Monmouthshire County Council

INFORMATION SECURITY POLICY

1.0 Aims of Policy

1.1 Scope

1.1.1 This policy applies to all Monmouthshire County Council employees, contractors, and third-parties with access to our information assets. They are referred to as 'users' throughout this policy.

1.1.2 It sets out the approach Monmouthshire County 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.

1.2 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 Monmouthshire County 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 its 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 Monmouthshire County 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

- 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.
- 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 While the intention of this policy is to identify a range of protective security measures, considerably more detail is necessary to provide practitioners with clear procedural requirements and guidance. Such detail will be contained in a series of 'Security Policies and Procedures' that will be approved by the Information Governance Group. These will be published on the intranet or otherwise circulated to those who need to know the content:-

- Acceptable use policy
- Data Protection Policy
- PCIDSS Policy
- Cyber Incident Response Policy

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 Monmouthshire County 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 must counter unauthorised or illegal internal activity including any other deliberate or accidental act or omission which could lead to loss of or compromise information.

1.5 Roles and Responsibilities

1.5.1 All Monmouthshire County Council employees 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 Chief Information Security Officer via security@monmouthshire.gov.uk

1.5.3 All users are responsible for ensuring their Monmouthshire County 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) or the Chief Information Security Officer via security@monmouthshire.gov.uk who will liase with the appropriate partners at the SRS and within Monmouthshire County Council.

1.7 Confidentiality

1.7.1 Information has uses beyond the normal day to day job, and Monmouthshire County 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 Monmouthshire County 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.

1.8 Need to Know

1.8.1 As an employee of Monmouthshire County Council, it is normal for you to encounter personal, confidential information.You will be required to sign a confidentiality agreement to this effect. 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 & Desk Practices

1.9.1 Monmouthshire County 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 Staff and partner agencies 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 its 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. Passwords must not be divulged to others, nor written down.

1.11.3 Passwords should be a minimum of eight characters and include the following complexity – special characters (!"£%^….), uppercase characters, lowercase characters, and numbers.

1.11.4 Users will create secure passwords following best practice guidance. The password configuration should not be compromised of obvious dates or names that could easily be associated with the user.

1.11.5 Users will not logon to/or attempt to access any Monmouthshire County Council system using another user's credentials.

1.12 Corporate Software

1.12.1 You will be prevented from loading unauthorised software onto any Monmouthshire County Council systems or devices. This is a critical part of Monmouthshire County Council security arrangements and you must not attempt to bypass this security in any way. In addition, approved/licenced software loaded onto Monmouthshire County Council systems must not be downloaded or copied.

1.12.2 Line of business systems (O365, Aggresso, HR/Payroll etc) must only be used for business purposes.

1.12.3 The internet can be used for personal use with the provisor that it is within personal time not work time and that you don't bypass the internet security filtering.

1.13 Oversight or Eavesdropping

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

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.

1.14.2 SENSITIVE paper documents must be shredded and not put in the general paper waste facilities.

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
- Chief Information Security Officer -
  - security@monmouthshire.gov.uk
- The Data Protection Officer –
  - Dataprotection@monmouthshire.gov.uk
- The Digital Programme office -
  - DigitalProgrammeOffice@monmouthshire.gov.uk
- The SRS –
  - security@SRSwales.com

1.16 Contractors

1.16.1 Contractors must agree to adhere to this policy before access to Monmouthshire County Council 's Information Assets or Sites is provided. Contractors' access to Information Assets or Sites must be the minimum necessary to achieve business purposes. Contractors must connect to Monmouthshire County Council network in a secured way. Monmouthshire County Council Contractors will be connected to the wifi by the IT Team. Contractors that breach Monmouthshire County Council's policies, procedures or contractual clauses will be subject to termination of contract or criminal proceedings if deemed appropriate.

1.16.2 On termination of contract, Contractors must immediately relinquish any assigned software licences and passwords to 3rd party systems and must alos return any Monmouthshire County 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, proximity cards, passes etc.; and

1.17 Remote Working / Mobile Devices

1.17.1 When working remotely users must make all reasonable efforts to secure data and assets of Monmouthshire County Council. Users must immediately report any incidents that involves loss, theft, or compromise of an asset or loss or corruption of data.

1.17.2 When working from home/remotely only print documents if there is a real business need – avoid printing sensitive business data on public printers. Printers have internal memory which will store a copy of the documents you print.

1.17.3 Monmouthshire County Council equipment should never be taken abroad unless you have sought approval from the SIRO, DPO and CISO.

1.18 Physical security

1.18.1 All visitors to Monmouthshire County 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 employees should -

- Information Assets should be stored in a locked area, cupboard or safe, out of plain sight, and protected from any physical damage when not in use.
- When using public transport or a car Monmouthshire County Council Information Assets must not be left unattended, and not left in plain sight.
- Tailgating – is the ability to enter a building without a access card by following someone through a door. Never allow someone to follow you - they *must* use their card
- Open windows - never leave windows open on the ground floor and any easily accessible area and always ensure windows are closed/locked at the end of your work session.
- Propping doors (inc fire doors) - never prop a door open, as this allows unrestricted access to different areas of the building. Access controlled doors are there to stop intruders and protect you as members of staff.
- Visitors - ensure all visitors sign in and out. Visitors should be escorted at all times

1.19 Compliance

1.19.1 If a User breaches this policy, Monmouthshire County Council reserve the right to:

- Restrict or terminate a 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 who might take legal action
- Take such other action as it deems appropriate, including under the **Disciplinary policy** up to and including dismissal.

2.0 Compliance with The Welsh language Scheme

2.0.1 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	**Head of Digital**
Department Responsible:	**The Digital Programme Office Monmouthshire County Council**
Links to other Policies/Procedure:	**Code of Conduct, Agile Working Policy, Remote Access Policy, Digital Media Policy, Data Protection Policy, Information Management policy, Information Strategy**
Policy Implementation Date:	**01/05/19**
Next policy review date:	**01/07/26**