



CONTENTS:		Page No:
1.	Aims of the Policy	2
1.1	Scope	2
1.2	Roles & Responsibilities	3
1.3	Challenges & Representations	3
1.4	Clear Workstation Practices	3
1.5	Clear Screen Practice	3
1.6	Corporate Assets (Software / Hardware)	3
1.7	<u>Email</u>	5
1.8	<u>Internet</u>	5
1.9	Remote Working / Mobile Devices	6
1.10	User IDs and passwords	6
1.11	Unacceptable use	6
1.12	Monitoring	7
1.13	Compliance	7

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 This policy contains mandatory controls that are required in order to meet regulation and standards 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.

1.1.3 It is intended to provide you with guidance and understanding of acceptable usage of systems, resources and workspaces within the organisation.

1.1.4 This policy and the statements contained within apply to all information, hardware devices and data, within Blaenau Gwent County Borough Council.

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

1.1.6 Failure to comply with certain statements within this document may result in the council being subject to penalty fines or regulatory action and could lead to disciplinary action being taken.

1.2 Roles and Responsibilities

- 1.2.1 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.
- 1.2.2 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
- 1.2.3 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.

1.3 Challenges & Representations

- 1.3.1 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

1.4 Clear Workstation Practices

- 1.4.1 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.
- 1.4.2 Blaenau Gwent County Borough Council users should not leave any documents on their desks or workstations overnight.

1.5 Clear Screen Practice

- 1.5.1 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.

1.6 Corporate Assets (Software / Hardware)

- 1.6.1 Use of corporate systems is granted subject to the users understanding & acceptance of the following statements:
- 1.6.2 Individuals must undergo security awareness education upon hire and at least annually. It is the responsibility of management to ensure this is completed.

- 1.6.3 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
- 1.6.4 Data created & stored on corporate systems remains the property of Blaenau Gwent County Borough Council
- 1.6.5 Corporate resources or devices are not to be used for personal use or business use that implicates illegal activity.
- 1.6.6 Monitoring and auditing may be performed on systems and user activity.
- 1.6.7 Access credentials including but not limited to passwords, door entry cards, PINs and ID badges must not be shared, divulged, published, copied or written down.
- 1.6.8 It is a disciplinary offence to attempt to circumvent or by-pass information security controls and policies.
- 1.6.9 Corporate devices, including workstations, PCs, laptops, and mobile phones must be screen locked or logged off when not in use or unattended.
- 1.6.10 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.
- 1.6.11 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.
- 1.6.12 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.

1.7 Email

- 1.7.1 Use of Email systems is granted subject to the users understanding & acceptance of the following statements:-
- 1.7.1 Email access may be revoked at any time if access is abused or is no longer necessary.
- 1.7.2 Email is primarily for business communication and purposes.
- 1.7.3 Email traffic and content is subject to monitoring and should not be considered private.
- 1.7.4 Users using corporate email represent the business in their behaviour and communications. Individuals must not discuss, divulge, publish or post information that may compromise the council's interests or bring the council into disrepute.
- 1.7.5 Email encryption method must be used when transferring confidential data externally. Please contact the SRS Service Desk if you require assistance with the email encryption process.
- 1.7.6 The forwarding of chain-mails, unsolicited 'spam' emails or suspicious email is prohibited.

1.8 Internet

- 1.8.1 Internet access is granted subject to the users understanding & acceptance of the following statements:-
- 1.8.2 Internet access to certain websites is granted to users for business use.
- 1.8.3 Internet websites may be blocked depending on their content or category.
- 1.8.4 Internet access to certain websites is based on job roles or department requirements. As such, some individuals will have different access to others.
- 1.8.5 Internet access may be revoked at any time if it is abused or is no longer deemed necessary.
- 1.8.6 Occasional personal internet use is allowed at the discretion of management, and personal browsing should only be undertaken at the end of the users working day/shift.
- 1.8.7 Internet usage, traffic and content is subject to monitoring.
- 1.8.8 Individuals using corporate internet connections represent the business in their behaviour and communications. Individuals must not discuss, divulge, publish or post information that may compromise the council's interests or bring the council into disrepute.
- 1.8.9 Users will only access appropriate content using Blaenau Gwent County Borough Council technology and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity.

- 1.8.10 Do not attempt to bypass Blaenau Gwent County Borough Council web filters.
- 1.8.11 Users will use social media appropriately by making themselves aware of the Social Media policy.
- 1.8.12 Users will not put Blaenau Gwent County Borough Council information including anything that is sensitive / personal information onto online forums, blogs or social networking sites.
- 1.8.13 Users will only use approved Blaenau Gwent County Borough Council social media accounts for official business and where appropriate, use Blaenau Gwent County Borough Council branding and a professional image or persona on such accounts.
- 1.8.14 Users must be aware that their social media content may be available for anyone to see, indexed by Google and archived for posterity.

1.9 Remote Working / Mobile Devices

- 1.9.1 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.
- 1.9.2 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.
- 1.9.3 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.
- 1.9.4 Users must immediately report any incidents that involves loss, theft, or compromise of an asset or loss or corruption of data.

1.10 User IDs and passwords

- 1.10.1 Users will protect usernames, staff numbers, ID badges and passwords appropriately.
- 1.10.2 Users will create secure passwords following best practice guidance.
- 1.10.3 Users will not logon to/or attempt to access any Blaenau Gwent County Borough Council system using another user's credentials.

1.11 Unacceptable use

- 1.11.1 Users will not trade or canvass support for any organisation on official premises, whether it is for personal gain from any type of transaction or on behalf of external bodies.
- 1.11.2 Users will not send messages or material that solicit or promote religious, political or other non-business-related causes, unless authorised by Blaenau Gwent County Borough Council.

- 1.11.3 Users will not create or transmit any offensive, obscene or indecent images, data or any data capable of being resolved into obscene or indecent images or material on Blaenau Gwent County Borough Council corporate assets or network.
- 1.11.4 Users will not create or transmit any material which is considered to facilitate harassment, bullying and/or victimisation of a user within Blaenau Gwent County Borough Council
- 1.11.5 Users will not provide unauthorised views or commitments that could appear to be on behalf of Blaenau Gwent County Borough Council.
- 1.11.6 Users will not use any type of applications and/or devices to circumvent management or security controls.
- 1.11.7 Users will not access personal webmail accounts on Blaenau Gwent County Borough Council equipment.
- 1.11.8 Users will not download photographs, music, video or other media-related files for non-business purposes or store such files on network drives
- 1.11.9 Users will not access or try to access data or physical areas within Blaenau Gwent County Borough Council where the user knows or ought to know that they should have no access
- 1.11.10 Users will not carry out hacking activities
- 1.11.11 Users will not intentionally or recklessly introduce any form of spyware, computer virus, data-interception, password-detection or other potentially malicious software onto Blaenau Gwent County Borough Council's network, systems, corporate devices, etc
- 1.11.12 Users will not use any information that they access or obtain as part of their role for any other purpose other than what their role permits.

1.12 Monitoring

- 1.12.1 Blaenau Gwent County Borough Council records and monitors the use of its assets (hardware and software) under the Regulation of Investigatory Powers Act (2000) for the purposes of:
- 1.12.2 The effective and efficient planning and operation of its assets (hardware and software)
- 1.12.3 Investigation, detection and prevention of infringement of the law, this policy or other council policies
- 1.12.4 Investigation of alleged misconduct by users

1.13 Compliance

- 1.13.1 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.

Version Control

Author	Version	Date	Comment
Information Security Manager	2021_1	January 2021	