Cyngor Bwrdeisdref Sirol
Blaenau Gwent
County Borough Council

Information Security Policy

V1.2

Issued: February 2021 Review: January 2023

Document History

Author	Version	Date	Review Date	Reason for Change
Rhian Hayden	V1.0	February 2021	March 2022	Policy creation – redrafted policy replacing old Information Security Policy 2013
Steve Berry	V1.1	April 2021	March 2022	Introduction of Document History table and minor amendments to detail removal of equipment from country, external information sharing and references to “Home Drives” to “Personal Storage Areas”
Kathy Buckley	V1.2	February 2022	February 2023	Minor updates and yearly review

1.0 AIMS OF POLICY

1.1 SCOPE

1.1.1 This policy applies to all Blaenau Gwent County Borough Council employees, schools, volunteers, members, contractors, third-parties and all authorised users with access to our information assets. They are referred to as 'users' throughout this policy.

1.1.2 It sets out the approach Blaenau Gwent County Borough Council have adopted to develop, manage and improve Information Security and ensure that our valuable information resources are properly protected against loss or compromise.

1.1.3 Where this policy refers to other standards, procedures and guidelines they must be read in conjunction with this policy.

1.1.4 Within the context of Information Security, the term 'information' includes data and any form of communication recorded or transmitted in transcript, verbally, manually or electronically. In terms of tangible assets, Information Security principles extend to paper documents, computer files, electronic records, data sticks, CDs, drives or any other storage or processing medium.

1.1.5 Blaenau Gwent County Borough Council recognise that users access various social media platforms, the internet and forums both as part of their business-operation and within their personal lives. In conjunction with this policy all users are expected to read, understand and adhere to the Social Media policy.

1.2 INTENTION

1.2.1 Information Security is different to 'Information Governance' which embraces a much broader set of administrative procedures necessary to manage the entire life of information from origin, through processing, to disposal. However, Information Security is an integral component of Information Governance and for this to be effective, a consistent, well organised and properly administered information structure must be established in all working environments throughout the organisation.

1.2.2 Blaenau Gwent County Borough Council adopts the view that information should be open unless its sensitive or personal. This is because sharing of information is critical to our day to day business decision making and helps other agencies use our information to develop innovative solutions and inform policy making. Open Data principles do not apply to sensitive or personal information, and it's critical that security arrangements are in place to prevent accidental sharing of this.

1.2.3 Every aspect of carrying out our business involves Information Security considerations, therefore it remains the responsibility of all people who work for or partner with Blaenau Gwent

County Borough Council to safeguard our information resources and ensure that all necessary protective measures are in place to prevent its loss or damage.

1.2.4 In applying this policy, it is also important that the breadth of protective security principles relating to information, IT, personnel and physical security are fully integrated to create sufficient depth and resilience to complement business continuity requirements and guard against all prevailing threats.

1.2.5 Finally, Information Security must take full account of a range of legislation (including DPA and GDPR) governing the manner in which information and data is managed and protected. A common theme is 'confidentiality' and, to remain legally compliant, obligations are placed upon staff to ensure that information is protected.

1.3 GENERAL PRINCIPLES

1.3.1 The organisation cannot function without information, processes and networks that combine to create a complicated data infrastructure. From this it is important to identify the more sensitive operational, financial or business information that requires specific protection and to develop measures to prevent, detect and mitigate loss or compromise.

1.3.2 There is always a need to balance the needs of the business operation with the need to keep sensitive and confidential data secure. Every attempt will be undertaken to do this electronically and seamlessly, but there is a still a need to adopt measures that preserve:

- Confidentiality – ensuring that information is accessible only to those authorised to have access, and protecting assets against unauthorised disclosure. Unauthorised access will not be tolerated.
- Integrity – safeguarding the accuracy and completeness of information, and protecting assets from unauthorised or accidental modification
- Availability – ensuring that authorised users have access to information and associated assets to carry out their duties effectively.

1.3.3 Another significant aim is to reinforce 'confidentiality' and 'need to know' principles. Information supplied in confidence, used to support business operations or connected with other sensitive business activities, must be treated in a confidential manner and only imparted to others in the official course of duties on a strict 'need to know' basis. This requirement is supported by legislation including:

- Data Protection Act 2018 / GDPR - requires personal data to be properly safeguarded and not disclosed unless properly authorised and justified. It also requires us to state the legal basis under which we gather, retain and use data along with allowing the data subject the right access to see the information and ensure its accuracy.
- Computer Misuse Act 1990 (and amendments within The Serious Crime Act 2015) – renders it illegal to gain access to or use a computer without authority.
- Freedom of Information Act 2000 - provides for disclosure of non-personal data, subject to exemptions including the prevention and detection of crime.

1.3.4 You must act honourably at all times and protect the reputation of the council.

1.4 THREATS AND VULNERABILITIES

In adopting relevant protective measures, the nature of threats and vulnerabilities must be considered.

1.4.1 Much of the work of Blaenau Gwent County Borough Council is of interest to others and, while the organisation must operate as an open public service, it is important to protect sensitive assets and guard against undesirable elements including cyber-attacks and, in some cases, the media.

1.4.2 As well as external vulnerabilities, the organisation and its users must avoid, deter, and counter unauthorised or illegal internal activity including any deliberate or accidental act or omission which could lead to loss of or compromise information.

1.5 ROLES AND RESPONSIBILITIES

1.5.1 All Blaenau Gwent County Borough Council users have a duty of care to ensure security is maintained. When data is processed as part of a business requirement they must ensure it is safe and secure at all times and is only distributed to the correct people.

1.5.2 Any security issues identified or suspected must be reported to the Data Protection Officer through the escalation procedures (dataprotection@blaenau-gwent.gov.uk) as well as the Information Security Officer via security@blaenau-gwent.co.uk

1.5.3 All users are responsible for ensuring their Blaenau Gwent County Borough Council equipment including laptops, mobiles and tablets are secure and are never left unattended, particularly in public places.

1.6 CHALLENGES & REPRESENTATIONS

1.6.1 Challenges and representations concerning this policy should be directed to the Senior Information Risk Owner (SIRO) and Information Security Officer at security@blaenau-gwent.co.uk

1.7 CONFIDENTIALITY

1.7.1 Information has uses beyond the normal day to day job, and Blaenau Gwent County Borough Council operates a policy of opening up key data for others to use for a variety of different reasons, not least of all to inform critical decisions on the levels of service provision.

1.7.2 However, much of the information in Blaenau Gwent County Borough Council is sensitive because of its operational, business or personal content, and where this is the case strict rules of confidentiality apply.

1.7.3 Sensitive and personal information is available to relevant staff and partner agencies to do their jobs, and is provided for official use only. Communication of sensitive or personal information to anyone not authorised to receive it is **strictly not permitted**, and disciplinary action will be taken against anyone who wilfully uses or discloses this information.

1.7.4 All printing of documents must be kept to a minimum, and only printed if there is an absolute business need.

1.7.5 When transferring information either internally or externally of the organisation users are responsible for ensuring that an appropriate secure method of transfer is used. Where unsure whether a method is appropriate or secure users should seek advice from the Data Protection Officer or Information Security Manager.

1.8 NEED TO KNOW

1.8.1 As an employee of Blaenau Gwent County Borough Council it is normal for you to encounter personal, confidential information. You will be required to sign a confidentiality agreement to this effect – normally as part of your employment contract. It goes without saying that this confidentiality must be protected. This includes information that is stored and displayed electronically, held in documents or publications and over the telephone or in conversations. Therefore, users must not discuss or divulge any information to anyone else, other than those who have to a need to know and must not use information for any other purpose than it was intended.

1.9 CLEAR WORKSTATION PRACTICES

1.9.1 Blaenau Gwent County Borough Council works in a very agile way, and as a result much of its information is electronic. However, where paper documents are used they must be managed in a way that prevents unauthorised access to sensitive information. This includes securing physical information in appropriate cabinets when not in use, particularly outside normal working hours. It's also important to make sure that paper documents taken away from the office are stored separately from desirable items like laptops or other mobile devices.

1.10 CLEAR SCREEN PRACTICE

1.10.1 Password protected screen savers must be activated when you leave your laptop or mobile device to prevent unauthorised access to information or systems. Be aware that mobile devices are desirable and can be the target for thieves. Make sure they are all password protected and that screen locks are activated if they haven't been accessed for 30 seconds.

1.11 SYSTEMS ACCESS AND PASSWORDS

1.11.1 Users and third parties are only permitted access to files and systems for which they have been specifically authorised. Access permissions are set up at the time of employment, and must be reviewed when there is a restructure, change of job or change of system. It's the responsibility of the manager to ensure this is done, and it's your personal responsibility to inform your manager immediately if you find you have access to anything you shouldn't see. Having unauthorised access to information does not entitle you to view it.

1.11.2 Passwords and other security processes are in place as part of the normal security arrangements and no attempt must be made to bypass them.

1.11.3 Passwords must not be divulged to others, nor written down.

1.11.4 Your password should not comprise of obvious names or dates that could easily be associated with you.

1.12 CORPORATE ASSETS (SOFTWARE/HARDWARE)

1.12.1 You will be prevented from loading unauthorised software onto any Blaenau Gwent County Borough Council's systems or devices. This is a critical part of Blaenau Gwent County Borough Council's security arrangements and you must not attempt to alter/amend/compromise the security in any way.

1.12.2 Anti-Virus software runs on either a server or workstation and monitors network connections looking for malicious software. Anti-virus software is generally reactive, meaning a signature file must be developed for each new virus discovered and these virus definition files must be sent to the software in order for the software to find the malicious code.

1.12.3 Virus definition files are periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software.

1.12.4 All computer devices connected to the Blaenau Gwent County Borough Council network shall have anti-virus software installed, configured so that the virus definition files are current, routinely and automatically updated, and the anti-virus software must be actively running on these devices. All files on computer devices will be scanned periodically for viruses.

1.12.5 You must not prohibit anti-virus or updates on any software from running, or bypass, exploit or deliberately avoid updates from running, as this will deemed to be a violation of this policy and subject to disciplinary. This is not restricted to antivirus software and includes patches and updates to all software and hardware owned by the Council.

1.12.6 Approved/licenced software and/or Blaenau Gwent County Borough Council's corporate information must not be downloaded, copied, shared, compromised, deleted, or distributed in any way that may have the potential to cause the council harm.

1.12.7 If you require additional software as part of your role, please raise with the SRS Service Desk.

1.12.8 Line of business systems (email, HR/Payroll etc) must only be used for business purposes.

1.12.9 The internet is a business tool, and activity is monitored. Please refer to the Acceptable Use Policy for more information.

1.12.10 Email and messaging services (including but not limited to Microsoft Teams, Skype, etc) are business tools, and all communications should be conducted in a professional manner as you are representing Blaenau Gwent County Borough Council. Spam (chain email) is not to be forwarded on, and any suspicious email (phishing email) should not be opened, and referred to security@blaenau-gwent.co.uk for investigation.

1.12.11 You will be provided as part of your role computer equipment, and potentially a mobile phone. You must look after these devices and not leave them unattended, or unlocked. You must not attach/connect any unapproved third party hardware to your Blaenau Gwent County Borough Council equipment. If you require access to additional equipment or require third party hardware to be connected to your devices, you must request this via SRS Service Desk.

1.12.12 Corporate equipment should not be used to store personal information.

1.12.13 The Social Media policy should be referred to prior to presenting the council on any social media platform, and should be read in conjunction with this policy.

1.12.14 Any employee or third party working on behalf of the council must seek approval from SIRO, DPO and Information Security Manager prior to taking any Blaenau Gwent County Borough Council equipment abroad

1.13 OVERSIGHT OR EAVESDROPPING

1.13.1 When discussing or processing issues of a sensitive nature on Blaenau Gwent County Borough Council premises or in public, extra care must be taken to avoid oversight of mobile computing devices, or eavesdropping on conversations.

1.13.2 When working remotely, be mindful of meetings and telephone conversations you are having in the home environment. Make sure that your door is shut when discussing confidential/corporate issues so that members of your family/third parties are not able to hear the detail of that conversation.

1.13.3 When attending a confidential call through MS Teams, either in the office or working remotely, a headset connected to your laptop must be used for the call. This is to avoid eavesdropping of calls and the two-way conversation being heard by third parties.

1.14 DISPOSAL OF DEVICES AND INFORMATION

1.14.1 Mobile devices must be disposed of by the SRS when they become obsolete. The SRS have a contract for this that ensures devices are wiped and correctly disposed of using approved methods. You must not attempt to dispose of mobile devices yourself. Please contact SRS Service Desk for old equipment to be collected.

1.14.2 All sensitive/corporate paper documents must be shredded using the onsite Confidential Waste bins provided and not put in the general paper waste facilities.

1.14.3 All printing of documents must be kept to a minimum, and only printed if there is an absolute business need.

1.14.4 This section of the policy should be read in conjunction with the Record Retention and Disposal Policy.

1.15 BREACHES OF SECURITY

1.15.1 Any security incident or occurrence that has the potential to compromise the organisation, staff, information or other assets, must be reported immediately to –

- Your Line Manager;
- The Data Protection Officer - dataprotection@blaenau-gwent.co.uk
- Information Security Officer - security@blaenau-gwent.co.uk

1.16 CONTRACTORS/THIRD PARTIES

1.16.1 Contractors and Third Parties must agree to adhere to this policy before access to Blaenau Gwent County Borough Council's Information Assets or Sites is provided.

1.16.2 All contractors and third parties must sign an NDA prior to accessing Blaenau Gwent County Borough Council's sites, systems or network.

1.16.3 Contractors and Third Parties' access to Information Assets or Sites must be the minimum necessary to achieve business purposes.

1.16.4 Contractors and Third Parties must connect to Blaenau Gwent County Borough Council network in a secured way.

1.16.5 Contractors and Third Parties that breach Blaenau Gwent County Borough Council's policies, procedures or contractual clauses will be subject to termination of contract or criminal proceedings if deemed appropriate.

1.16.6 On termination of contract, Contractors and Third Parties must relinquish any assigned software licences and passwords to 3rd party systems and must also return any Blaenau Gwent County Borough Council or related asset(s) issued during the contract, including-

- Information Assets (paper records, laptops, files, removable media, hard drives, mobile phones, End User Devices etc.);
- Access control software, hardware tokens, ID, passes etc.

1.17 REMOTE WORKING/MOBILE DEVICES

1.17.1 When working remotely users must make all reasonable efforts to secure the data and assets of Blaenau Gwent County Borough Council. Remote users should not leave their equipment unlocked or unattended at any time.

1.17.2 Remote workers must keep Information Assets in a locked area, cupboard or safe, out of plain sight, out of the reach of children and animals, away from any sources of heat, cold, or liquid.

1.17.3 When working remotely, be mindful of meetings and telephone conversations you are having in your environment. Make sure that your door is shut or nobody can eavesdrop when discussing confidential/corporate issues so that members of your family/third parties are not able to hear the detail of that conversation.

1.17.4 Users must immediately report any incidents that involves loss, theft, or compromise of an asset or loss or corruption of data.

1.17.5 This section should be read in conjunction with the Agile Working Policy.

1.18 PHYSICAL SECURITY

1.18.1 All visitors to Blaenau Gwent County Borough Council must sign in at reception and be accompanied throughout the duration of their visit. Users are encouraged to challenge people they don't recognise to ensure they are authorised to access sites.

1.18.2 To ensure the physical security of Information Assets users should –

- Keep Information Assets in a locked area, cupboard or safe, out of plain sight, out of the reach of children and animals, away from any sources of heat, cold, or liquid.
- When using public transport Blaenau Gwent County Borough Council Information Assets must not be left unattended.
- When transported in a car or vehicle, Blaenau Gwent County Borough Council Information Assets must be out of plain sight and not left unattended. Equipment should not be left in a vehicle overnight.
- Take reasonable care when transporting Blaenau Gwent County Borough Council Information Assets in hand luggage, bags, and backpacks and not leave them unattended.

1.18.3 As part of your role, users will be issued with an ID badge/access card. This card will provide you entry only into the areas you are permitted. Users should not try to gain access to areas where their card does not provide access. Under no circumstances should a user allow another person to use their ID card to gain access into a building/area.

1.18.4 Lost cards should be reported immediately to a line manager and access to the card should be disabled.

1.19 HOME DRIVES/PERSONAL FILE STORAGE & STORAGE OF FILES/DATA

1.19.1 Each employee of Blaenau Gwent County Borough Council will have access to their own storage area, called a "Home Drive" or "Personal File Storage". Home Drives/Personal File Storage areas are part of the corporate network and are to be used for business purposes only.

- Personal photographs and files/data are not to be stored in this location.
- Files/data relating to your operational performance, or staff records can be stored here to avoid other persons viewing this information.
- All files/data relating to normal business activity should be saved on the network drives.

1.20 COMPLIANCE

1.20.1 If a Blaenau Gwent County Borough Council Employee, Members, Contractor or Third Party breaches this policy, Blaenau Gwent County Borough Council may:

- Restrict or terminate the User's right to use Information Assets;
- Withdraw or remove any material uploaded by that User in contravention of this policy;
- Disclose information to law enforcement and regulatory agencies and take legal action;
- Take such other action as it deems appropriate, including up to and including dismissal through the disciplinary procedure.

Blaenau Gwent County Borough Council reserves the right to monitor employee, members, contractor, and third party activity across all Information Assets owned by the council.

2.0 COMPLIANCE WITH THE WELSH LANGUAGE SCHEME

2.1 This Policy will comply with the organisation's Welsh Language Scheme in terms of dealing with the Welsh speaking public, impact upon the public image of the organisation and the implementation of the Language Scheme.

3.0 IDENTIFICATION SECTION

Policy Title:	**Information Security Policy**
Policy Owner:	**Senior Information Risk Owner**
Department Responsible:	**All**
Links to other Policies/Procedure:	• **Data Protection Policy** • **Acceptable Usage Policy** • **Information Governance Polices** • **Social Media Policy** • **Record Retention & Disposal Policy** • **Cyber Security Incident Response Policy** • **Agile Working Policy**
Policy Implementation Date:	**1 February 2021**
Next policy review date:	**February 2023**
