%*
Review Child Protection Conferences	**63**		**36**		**56**		**43**	
Outcome:								
Continue with registration	30	*48%*	19	*53%*	32	*57%*	19	*44%*
Cease registration	33	*52%*	17	*47%*	24	*43%*	24	*56%*

Fig 2.7 Initial Child Protection Conferences



	Q4 (Mar) 18.19	Q1 (Jun) 19.20	Q2 (Sep) 19.20	Q3 (Dec) 19.20
Number of initial conferences held	20	30	14	39
Number of initial conferences held within 15 working days of the strategy discussion	20	30	14	39
Percentage of initial conferences held within timescale	100%	100%	100%	100%

Fig: 2.8 Child Protection Review Conferences



	Q4 (Mar) 18.19	Q1 (Jun) 19.20	Q2 (Sep) 19.20	Q3 (Dec) 19.20
Number of Review Child Protection Conferences held	63	36	56	43
Number of Review Child Protection Conferences held within timescale	62	36	51	43
Percentage of Review Child Protection Conferences held within timescale	98.4%	100.0%	91.1%	100.0%

03 Referrals to Education

Fig 3.1 Contacts by Source – Primary School

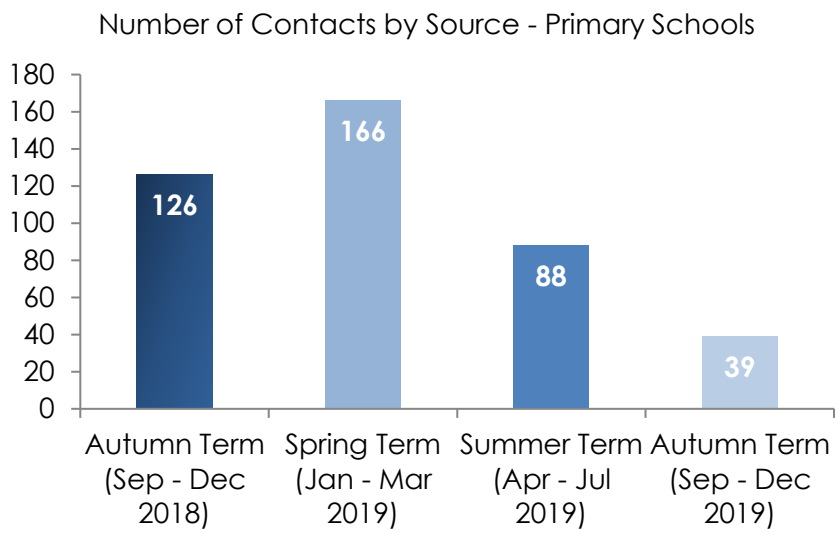


Fig 3.2 Contacts by Source – Secondary School

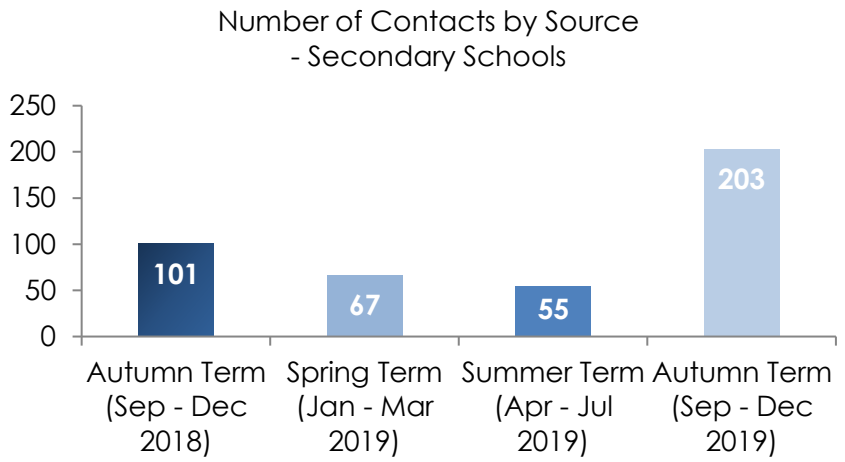


Fig: 4.1 RPI Incidents

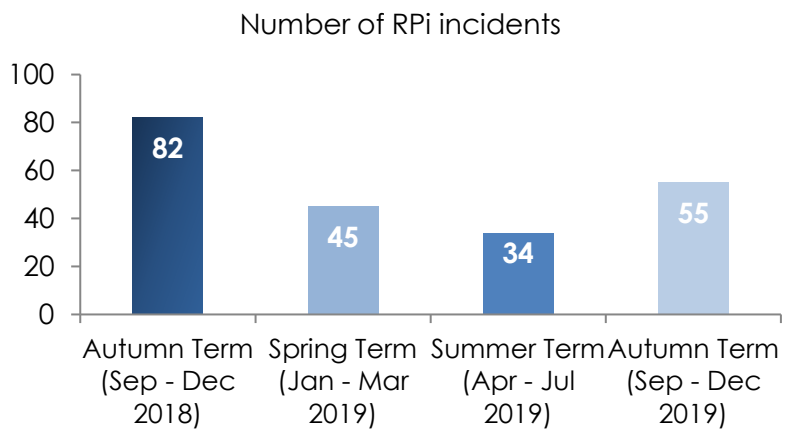


Fig 4.3 Quality Assurance Visits

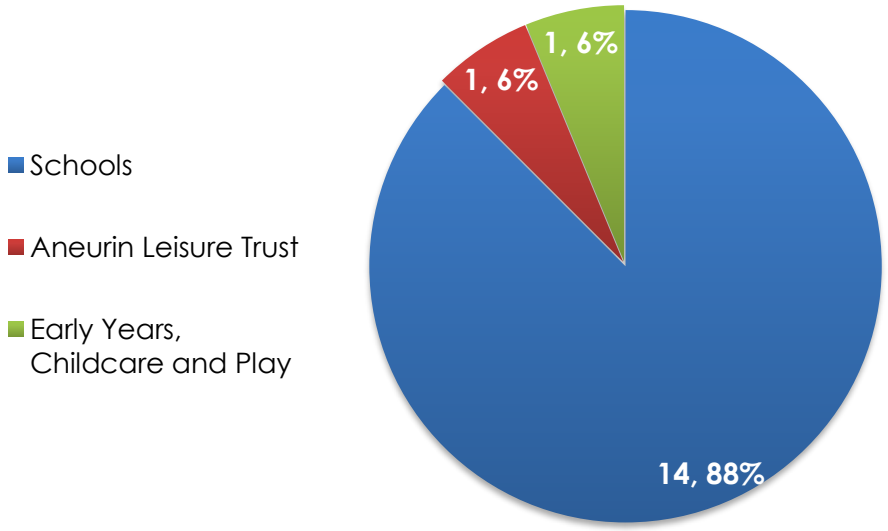
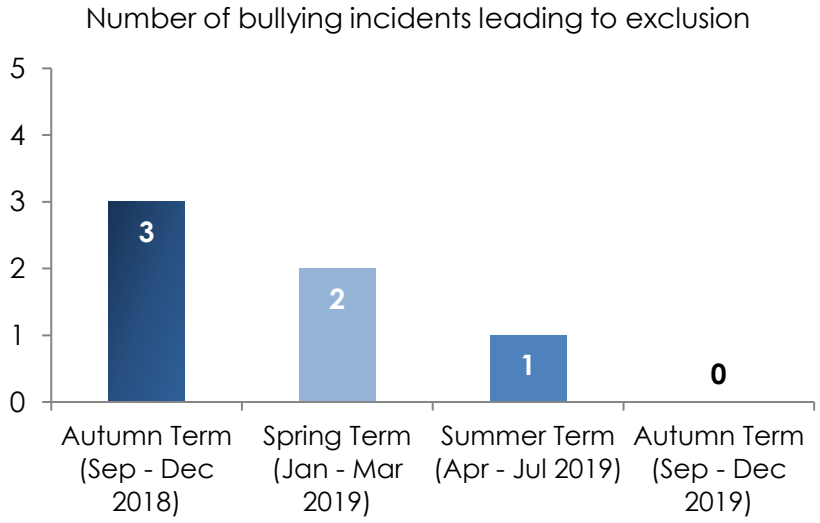


Fig: 4.2 Bullying incidents leading to exclusion

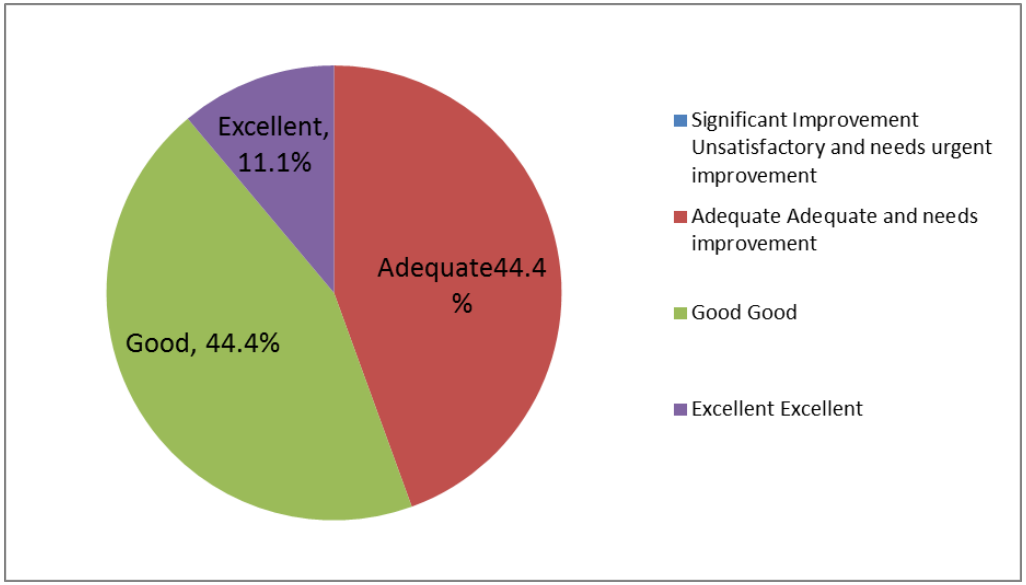


4.4 Estyn Judgements

The table below provides an overview of the Estyn judgements for schools inspected under the new arrangements from September 2017 up until December 2020.

Estyn Inspection Framework September 2017							Inspection Areas					
LA	Phase	School #	School	Date report Published	Follow-up Activity	Monitoring Visit 1	Standards	Wellbring and attitudes to learning	Teaching and learning experiences	Care, Support and guidance	Leadership and management	Out of Follow - up activity
BG	Secondary	6775401	Brynmawr Foundation School	Dec-19	SM		Unsatisfactory	Unsatisfactory	Unsatisfactory	Adequate	Unsatisfactory	
BG	Primary	6773309	St Marys CIW Primary School	Mar-19	_		Good	Good	Good	Good	Good	
BG	Primary	6772310	Rhos y Fedwen Primary **	Feb-17	Estyn Review		Adequate	Adequate	Adequate	Adequate	Adequate	Jul-18
BG	Primary	6772310	Blaenycwm Primary	May-18	-		Good	Good	Good	Excellent	Good	
BG	Secondary	6772306	Abertillery Learning Community	01/02/2018 (revist June 19)	SI	SI	Adequate	Adequate	Adequate	Adequate	Unsatisfactory	
BG	Primary	6774074	St. Joseph's R.C. Primary	Jan-18	-		Good	Good	Good	Good	Good	
BG	Primary	6773316	St. Illtyd's Primary	01/10/2017 (revisit Mar 19)	Estyn Review	-	Adequate	Adequate	Adequate	Adequate	Adequate	Mar-19
BG	Primary	6772312	Glyncoed Primary*	Nov-17	-		Good	Good	Good	Good	Good	
BG	Primary	6772309	Glanhowy Primary*	Feb-18	-		Good	Good	Good	Good	Good	

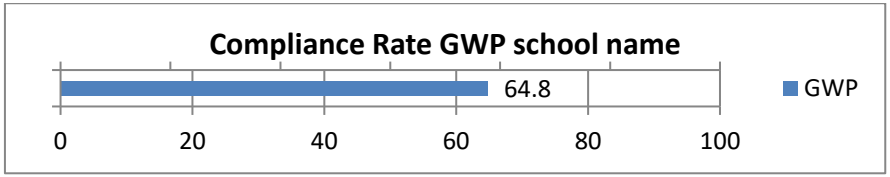
Care and Support Guidance Inspection Ratings

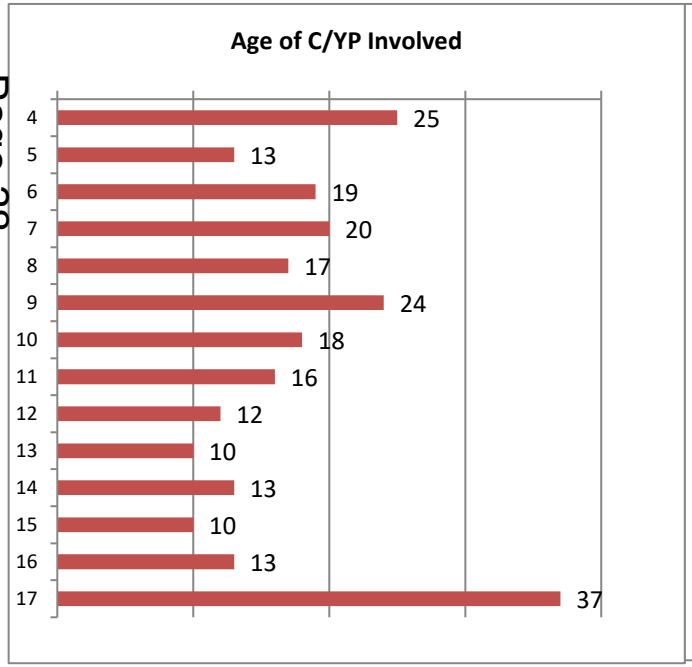


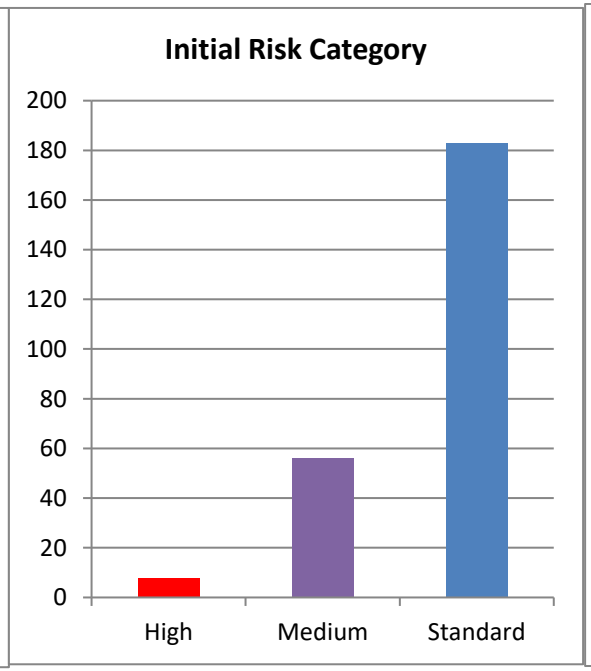
4.5 Operation Encompass

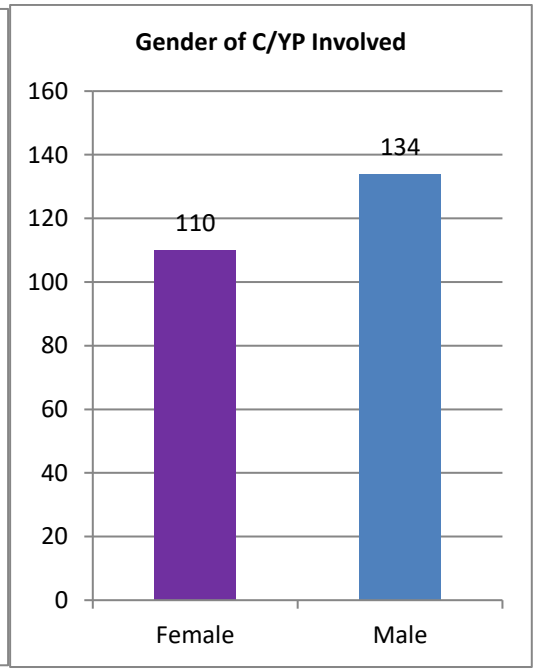
For the period Quarter 3 – October to December

Occurences	CYP
156	247









4.6 Elected Home Education (EHE)

	December 2019	December 2018
Total number of children electively home educated	77	76

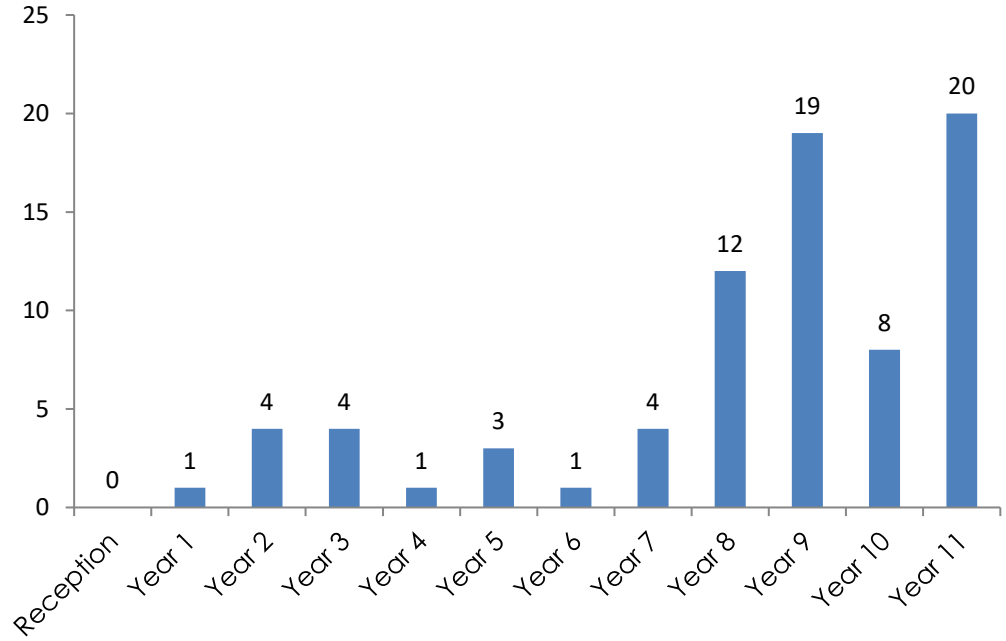
4.7 The table below sets out the number of secondary age pupils who have become EHE or who have returned to school from being EHE during the Autumn and Spring term.

Month	School 1		School 2		School 3		School 4	
	Out	In	Out	In	Out	In	Out	In
Jan – Mar 2019	1	0	2	0	1	0	2	0
Apr – Jul 2019	0	0	2	0	2	3	6	0
Sept – Dec 2019	3	1	0	1	2	5	1	0
Total	**4**	**1**	**4**	**1**	**5**	**8**	**3**	**0**

4.8 The table below sets out the number of additional pupils who have become EHE or who have returned to school from being EHE during the Spring, Summer and Autumn term.

Month	Primary		College		Did not transition		Moved into/out of Borough (including BG pupils that were in OOC schools)		School place unavailable	
	Out	In	Out	In	Out	In	Out	In	Out	In
Jan – Mar 2019	2	0	0	0	0	0	0	1	0	0
Apr – Jul 2019	2	0	0	0	0	0	0	1	0	0
Sept – Dec 2019	0	2	0	2	2	0	3	3	0	0
Total	**4**	**2**	0	**2**	**2**	**0**	**3**	**5**	**0**	**0**

4.9 Breakdown per year group EHE



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:	**23rd March 2020**
Report Subject:	**Adult Safeguarding Report 1st July to 31st December 2019**
Portfolio Holder:	**Cllr John Mason, Executive Member Social Services Cllr Clive Meredith, Executive Member Education**
Report Submitted by:	**Andrew Day, Adults Service Manager for Development, Commissioning and Safeguarding and Sarah Jones, Adults Safeguarding 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)**
28.02.2020	03.03.2020	09.03.20			23.03.2020	22.04.20		

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 July 2019 to the 31st December 2019. 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 To enable greater focus on the Safeguarding agenda, Corporate Leadership Team and Elected Members agreed for safeguarding information to be reported to a Joint Social Services/Education and Learning Scrutiny Committee after each school term.

2.2 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.

3.2 **<u>Option 1</u>**

Members are asked to consider the detail contained in the Adult Safeguarding Report and contribute to the continuous assessment of effectiveness by making appropriate comments and or recommendations for amendment to the report before consideration at Executive Committee.

Option 2

Accept the report as provided and recommend for the Executive Committee to consider the report.

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.

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 (short and long term impact)***

We have received confirmation from Welsh Government and the RPB that the support worker post funded through the Integrated Care Funding (ICF) has been approved for a further 12 months from the 1ST April 2020.

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***

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 286. During the same period for the previous year (2019/20) there were a total of 269 referrals received. This evidences that the figures are fairly static year on year.

Number of reports of an adult suspected of being at risk received during the first quarter of 2019/2020 1st July 2019 to 30th September 2019 – 161 1st October 2019 to 31st December 2019 – 125	286

6.3 The number of referral received within the different categories of abuse or neglect are shown below for July 1st 2019 – 31st Dec 2019. It should be noted that concerns about more than one type of abuse can be reported within the same referral.

Category of Abuse	Gender	Age 18-64 01/07/19 – 30/09/19	Age – 65 and over 01/07/19 – 30/09/19	Age 18-64 01/10/19 – 31/12/19	Age – 65 and over 01/10/19 – 31/12/19
Physical	Male	6	9	9	4
	Female	12	18	12	18
	Transgender	0	0	1	0
Sexual	Male	0	2	1	0
	Female	1	0	6	1
Emotional/Psychological	Male	5	6	3	4
	Female	8	6	10	12
	Transgender	0	0	1	0
Financial	Male	8	0	8	3
	Female	4	5	9	7
Neglect	Male	16	27	6	18
	Female	14	34	7	24
	Transgender	0	0	1	0
Total	**Male**	**32**	**39**	**20**	**23**
	Female	**31**	**59**	**27**	**54**
	Transgender	**0**	**0**	**1**	**0**
	Total	**63**	**98**	**48**	**77**

Quarters 2 and 3 are showing a similar trend to the previous year where neglect is the most prevalent category and sexual abuse the least prevalent.

6.4 Referrals of domestic abuse are captured as part of the data return for the Welsh Government.

		Age 18-64 01/07/19 – 30/09/19	Age – 65 and over 01/07/19 – 30/09/19	Age 18-64 01/10/19 – 31/12/19	Age – 65 and over 01/10/19 – 31/12/19
Domestic	Male	1	2	3	0
	Female	9	3	7	5

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.

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** 01/07/19 – 30/09/19	**Total** 01/10/19 – 31/12/19
Own Home	61	62
Community	6	2
Care Home Setting	79	43
Health Setting	4	3
Other	**11**	**15**
Total	**161**	**125**

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.

The persons alleged responsible for the abuse are broken down in the table below. Paid employees being alleged perpetrators for 65 in quarter 2 and 10 in quarter 3 and 22 being a relative or friend in quarter 2 and 16 in quarter 3. 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. During quarters 2 and 3, of the 26 referrals received 18 were inappropriate, 1 case was closed with no further action and 7 remain open cases.

Person alleged responsible	Total 01/07/19 – 30/09/19	Total 01/10/19 – 31/12/19
Paid Employee	65	10
Relative / Friend	22	16
Volunteer / Unpaid employee	0	0
Other service user	10	10
Other	1	3
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	63	86
Total	**161**	**125**

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.

Source of Referral	Total 01/07/19 – 30/09/19	Total 01/10/19 – 31/12/19
Self-reported	4	0
Relative / friend	2	1
Local authority	41	31
Police	1	4
Local health board	9	19
Independent hospital	1	0
Ambulance service	2	3
Care regulator	1	1
Provider agency	86	48
Probation	1	0
Third sector	7	10
Advocate	0	0
Other	6	8
Total	**161**	**125**

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 action plan developed to address the recommendations required. A further update will be provided at the next meeting.

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 Social Services Scrutiny Committee.

Background Documents /Electronic Links
The following hyperlink provides further details on the governance and

Structure: www.gwentsafeguarding.org.uk .

REF:

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**
Date of meeting:	**23rd March 2020**
Report Subject:	**360 Degree Safe Cymru Online Safety Policy for Schools**
Portfolio Holder:	**Cllr J Collins, Executive Member for Education**
Report Submitted by:	**Lynette Jones, 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)**
✔	25.02.2020	07.03.20			23.03.2020	22.04.20		

1. Purpose of the Report

1.1 This report presents the 360 Degree Safe Cymru Online Safety Policy for schools in order to seek members' views on the policy template and adoption of such by the Council as the model policy for schools.

1.2 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. 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 the Council and schools' wider duty of care.

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 has been developed by South West Grid for Learning and a range of individuals and organisations have contributed to the development of this policy.

2.3 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.

2.4 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 schools and the Council.

2.5 The 360 Degree Safe Cymru Online Safety policy is compliant with the Estyn recommendation as set out in the Prevent Thematic Review that was published in February 2020, which is to ensure that ICT and Online Safety policies cover the management of risks to pupils from radical and extremist ideologies.

3. Options for Recommendation

3.1 **Option 1**

Members are requested to scrutinise the information detailed within the report and contribute to the continuous assessment of effectiveness by making appropriate recommendations to the 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

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.
- Blaenau Gwent wants safe and friendly communities.

5. Supporting Evidence

51 ***Performance Information and Data***

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

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.

The latest data shows that there are presently 22 schools registered in Blaenau Gwent to use the 360 Degree Safe Cymru assessment tool and 20 schools have presently used it.

5.2 ***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.

5.3 ***Involvement (consultation, engagement, participation)***

The proposed policy demonstrates an integrated approach to online safety across schools.

School views have been sought through the Designated Safeguarding Persons meetings. There were no objections to this 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:

- 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.

5.4 ***Thinking for the Long term (forward planning)***

Welsh Government encourages schools to make full use of social technologies to engage learners and improve learner outcomes. The proposed policy supports this.

5.5 ***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.

5.6 ***Collaboration / partnership working***

The Council collaborates with a range of services to discharge its Local Government Education Service functions.

This policy has been developed by South West Grid for Learning, working in partnership with Welsh Government. A range of individual and organisations have contributed to the development of the policy and appendices.

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

5.7 ***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

5.8 ***EqIA (screening and identifying if full impact assessment is needed)***

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

6. **Monitoring Arrangements**

6.1 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.

7. **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:

REF: 360DSOLSPFS.212

Online safety policy template

for schools and colleges

Contents

Introduction 1
Development/monitoring/review of this policy 5
Roles and responsibilities 6
Policy statements 9
Communication technologies **Error! Bookmark not defined.**
User actions 19
Responding to incidents of misuse 20
Learner actions 23
Staff actions 24
Appendix 25
Appendices: Section A – Acceptable use agreement 26
Appendices: Section B – Specific policies 26
Appendices: Section C – Supporting documents and links 26
A1 Learner acceptable use agreement template – for younger learners (Foundation) 27
A2 Learner acceptable use agreement (AUA) template – for older learners 28
A3 Staff (and volunteer) acceptable use agreement template 30
A4 Parent/carer acceptable use agreement template 34
A5 Acceptable use agreement for community users template 38
B1 School/college technical security policy template (including filtering and passwords) 40
B2 School/college personal data handling guidance 47
B3 School/college mobile technologies policy template (inc. BYOD/BYOT) 57
B4 Social media template policy 61
B5 School/college policy template – Online safety group terms of reference 65
C1 Responding to incidents of misuse – flow chart 67
C2 Record of reviewing devices/internet sites 68
C3 Reporting log template 69
C4 Training needs audit log template 70
C5 Summary of legislation 71
C6 Office 365 – further information **Error! Bookmark not defined.**
C7 Links to other organisations or documents 74
C8 Glossary of terms 77

Introduction

The online safety policy template

These school/college online safety policy templates are intended to help school/college leaders produce a suitable online safety policy document which will consider all current and relevant issues, in a whole school/college 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/colleges are bound. Schools/colleges 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/college'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/college online safety policy, based on good practice. In addition there are a range of alternative statements that schools/colleges should consider and choose those that are most suitable, given their particular circumstances.

An effective school/college online safety policy must be tailored to the needs of each school/college 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/college 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/college 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/colleges 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/colleges 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/college, 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/college. 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/colleges 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/college online safety policy.

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

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

[Name of school/college]

Online safety policy

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

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/college 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/college 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/college should have a named member of staff with a day to day responsibility for online safety; some schools/colleges may choose to combine this with the designated senior person role. Schools/colleges 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/college.

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/college 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/college/local authority) technical staff

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

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

- the *school/college* technical infrastructure is secure and is not open to misuse or malicious attack
- the school/college 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/college 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/college 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/college 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/college activities (where allowed) and implement current policies with regard to these devices

[4] The school/college 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/colleges 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/college 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/college 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/college online safety policy/documents
- *the production/review/monitoring of the school/college filtering policy (if possible and if the school/college 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/college 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] School/colleges 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/college and realise that the school/college's online safety policy covers their actions out of school/college, if related to their membership of the school/college.

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/college 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/college in promoting good online safety practice and to follow guidelines on the appropriate use of:

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

Community users

Community users who access school/college systems/website/Hwb/learning platform as part of the wider school/college provision will be expected to sign a community user AUA before being provided with access to school/college 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/college's online safety provision. Learners need the help and support of the school/college 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/college 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/colleges under the Counter Terrorism and Securities Act 2015 which requires schools/colleges 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/college.*
- *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/college 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/college will provide opportunities for local community groups/members of the community to gain from the school/college'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/college 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/college 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/college training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

If the school/college has a managed ICT service provided by an outside contractor, it is the responsibility of the school/college to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school/college, as suggested below. It is also important that the managed service provider is fully aware of the school/college online safety policy/acceptable use agreements. The school/college 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/college will be responsible for ensuring that the school/college 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/colleges 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/college technical systems will be managed in ways that ensure that the school/college 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/college 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/college networks and system will be protected by secure passwords.**
- **The master account passwords for the school/college systems should be kept in a secure place, e.g. school/college 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/college 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/college.
- (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/college 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/college 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/college 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/colleges under the Counter Terrorism and Securities Act 2015 which requires schools/colleges 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/college technical staff regularly monitor and record the activity of users on the school/college technical systems and users are made aware of this in the acceptable use agreement. (schools/colleges 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/colleges 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/college systems and data. These are tested regularly. The school/college 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/college 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/college devices that may be used out of school/college.
- An agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school/college 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/college devices. Personal data cannot be sent over the internet or taken off the school/college site unless safely encrypted or otherwise secured. (See school/college personal data policy template in the appendix for further detail.)

Mobile technologies

Mobile technology devices may be school/college 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/college's wireless network. The device then has access to the wider internet which may include the school/college 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/college context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school/college 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/college's online safety education programme.

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

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

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

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

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

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

School/college owned/provided devices:

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

Personal devices

- Which users are allowed to use personal mobile devices in school/college (staff/learners/visitors).
- Restrictions on where, when and how they may be used in school/college.
- Storage.
- Whether staff will be allowed to use personal devices for school/college 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/college responsibility).
- Identification/labelling of personal devices.
- How visitors will be informed about school/college requirements.
- How education about the safe and responsible use of mobile devices is included in the school/college 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/college 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/college 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/college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/college 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/college 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/college 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/college 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/college 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 / college 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 and colleges 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/college, 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/college policy (below) once it has been transferred or its use is complete.**

Staff must ensure that they: (schools/colleges 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/college 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/college 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/college's responsibilities and on good practice.

Communication technologies

This is an area of rapidly developing technologies and uses. Schools/colleges will need to discuss and agree how they intend to implement and use these technologies, e.g. few schools/colleges 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/college 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/college 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/college								
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/college, or on school/college network								
Use of school/college e-mail for personal e-mails								
Use of messaging apps								
Use of social media								
Use of blogs								

The school/college 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/college considers the following as good practice:

- **the official school/college 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/college email service to communicate with others when in school/college, or on school/college systems (e.g. by remote access)*

- **users must immediately report to the nominated person – in accordance with the school/college 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/college 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/college e-mail addresses for educational use.* (Schools/colleges 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/college 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/college 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/colleges and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools/colleges 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/college 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/college 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/college staff should ensure that:

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

When official school/college 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/college 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/college it must be made clear that the member of staff is not communicating on behalf of the school/college 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/college are outside the scope of this policy.
- Where excessive personal use of social media in school/college is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- *The school/college 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/college..
- The school/college should effectively respond to social media comments made by others according to a defined policy or process.

School/college 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/college'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/college 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/college context, either because of the age of the users or the nature of those activities.

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

or comments that contain or relate to:	character), contrary to the Criminal Justice and Immigration Act 2008					
	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/college or brings the school/college into disrepute				X	
Using school/college 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/college					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						

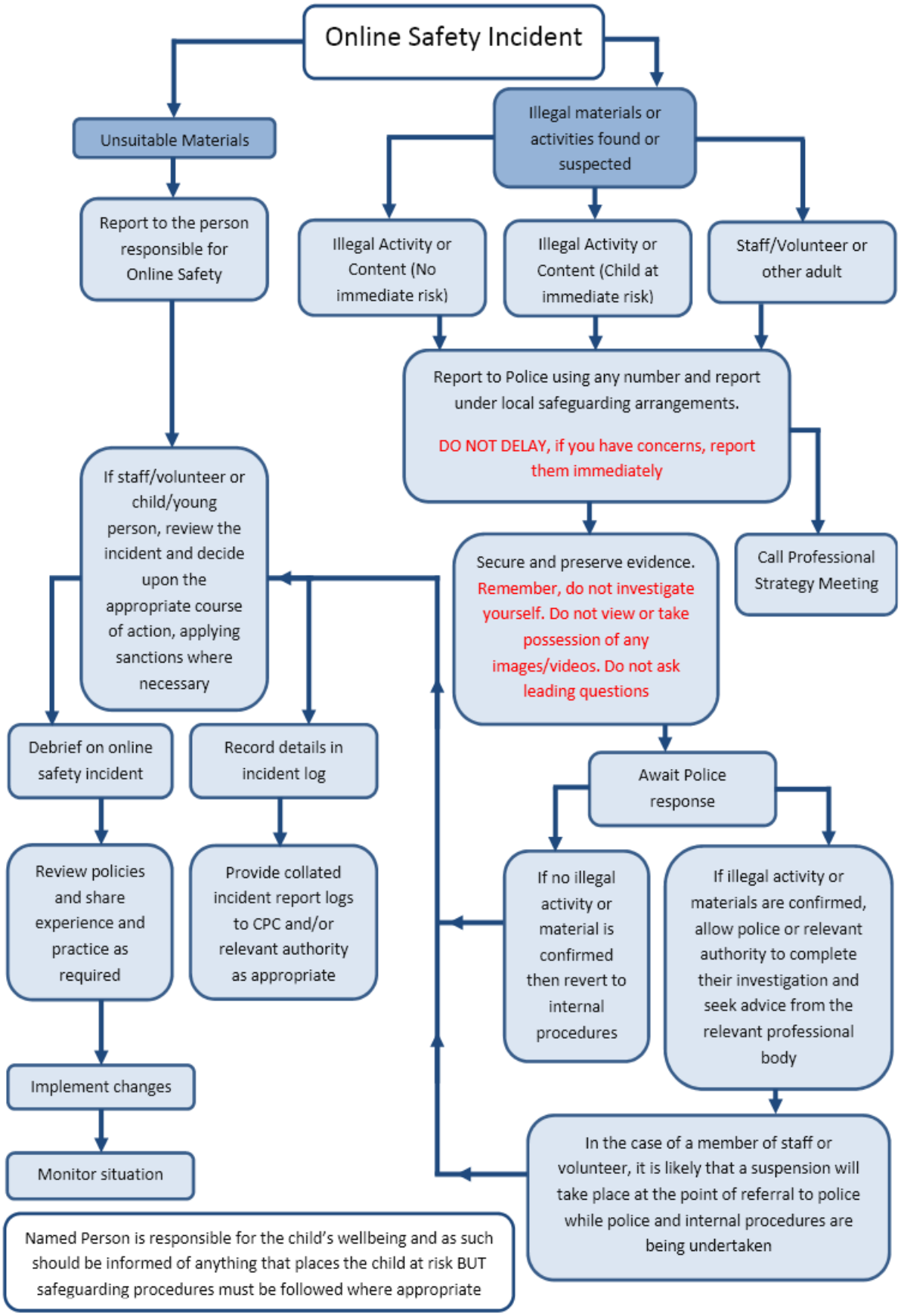
(The school/college should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools/colleges to decide their own responses).

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/college community will be responsible users of digital technologies, who understand and follow school/college 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/college 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/college actions

It is more likely that the school/college 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/college 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/college 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/colleges 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/college network by sharing username and passwords.									
Attempting to access or accessing the school/college network, using another learners' account.									
Attempting to access or accessing the school/college 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/college into disrepute or breach the integrity of the ethos of the school/college.									
Using proxy sites or other means to subvert the school/college'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/college network by sharing username and passwords or attempting to access or accessing the school/college 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/college into disrepute or breach the integrity of the ethos of the school/college.								
Using proxy sites or other means to subvert the school's/college'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/college 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/colleges 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/college 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/college 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/colleges 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/colleges will remove these sections from their final AUA document. Schools/colleges should review and amend the contents of this AUA to ensure that it is consistent with their online safety policy and other relevant school/college 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/college policy

Digital technologies have become integral to the lives of children and young people, both within and outside schools/colleges. 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/college systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school/college 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/college 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/college 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/college 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/college 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/colleges 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/college has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school/college:

- I will only use my own personal device(s) in school/college if I have permission (schools/colleges 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/college, I will follow the rules set out in this agreement, in the same way as if I was using school/college 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/college device, if I have permission
- I will only use social media sites with permission and at the times that are allowed (schools/colleges 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/college:

- I understand that the school/college 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/college and where they involve my membership of the school/college 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/colleges should amend this section to provide relevant actions as per their behaviour policies) loss of access to the school/college 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/college 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/college systems. (Schools/colleges 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/college systems and devices (both in and out of school/college)
- I use my own devices in the school/college (when allowed), e.g. mobile phones, gaming devices, cameras etc
- I use my own equipment out of the school/college in a way that is related to me being a member of this school/college, e.g. communicating with other members of the school/college, accessing school/college email, learning platform, website, etc.

Name of Learner:.....

Group/Class .....

Signed: .....

Date: .....

Parent/Carer Countersignature (optional)

Note: It is for schools/colleges 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/colleges 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/colleges will remove these sections from their final AUA document. Schools/colleges should review and amend the contents of this AUA to ensure that it is consistent with their online safety policy and other relevant school/college 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/college policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/colleges and in their lives outside school/college. 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/college 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/college 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/college 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/college 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/college ICT systems (e.g. laptops, email, VLE etc.) out of school/college, and to the transfer of personal data (digital or paper based) out of school/college (schools/colleges should amend this section in the light of their policies which relate to the use of systems and equipment out of school/college)
- I understand that the school/college 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/college (schools/colleges should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school/college 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/college 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/college'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/college 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/college in accordance with the school/college's policies. (schools/colleges 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/college systems. Any such communication will be professional in tone and manner. (schools/colleges 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/college and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school/college :

- When I use my mobile devices laptops/mobile phones/USB devices etc) in school/college, I will follow the rules set out in this agreement, in the same way as if I was using school/college equipment. I will also follow any additional rules set by the school/college 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/colleges 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/college digital technology systems. (schools/colleges should amend this section in the light of their email policy – some schools/colleges 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/college 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/college policies (schools/colleges/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/college 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/college/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/college 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/college 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/college:

- I understand that this acceptable use agreement applies not only to my work and use of school/college digital technology equipment in school/college, but also applies to my use of school/college 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/college
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools/colleges 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/college digital technology systems (both in and out of school/college) and my own devices (in school/college and when carrying out communications related to the school/college) 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/colleges and outside school/college. 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/college 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/college 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/college expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school/college in this important aspect of the school's/college's work. (Schools/colleges 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/college.

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/college.

Or: (Foundation)

I understand that the school/college 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/college.

I understand that the school/college 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/college 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/college 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/college if I have concerns over my child's online safety.

As the school/college 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/college. 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/college to take and use images of their children and for the parents/carers to agree.

As the school/college 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/college 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/college	Yes / No
I agree that if I take digital or video images at, or of – school /college 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/college 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 /college uses biometric systems for the recognition of individual learners in the following ways (the school/college 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/college 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/college 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/college that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school/college 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 and colleges 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/college, but new permission is required if there are changes to the biometric systems in use.

Use of Cloud Systems Permission Form

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

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

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

As the school/college 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/college digital technologies will be responsible users and stay safe while using these systems and devices
- that school/college 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/college 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/college

- I understand that my use of school/college systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school/college for any activity that would be inappropriate in a school/college 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/college on any personal website, social networking site or through any other means, unless I have permission from the school/college.
- 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/college 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/college 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/college has the right to remove my access to school/college systems/devices.

As the school/college 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/college digital technology systems (both in and out of school/college) and my own devices (in school/college and when carrying out communications related to the school/college) within these guidelines.

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

B1 School/college 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/colleges 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/colleges 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/college online safety policy.

The template uses various terms such as school/college. 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/college will be responsible for ensuring that the school/college 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/college's policies)
- access to personal data is securely controlled in line with the school/college'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/college computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

If the school/college has an externally managed ICT service, it is the responsibility of the school/college to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the school/college itself (as suggested below). It is also important that the managed service provider is fully aware of the school/college online safety policy/ acceptable use agreements. The school/college 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/colleges will probably choose the Network Manager/Technical Staff/Head of Computing or other relevant responsible person)

Technical Security

Policy statements

The school/college 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/college technical systems will be managed in ways that ensure that the school/college 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/college 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/college systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school/college, local authority or managed provider level)
- all users will have clearly defined access rights to school/college 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/college 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/college systems). (schools/colleges may wish to add details of the mobile device security procedures that are in use).
- *school/college/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school/college technical systems and users are made aware of this in the acceptable use agreement.* (schools/colleges 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/college system
- *an agreed policy is in place* (to be described) *regarding the downloading of executable files and the installation of programmes on school/college 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/college devices that may be used out of school/college*
- an agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school/college devices (see school/college personal data policy template in the appendix for further detail)
- the school/college 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/college site unless safely encrypted or otherwise secured. (see school/college 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/college 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/colleges 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/college networks and systems will be protected by secure passwords.**
- **All users have clearly defined access rights to school/college 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/college**
- **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/college 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/colleges 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/colleges 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/college.

- **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/college.
- Users will be required to change their password if it is compromised. Some schools/colleges 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/colleges 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/college systems should also be kept in a secure place e.g. school/college 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/college* 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/colleges may wish to have someone other than the school's/college'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/college 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/college's password policy:

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

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

- in lessons (the school/college 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/college has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school/college.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools/colleges. Where available, schools/colleges 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/colleges 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/college's filtering policy will be held by (insert title). They will manage the school/college 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/college filtering service must (schools/colleges 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/college'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/college. 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/college 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/college network, filtering will be applied that is consistent with school/college practice.

- *Either - The school/college maintains and supports the managed filtering service provided by the internet service provider (ISP)* (or other filtering service provider)
- *and/or – the school/college manages its own filtering service* (NB. If a school/college 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/college was able to meet its statutory requirements to ensure the safety of staff/learners)
- *the school/college 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/college internet connection (whether school/college or personal devices) will be subject to the same filtering standards as other devices on the school/college 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/colleges 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/college'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/college should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in school/college or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools/colleges 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/college level changes (as above).

Monitoring:

Some schools/colleges supplement their filtering systems with additional monitoring systems. If this is the case, schools/colleges 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/college will therefore monitor the activities of users on the school/college network and on school/college equipment as indicated in the school/college online safety policy and the acceptable use agreements. *Monitoring will take place as follows:* (details should be inserted if the school/college so wishes).

Audit/Reporting:

Logs of filtering change controls and of filtering incidents will be made available to: (schools/colleges 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/colleges 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/colleges 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/colleges in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school/college, 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/college personal data advice and guidance

Suggestions for use

This document is for advice and guidance purposes only. It is anticipated that schools / colleges will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school/college 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/college 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, colleges and other organisations. It is important that the school/college 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/college 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/colleges are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school/college will want to avoid the criticism and negative publicity that could be generated by any personal data breach
- the school/college 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 / colleges to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

Schools / Colleges have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school/college 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 / Colleges will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

Introduction

Schools / Colleges 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/college 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/college 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/college 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 / colleges 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 / colleges and the personal data required in a variety of forms to operate a school/college this means that all educational establishments in the UK are required to comply.

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

Personal Data

The school / college 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/college 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/college 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 / colleges 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 college 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 / colleges were able to rely on the 'legitimate interests' justification. But under the new laws, this has been removed for Public Bodies (which includes schools /colleges). 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/college 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/college equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school/college 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/college policy once it has been transferred or its use is complete.

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

The school/college 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/college 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/college 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/college recognises that personal data may be accessed by users out of school/college 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/college 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/college
- 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/college 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/college 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/college 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/ college 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 / colleges 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/college 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/college context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and colleges, 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/college 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 college 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/college should pay the relevant fee to the Information Commissioner's Office (ICO).

Responsibilities

Every maintained school/college 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/college may also wish to appoint a Data Manager. Schools/colleges 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 / college's information risk policy and risk assessment
- oversee the System Controllers

The school/college 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/college 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/college or elsewhere if on school/college 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 / colleges 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/college 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/college 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/college'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/college 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 / college's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools / colleges 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/college 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/college will be provided with the privacy notice through an appropriate mechanism.

Parental permission for use of cloud hosted services

Schools / colleges 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 / colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools / colleges 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 / colleges makes it clear that they are not able to use pupils' biometric data without parental consent. Schools / colleges 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 / colleges should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

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

Mobile technology devices may be a school/college owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's/college's wireless network. The device then has access to the wider internet which may include the school's/college'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/college 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/college 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/colleges 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/colleges should consider the following statements and remove those that do not apply to their planned implementation approach.

- **The school/college 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/college has provided technical solutions for the safe use of mobile technology for school/college devices and for personal devices**
- **For all mobile technologies, filtering will be applied to the school/college internet connection and attempts to bypass this are not permitted**
- **Where mobile broadband (e.g. 3G and 4G) use is allowed in the school /college, users are required to follow the same acceptable use requirements as they would if using school/college 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/college 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		
	School/collegeowned and allocated to a single user	School/college owned for use by multiple users	Authorised device[9]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school/college	**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/college 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/college 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/college 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.

[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

- **The software/apps originally installed by the school/college must remain on the school/college owned device in usable condition and be easily accessible at all times. From time to time the school/college 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/college will ensure that school/college devices contain the necessary apps for school/college work. Apps added by the school/college will remain their property and will not be accessible to learners on authorised devices once they leave the school/college roll. Any apps bought by the user on their own account will remain theirs**
- **The school/college 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/college 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**
- *All school/college 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/college 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/college is located in a position with a good 3G/4G signal, the school/college should provide guidance on the usage of this internet connectivity given that devices using these connections will not be covered by the normal school/college filtering. Schools/colleges 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/college entirely at the risk of the owner and the decision to bring the device in to the school/college 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/college*
- *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/college accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school/college or on activities organised or undertaken by the school/college (the school/college recommends insurance is purchased to cover that device whilst out of the home)*
- *the school/college accepts no responsibility for any malfunction of a device due to changes made to the device while on the school/college network or whilst resolving any connectivity issues*
- *the school/college 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/college 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/college 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/college to users concerning where and when mobile devices may be used** (the school/college 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/college**
- **devices must be in silent mode on the school/college site and on school/college 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/college policy on taking images.

Residential settings

Where a school/college 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/college 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/college 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/colleges 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/college 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/college its staff, parents and carers and learners.

Scope

This policy is subject to the school's/college'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/college 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/college's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school/college 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/college, it must be made clear that the member of staff is not communicating on behalf of the school/college 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/college (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/college

Managing accounts

- Process for creating new accounts
  The school/college 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/college" Facebook page. Anyone wishing to create such an account must present a business case to the school/college 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/college has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/college, including volunteers or parents.

Monitoring

- **School/college 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/college 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/college 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/college activity.
- If a journalist makes contact about posts made using social media staff must follow the school/college 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/college 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/college policies. *The school/college 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/college will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school/college will deal with the matter internally. Where conduct is considered illegal, the school/college 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/college, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school/college 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/college 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/college'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/college owned social media accounts**
- staff should exercise their professional judgement about whether an image is appropriate to share on school/college social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school/college 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/college, it must be made clear that the member of staff is not communicating on behalf of the school/college 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/college are outside the scope of this policy
- where excessive personal use of social media in the school/college is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the school/college 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/college on any personal social media network account
- the school's/college'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/college 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/college. In the event of any offensive or inappropriate comments being made, the school/college 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/college'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/college
- the school/college 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/college policy template - Online safety group terms of reference

1. PURPOSE

To provide a consultative group that has wide representation from the school/college 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/college 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/colleges 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/college 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/college (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/college]
- 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): .....

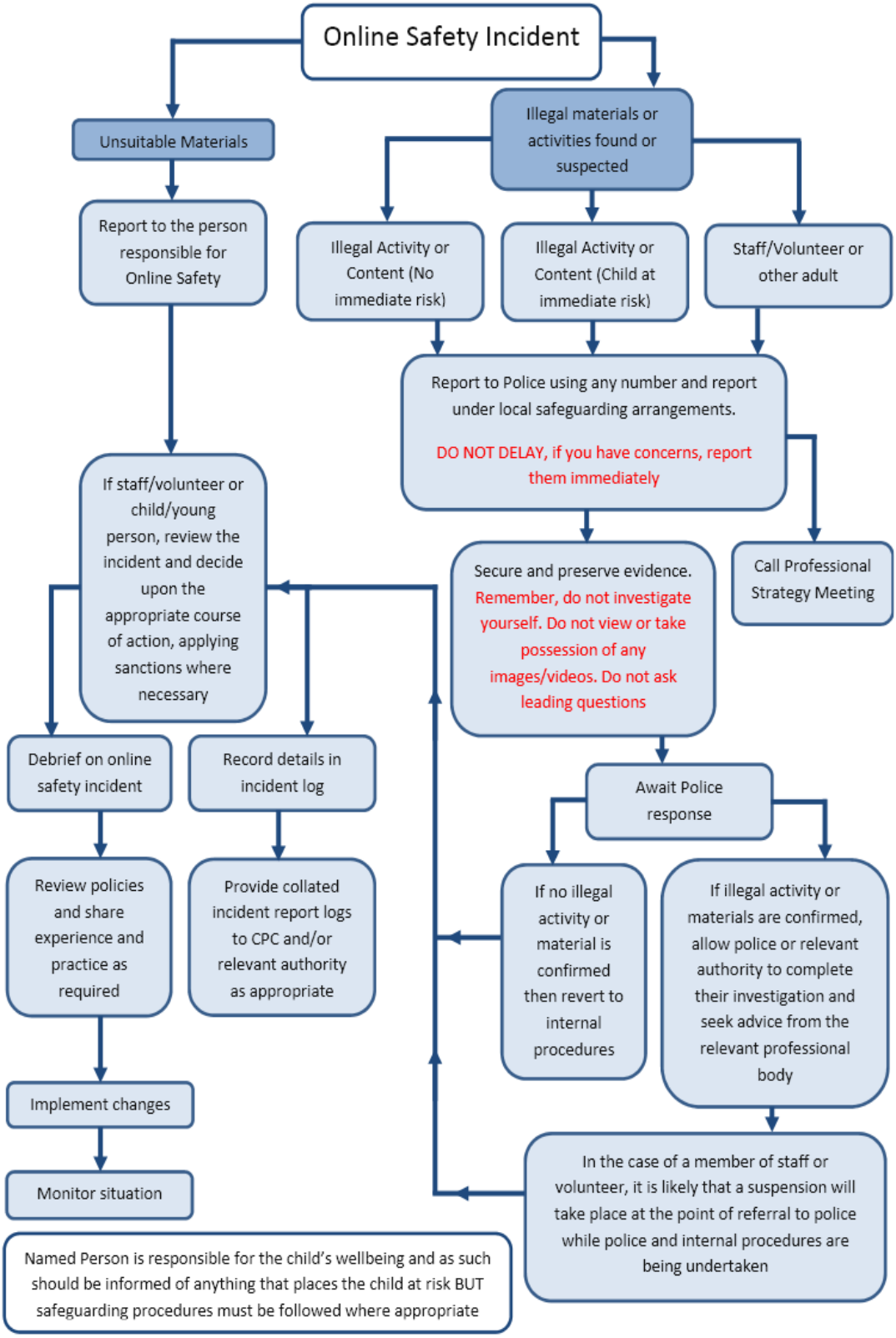
Date: .....

Date for review: .....

Acknowledgement

This template terms of reference document is based on one provided to schools/colleges 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/colleges 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/college 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/college 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/colleges 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 and colleges (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/colleges 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/colleges 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/colleges and other organisations in the SW
TUK	Think U Know – educational Online safety programmes for schools/colleges, 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 (Safeguarding) Scrutiny Committee**
Date of meeting:	**23rd March 2020**
Report Subject:	**Educational Neglect Policy**
Portfolio Holder:	**Cllr Joanne Collins, Executive Member for Education**
Report Submitted by:	**Lynette Jones, Corporate Director of Education**

Reporting Pathway								
Directorate Management Team	**Corporate Leadership Team**	**Portfolio Holder / Chair**	**Audit Committee**	**Democratic Services Committee**	**Scrutiny Committee**	**Executive Committee**	**Council**	**Other (please state)**
23/01/20	✔	07.03.20			23.03.20	22.04.20		

1. Purpose of the Report

1.1 The purpose of the report is to inform members of the Committee about the Educational Neglect Policy prior to consideration for approval by the Executive Committee and adoption by the local authority and school governing bodies. This policy has been written to ensure that there is a consistent and joined up approach by Education and Children's Services to address educational neglect.

2. Scope and Background

2.1 Improving educational outcomes for our children and young people is a key priority for the Council. The links between poor attendance and attainment are compelling and the Council is aiming to address the root causes of non-attendance, one of these being, 'safeguarding and long-term absence'.

2.2 The link between neglect and poor school attendance has been articulated in a number of recent reports. The Department for Education accepted a recommendation in 2012 that, 'persistent failure to send children to school is a clear sign of neglect and that Children's Services should work with schools to address underlying difficulties'.

2.3 In 2013, the NSPCC cited, 'failure to ensure regular school attendance that prevents the child reaching their full potential academically' (2) as one of their six forms of neglect.

2.4 Within the United States educational neglect is used to describe excessive unauthorised absence, failing to register for education or not supporting a child to get help for any special educational needs they are entitled to. The reporting of educational neglect is required as part of social services legislation in each school district in New York State.

2.5 Within Blaenau Gwent a number of young people who fail to attend school regularly are on the caseload of both Children's Services and the Education Welfare Service and it was felt that a collaborative approach was needed to address these pupils. The intention is not to necessarily increase the number of Children's Services referrals, rather, the purpose is to create a descriptor that highlights the critical educational and life implications relating to a child/young person that may not previously otherwise have been communicated. This is why it was agreed the 'education neglect' term should not be used unless a 12 month period has elapsed in which certain thresholds have been met.

3. Options for Recommendation

3.1 The options for Scrutiny to consider are:

3.2 **Option 1:** Consider the policy and provide challenge and/or further improvements for consideration.

Option 2: Accept the policy as drafted and recommend to the Executive Committee for approval.

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

4.1 ***Corporate Plan Priorities***

To improve pupil outcomes, progress and wellbeing, for all our pupils particularly for our more able and our most vulnerable learners.

4.2 ***Statutory Responsibilities***

To ensure that all pupils of compulsory school age attend school regularly and punctually in accordance with the 1996 Education Act and 1989 Children Act

4.3 ***Blaenau Gwent Well-being Plan***

To forge new pathways to prosperity - Good school attendance enables pupils to maximise their potential and obtain the highest possible outcomes. This is a fundamental pre-requisite of ensuring future local and national prosperity through the provision of an informed and well-educated workforce and society.

5. Implications Against Each Option

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

There are no financial implications for the local authority.

5.2 ***Risk including Mitigating Actions***

There is an ongoing need to improve school attendance so that pupils are attending school on a regular basis and are able to maximise their potential.

5.2.1 Failure to ensure that there is robust monitoring of attendance in schools and of the quality of Council services to support school improvement carries with it a number of significant risks:

- Undetected and unaddressed decline in school performance and the quality of provision;
- Students do not achieve to acceptable levels;
- Lack of overall improvement in schools' performance; and
- Negative impact on the reputation of the Council.

5.2.2 Similarly, ineffective monitoring of Council Services also poses a range of risks including:

- Reducing standards and quality of provision in schools;
- Poor value for money;
- Ineffective support for schools which hinders their improvement; and
- Negative impact on the reputation of the Council.

5.3 ***Legal***

To ensure that all pupils of compulsory school age attend school regularly and punctually in accordance with the 1996 Education Act and 1989 Children Act

5.4 ***Human Resources***

There are no direct workforce implications for the local authority.

6. **Supporting Evidence**

6.1 ***Performance Information and Data***

The statutory response from the Council regarding poor school attendance has been systematic and well evidenced.

6.1.1 There were 100 fixed penalty notices issued in 2017/18 and 41 prosecutions relating to school attendance.

6.1.2 There were 116 fixed penalty notices issued in 2018/19 and 80 prosecutions relating to school attendance.

6.1.3 When considering the data, the extent of re-offending and repeated court appearances regarding the same pupil and/or involving the same parents was considered of particular concern. This focused attention on those for whom behaviour was not changing over a period of time.

6.1.4 It was felt appropriate that it would be most useful to identify a term to characterise this neglect. The term 'educational neglect' was considered as being the most helpful, in that it could both support the narrative from professionals and simply convey to our school communities the level of concern the issue should invoke.

6.2 ***Expected outcome for the public***

There will be less young people out of education which has immediate implications for the public with regards to ensuring young people are better

safeguarded but also long term implications as it is widely researched that young people out of education cost health, police and other agencies more financial implications in later years than young people in full time education.

6.3 ***Involvement (consultation, engagement, participation)***
In order to devise this policy, a task and finish group was established comprising representatives from the Education Inclusion Service, Safeguarding in Education and the Service Manager for Children's Services. This policy has also been shared with Secondary Attendance Forum, Schools, Education DMT and Children's Services DMT.

6.4 ***Thinking for the long term (forward planning)***
Improved attendance levels will have no negative impact in the long term. It will, however, ensure that young people attend school more often to improve attainment of young people which in the long term improve their life chances.

6.5 ***Preventative focus***
Routine monitoring of attendance and collaborative working will keep the focus on the need for regular school attendance and ensure that families are supported to achieve this. Improved attendance will prevent young people from becoming NEET.

6.6 ***Collaboration / partnership working***
A regional approach to improving attendance is ongoing, involving the EAS and the five regional LAs.

6.7 ***Integration (across service areas)***
There is no direct impact in relation to an integrated approach however improvements in school attendance rates will prepare pupils for transition to adulthood reducing the effects of truancy.

6.8 ***EqIA (screening and identifying if full impact assessment is needed)***

An equality impact assessment has been completed and there are no adverse impacts in relation to the data contained in this report.

7. **Monitoring Arrangements**

7.1 This will be monitored termly through Education DMT and an annual report will also be provided as part of FADE reporting.

Background Documents / Electronic Links

Appendix A – Education Neglect Policy

REF. ENP.215

EDUCATIONAL NEGLECT POLICY

Education Inclusion Service

Educational Neglect Policy

February 2020

Cyngor Bwrdeisdref Sirol
Blaenau Gwent
County Borough Council

Contents

		Page
Part 1:	Introduction and background	2
Part 2:	Aims	4
Part 3:	Educational Neglect Descriptor and Definitions	5
Part 4:	Individual Attendance Rate Thresholds	7
Part 5:	Statutory Pathways	7
Part 6:	Appendix 1 - Callio and a five stepped approach to managing attendance	9

INTRODUCTION AND BACKGROUND

This policy aims to reduce persistent absenteeism in Blaenau Gwent.

Improving educational outcomes for our children and young people is a key priority for the Council. The links between poor attendance and attainment are compelling and the Council is aiming to address the root causes of non-attendance, one of these being, ‘safeguarding and long-term absence’.

In order to devise this policy, a task and finish group was established comprising representatives from the Education Inclusion Service, Safeguarding in Education and the Service Manager for Children’s Services.

The link between neglect and poor school attendance has been articulated in a number of recent reports. The Department for Education accepted a recommendation in 2012 that, ‘persistent failure to send children to school is a clear sign of neglect and that Children’s Services should work with schools to address underlying difficulties’.

In 2013, the NSPCC cited, ‘failure to ensure regular school attendance that prevents the child reaching their full potential academically’ as one of their six forms of neglect.

The statutory response from the Council regarding this issue has been systematic and well evidenced. There were 100 fixed penalty notices issued in 2017/18 and over 40 prosecutions relating to school attendance.

When considering the data, the task and finish group found of particular concern the extent of re-offending and repeated court appearances regarding the same pupil and/or involving the same parents. This focussed the group’s attention on being able to highlight those for whom behaviour was not changing over a period of time.

It was felt appropriate that it would be most useful to identify a term to characterise this neglect. The term ‘educational neglect’ was considered as being the most helpful, in that it could both support the narrative from professionals and simply convey to our school communities the level of concern the issue should invoke.

Whilst rarely used in the United Kingdom, the term has a resonance in the United States of America, where it is used to describe excessive unauthorised absence, failing to register for education or not supporting a child to get help for any special educational needs they are entitled to. The reporting of educational neglect is required as part of social services legislation in each school district in New York State.

In constructing the term for the Blaenau Gwent context, the group was aware that a number of young people who fail to attend school regularly are on the caseload of both Children’s Services and the Education Welfare Service. The intention is not to necessarily increase the number of Children’s’ Services referrals, rather, the purpose is to create a descriptor that highlights the critical educational and life implications relating to a child/young person that may not previously otherwise have been communicated. This is why it was agreed the term should not be used unless a twelve month period has elapsed in which certain thresholds have been met.

For it to be used in our local context, the task and finish group intend the term to be a descriptor that, on a continuum of need, demonstrates a critical state beyond the ‘persistent absence’ definition currently used across the country.

AIMS

The aim of this policy is to establish a common understanding and a common threshold for intervention in cases where educational neglect of children is a concern.

This document is aimed at practitioners working with children and families in Blaenau Gwent to support an improved understanding of educational neglect and how we can respond more effectively to achieve better outcomes for children.

This will be done by a) defining various levels of absenteeism and b) establishing clear procedures for intervention.

School attendance is primarily a whole school responsibility and schools work hard to ensure a cooperative relationship with the family of a child with attendance problems. During this time of working with the family there can sometimes be a delay in the escalation of appropriate interventions resulting in the number of absences continuing to accumulate. To avoid this problem, a two tiered approach to intervention has been developed. The tiers of intervention are tightly linked to the Borough's priority to reduce persistent absenteeism.

In the first stage, when a student is on his/her way to becoming persistently absent, the school and the Education Welfare Service conduct additional investigations to try to identify the underlying problems and causes of school absence and then provide additional and different school support services.

In the second stage, when the student's unauthorised absences reach the threshold for educational neglect, as defined below, then a referral should be submitted to Children's Services.

Hopefully, this collaborative approach will reduce persistent absenteeism rates and lessen the need for Court action.

EDUCATIONAL NEGLECT DESCRIPTOR AND DEFINITIONS

Certain risk factors will necessitate immediate referral to Children's Services.

The following definitions for Educational Neglect, where irregular school attendance is the only presenting or significant issue, requires evidence collated over a **twelve month period**. During this time a number of evidenced observations and actions will have ordinarily taken place by schools and the Education Welfare Service (Appendix 1 – Callio and a 5 stepped approach to managing attendance).

The following descriptor for neglect is provided which forms the basis of the following definitions.

> 'The persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development'.

1. DEFINITION OF EDUCATIONAL NEGLECT (OMISSION BY PARENT)

Meeting the Blaenau Gwent definition of Educational Neglect requires all of the following to be met over a twelve-month period:

- School attendance of 75% or less;
- Parent failing or inadequately maintaining schooling or identifying provision for their child;
- Parent failing to attend most school and LA meetings and/or engage with support offered;
- Parent unable to provide substantiated reasons for most absences from school; and
- At least one court intervention which fails to improve attendance. This could be a Section 444/444(1A) prosecution or School Attendance Order or Education Supervision Order.

This information, provided as part of a MARF should then lead to an integrated assessment.

School attendance of 75% or less over an academic year (three terms) in primary halves the possibility of achieving Level 4, the recognised average level for a child at the end of Key Stage 2 (11 years of age) and in a secondary setting is five times less likely to achieve 5 GCSE's including English and Mathematics, the recognised average level for a young person at the end of Key Stage 4 (16 years of age).

2. DEFINITION OF EDUCATIONAL NEGLECT (OMISSION BY YOUNG PERSON)

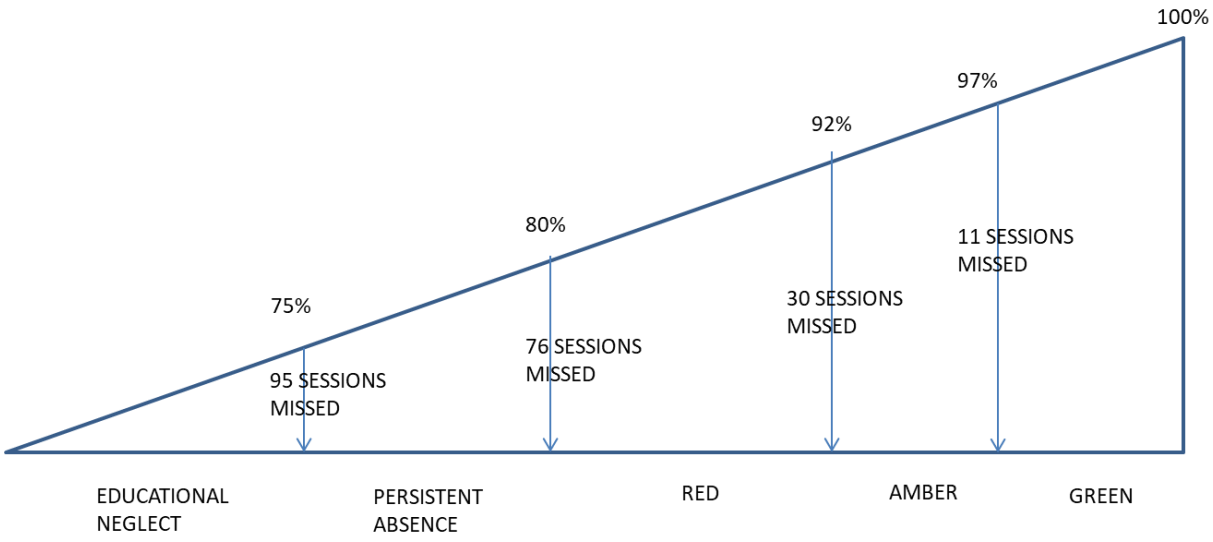
This definition is appropriate when pupils are old enough to determine their own actions and independently travel to school and where:

- parental co-operation is clearly demonstrated;
- current educational provision is appropriate for the young person's needs; and
- attendance levels are 75% or less.

Should these thresholds be met, the Education Welfare Service will consider applying to the Family Court for an Education Supervision Order.

If the young person or parent persistently fails to follow any directions made in the course of an Education Supervision Order, there is a legal duty for an integrated assessment, following a MARF.

INDIVIDUAL ATTENDANCE THRESHOLDS OVER 12 MONTHS



STATUTORY PATHWAYS

FIXED PENALTY NOTICE (Administered by the Council)

An early intervention where there is irregular attendance, unauthorised absence and reasonable expectation that this may change; discharges parent's liability for conviction of an offence by paying under the Education (Penalty Notices) (Wales) Regulations 2013.

PROSECUTION - ABSOLUTE OFFENCE (Magistrates Court)

Prosecution of a parent, under Section 444(1) of the Education Act 1996, for irregular attendance of child with unauthorised absence; this is a strict liability offence with limited defences.

PROSECUTION – AGGRAVATED OFFENCE (Magistrates Court)

Prosecution of a parent, under Section 444(1A) of the Education Act 1996, for irregular attendance of child with unauthorised absence; parent knows about irregular attendance and fails without reasonable justification to change this, potential of custodial sentence.

SCHOOL ATTENDANCE ORDER (Magistrates Court if not resolved)

Require parent(s), under Education Act 1996, to register a child of compulsory school age at a named school when not receiving a suitable education.

EDUCATION SUPERVISION ORDER (Family Court)

Twelve month Order under Section 36 of the Children Act 1989 on the grounds that the child is not being suitably educated; Supervising Officer to, ‘assist, advise and befriend’.

Appendix 1 Callio

Hours of Lost Learning and how attendance impacts on attainment

Green	100%	Not missing any lessons
	99%	Missing about 10 lessons
	98%	Missing about 20 lessons
	97%	Missing about 30 lessons
Amber	96%	Missing about 8 days of school. It will be difficult to catch up on lost learning from 40 lessons.
	95%	Missing about 2 weeks of school. Time to 'Callio'.
	93%	Missing 14 days of school. This is almost 3 weeks which is a significant amount of education to lose.
Red	92% and below	Missing more than 3 weeks of education. A serious loss of learning which is likely to have a detrimental effect on achievement and life chances.

For those pupils in the green category a well done letter is sent to parents

For those pupils in the amber category a warning letter is issued telling parents that they need to improve their child's attendance

For those pupils in the red category there would be an expectation that schools and the EWOs have taken a stepped approach to address the attendance issues.

STEP 1 – School Based Action

Initial school intervention should include:

1. 1st day of absence parental contact by telephone, text or e-mail.

2. Working together with parents and pupils to identify underlying causes of non-attendance, e.g.:

    - Medical needs
    - Bullying
    - Social Problems
    - Disaffection
    - Lateness
    - SEN

3. Developing and adopting in-school policies to identify underlying problems and where appropriate develop realistic strategies to address them.

4. Issuing advisory notices for unauthorised absences and persistent lateness.

STEP 2 – School-based in conjunction with advice from EWS

Where school-based interventions are still considered the appropriate level, Education Welfare Officer (EWO) expertise and advice may be sought.

The EWO, working in a consultative capacity, will act to assist the school in identifying possible alternative strategies through liaison with the school's senior manager with responsibility for attendance

At this level no formal referral is made. Though good practice would suggest that such consultations would result in a pupil's name being recorded in order to anticipate future intervention.

Where parents seek help from the Education Welfare Service (EWS) directly, Step1 intervention may be considered appropriate.

In order to move to Step 3 the appropriateness of a referral should be judged using the following criteria:

- Have all the school-based intervention strategies been adopted /considered?

The EWS would consider referral in the following cases in conjunction with information gained at Step 2.

- Block absences of more than 20 sessions without explanation.
- Irregular patterns of attendance with frequent unauthorised absences.
- Prolonged poor attendance pattern.
- Pupils with less than 90% attendance in a term period.
- Children at risk who exhibit poor or irregular attendance.
- Suspicious absences without medical corroboration.
- Known truants.
- School refusers.
- Absences connected with possible child safeguarding issues.
- Sudden deterioration in attendance without any specific reason and no explanation given.
- Pupils who are persistently late after close of registration
- Request for Fixed Penalty Notices

The following questions may be useful in considering whether a referral to the EWS is appropriate:

- Is the EWS the correct agency to undertake the task?
    - Is it, for example, a task for Families First, Children's Services, Educational Psychologist or YISP?
- Is the timing appropriate?
- What is the desired outcome of the intended referral?
- What will the impact be on others?
    - Parents/siblings.
- Is this a priority for the EWS or are there other agencies or strategies available?
- Have the parents been advised by the school that a referral could be made to the EWS?

All referrals should be made on the EWS Referral Form.

The referral form contains factual evidence and is essential for case management and review as well as providing statistical data to schools, governors and the Council.

In addition, the following must be attached to the referral form.

- A copy of the pupil's school attendance record.
- Copies of letters and contact with parents - with date, time and outcome.
- Copies of correspondence with other services/agencies.
- In order to ensure the health and safety of the EWO any details of concern of known risk factors associated with the pupil and the pupil's parents and family or the geographical location of the home must also be included.

STEP 3 Formal Referral to the EWS and requests for FPNs

Each pupil will be considered on an individual basis and a referral will be based on a number of factors outlined in Step 2, and not solely of a set target figure of attendance.

> School Staff are reminded that in order for legal action to be initiated at Step 5 absences must be recorded as unauthorised, as authorisation of an absence by the school constitutes a statutory defence to section 444 of the Education Act 1996

At Step 3 EWS action may include:

- Home visit.
- Writing to parents/carers.
- Contacting parents/carers by telephone.
- Emailing parents/carers
- Meeting with pupil in school with appropriate school staff.
- Meeting with pupil and parents in school with appropriate school staff.
- Support the school to draw up a contract between the school, EWS, parent and pupil.
- Issuing a Fixed Penalty Notice

Where a referral is agreed between the school and the EWO, the EWO will make an initial assessment and determine a course of action.

Where a home visit is considered the appropriate intervention the EWO will:

- Make a home visit within 5 school days of receipt of the referral.
- Provide a written response on process as part of the running referral record within 10 working days.
  The purpose of the home visit will be to:
- Assess family circumstances.
- Inform parents of their obligations in respect of school attendance.
- Provide advice and support to families

STEP 4 Case Management Approach

Where there has been little or no progress in improving attendance of individual pupils following EWS interventions at Step 3, the case will be subjected to a review in conjunction with the Senior EWO and other interested agencies where appropriate.

Consideration will be given to a number of complementary strategies. These may include:

- Intensive monitoring of individual pupil's attendance.
- A time limited in-depth programme with the family.
- Referral to other agencies/services.
- Holding an Attendance Case Review.
- Formal letters.
- Pre-court meeting.
- Consideration of Statutory Intervention – Step 5.

If there is no significant progress at Step 4, and there has been no evidence that the parents and or pupil have responded to a range of interventions which have been recorded and monitored, then parents will be informed that they have reached Step 5 Statutory Action.

Step 5 – Statutory Action

Where there is a need to implement statutory action the EWS will act within the following criteria (see EWS prosecution protocol):

- Prior to implementing action under Sect. 444 the EWS is required to give consideration of the suitability of the case for placing before the Family Court with regard to an Education Supervision Order under sect. 36 of the Children Act 1989 (*see below*)
- Are the absences in the attendance register shown as unauthorised? (*Under Sect. 444(1) Education Act 1996* – a statutory defence is the authorisation of absences by the school)
- Has consideration been given to all possible intervention?
- Have the parents co-operated with the school/LEA in supporting the pupil (*Parents who fail in this regard could be prosecuted under the aggravated offence Sect.444(1A) Education Act 1996 – where, if found guilty, the penalty is greater)*
- Are there any other circumstances that mitigate against prosecuting at this stage?

Where the above criteria have been met the EWO will present the case to their Senior EWO for consideration.

The Senior EWO responsible for legal matters will ensure that the following procedures are activated:

Section 444(1) or 444(1A) of the Education Act 1996 (Failure to secure regular attendance of registered pupil)
Where there is little or no improvement following the Pre-Court meeting the process will continue as detailed: -

- The EWO, in consultation with the Senior EWO will collate the following documentation for prosecution –
- Head Teacher's Certificate of Attendance
- Statement from the EWO and exhibits relevant to the case.
- Information regarding previous prosecutions.
- Supporting documentation, e.g. from other agencies

The Senior EWO responsible for legal matters will then progress the case with Legal Services.

Education supervision orders. S.36 the Children Act 1989

S.36 of the Children Act empowers the Council to apply for an Education Supervision Order (ESO). An ESO is a 'family proceedings' matter as defined by the Children's Act 1989, which regards the welfare of the child as the main concern and is a civil matter.

Courts may not make an ESO when the child is in the care of the L.A.

An ESO will only be considered under the following circumstances:-

- Where parent/s and pupil/s are committed to improving attendance
- Where parent/s and pupil/s are prepared to work closely with the designated EWSO
- Where the child is of an age to benefit from an ESO.

For children not registered with a school they could be prosecuted under Section 443 Education Act 1996. (Failure to comply with school attendance order.)

(This covers children not on the roll of any school or receiving education otherwise than in school)

- Established EWS intervention, i.e. letters, visits
- Series of notices relating to the School Attendance Order sent by EWS Head of Service to parents
- The School Attendance Order sent by 1st class post
- Statements prepared
- Procedure for prosecution is as above.

Support for Groups of Pupils at Particular Risk

Certain pupils have the potential to pose a particular risk in terms of attendance and may need additional support to ensure regular attendance.

The EWS may be able to provide additional advice and support in such cases.

These groups include:

- Pupils with Special Educational Needs/Additional Learning Needs
- Children in the care of the Council. (All absences authorised and unauthorised should be monitored and reported to the EWS)