Carmarthenshire County Council

Information Security Policy

Contents

1. Introduction

1.1 Information security management enables information to be shared, whilst ensuring the protection of information and hardware assets. It has three basic components:

- **Confidentiality:** protecting sensitive information from unauthorised disclosure or interception
- **Integrity:** safeguarding the accuracy of information
- **Availability:** ensuring that information is available to members, employees, outside bodies and the general public when required

1.2 The main objectives of the policy are to ensure:

- The Council's information assets and ICT equipment are adequately protected against any action that could have an adverse effect on the security of information.
- That all information assets must be "owned" by a named officer within the authority. The Council defines all Heads of Service as **Information Asset Owners.**
- That staff and elected members are aware and comply with all relevant legislation and council policies related to how they conduct their day-to-day duties in relation to ICT.

2. Scope

2.1 This policy is applicable to all information assets held by Carmarthenshire County Council. An information asset is defined as:

> *"an electronic or non-electronic asset owned or entrusted to the Council (by internal and external customers) and includes, but is not limited to, all hard copy documentation and electronic data held in our systems and databases."*

2.2 This policy applies to:

- All employees and elected members of the Council
- All employees and agents of other organisations who directly or indirectly support or use the Council's network
- All temporary staff directly or indirectly employed by the Council

- All persons carrying out work on behalf of the Council on a voluntary basis
- All users having access to systems, networks and ICT resources owned by the Council

3. Policy Statements

3.1 The Council will implement controls and practices to support the core concepts of Confidentiality, Integrity and Availability in order to prevent the loss or corruption of information assets and to reduce the risk of information being unavailable to the end-user.

3.1 The Council's information assets will be used in accordance with:

- This Information Security Policy
- Handling Personal Information Policy and Procedure
- Breach Reporting and Response Policy
- Email Usage and Monitoring Policy
- Internet Usage and Monitoring Policy
- Relevant legislation – including but not limited to the General Data Protection Regulation, the Data Protection Act 2018, the Computer Misuse Act 1990, the Freedom of Information Act 2000 and the Copyright, Designs and Patents Act

3.2 Any breaches of this policy may lead to disciplinary action being taken against those who fail to comply.

3.3 This policy is approved by, and has the full support of, the Council.

4. Responsibilities

4.1 Each member of staff is responsible for:

- Assisting in the protection of the Councils systems and equipment by complying with the security requirements contained in this document.
- Using all of the appropriate security measures and safeguards to protect application systems and data files, and making sure that personal or otherwise confidential information, whether electronic or paper based, is protected from theft, unauthorised disclosure/use, accidental loss and destruction.
- Not attempting to subvert or bypass any installed security mechanisms. This includes not sharing passwords; under no circumstances should users ever disclose their passwords to anyone or allow another user to share their credentials in order to overcome access controls.

- Following the Council's **Breach Reporting and Response Policy** when a suspected personal data breach occurs.
- On suspecting the presence of unauthorised use of Council equipment, a computer virus or cyber-attack, bringing the issue to the attention of the IT Helpdesk without delay.
- Ensuring that all Council data is stored on the council file plan or business system and not on the hard disk drive of the computer.
- Ensuring that portable devices and removable media are encrypted and are only used in exceptional circumstances and in accordance with the **Portable Device Usage Policy** and **Handling Personal Information Policy**.
- Ensuring that only authorised software runs on Council systems.
- Using only authorised devices on the Council's corporate network.
- ICT equipment must only be disposed of in a secure manner arranged by ICT Services.
- Ensuring that the Council's email system is used in accordance with the **Email Usage and Monitoring Policy**.
- Ensuring that any access to the internet is in accordance with the **Council's Internet Usage and Monitoring Policy**.
- Ensuring that personal data is dealt with in accordance with the Council's **Handling Personal Information Policy and Procedure**.
- Ensuring that they are aware of and understand all Information Governance Policies and associated guidance.

4.2 Line Managers are responsible for:

- Ensuring that their employees are aware of and observe all of the security requirements of the ICT equipment, facilities and data.
- Ensuring that their employees are aware of and observe all legal requirements concerning the use of proprietary software, e.g. respecting copyright and site licenses.
- Ensuring that employees for whom they have responsibility receive appropriate security awareness training, including material for legal requirements such as the General Data Protection Regulation (GDPR). Each line manager shall arrange training for each new employee and periodic training for all their personnel, to respond to changing procedures and legislation.
- Ensuring that on leaving the authority or transferring to another section, employees' access rights are reviewed and revoked when appropriate, and ICT equipment is returned

4.3 Heads of Service, as Information Asset Owners, are responsible for:

- The overall information security within their service area.

- Providing management support and resources for carrying out the requirements of this policy.
- Ensuring that all major applications systems and resources are identified and that a “System Owner” is appointed for each major application system.
- Ensuring compliance with all legal requirements concerning the use of commercial proprietary software e.g. respect of copyright and site licensing.
- Addressing security at the recruitment stage, ensuring that security requirements are included in job descriptions and employment contracts.
- Ensuring that potential recruits are adequately screened, especially for posts in sensitive areas such as social care.
- Ensuring that employees and third parties are aware that information is owned by the Council and should be treated as confidential, as unauthorised disclosure may result in disciplinary procedures or, in the case of third parties, a termination of contracts or association.
- Ensuring that users are provided with written authorisation describing their access rights and restrictions. For example, to permit access to an otherwise unpermitted resource of information.
- Providing resources and advice to ICT Services when responding to a personal data breach or security incident.
- Establishing business continuity plans to protect critical business processes from the effects of major failures or disasters. Procedures will be established to develop and maintain appropriate plans for the speedy restoration of critical business processes and services in the event of serious business interruptions.
- Business continuity planning to include measures to identify and reduce risks, limit the consequences should a breach be realised, and ensure speedy resumption of essential operations.
- Work with ICT Services to establish Business Continuity working zones where required by the service.
- Ensuring that procedures are in place to ensure continuity of services throughout the recovery period.
- All security issues including access permissions and security of manual information.
- Ensuring System Owners keep a register of system users to enable accurate access rights management.
- Ensuring that all system changes are formally documented through a change control procedure and reviewed to ensure that they do not compromise the security of either the system or the operating environment.

4.4 ICT Services are responsible for:

- Maintaining a schedule of all core servers, backup strategies and officers for effecting backup.

- Overseeing and coordinating cross-platform issues regarding computer security.
- Assisting system owners prior to award to any outside contractor, that their contract depends on compliance with all applicable security measures.
- Establishing procedures for the management of incidents of system and network intrusion and malicious software threats.
- Ensuring the security of all computers, including servers which support a system and its data and end user devices.
- Developing and maintaining contingency plans to include designated personnel to be responsible for effecting backup and recovery operations.
- Ensuring that ICT Services staff receive appropriate security awareness training.
- In collaboration with line managers, establishing and communicating the security safeguards required for protecting their application systems. This responsibility includes safeguards for hardware, software, communications and personnel.
- Identifying security requirements at the design stage of a system implementation. Appropriate security controls, including audit trails and fallback processing, will be designed into application systems. Additional countermeasures may be required for systems that process, or have an impact on sensitive, valuable or critical data.
- Evaluating security products and recommending solutions to multilevel security problems.
- Ensure a resilient and robust cyber-security strategy is in place
- Keep a record of network activity and access logs for use in investigating a breach or security incident for a period of 6 months
- Being aware of current security status of major systems and potential problems that may arise. This will include the commissioning of security certification tests, penetration tests and internal security audits.
- Awareness of and research into the value of new technological developments.

4.5 The Digital Security Officer:

Will oversee the implementation and monitoring of all IT security controls and also advise on the development of future strategies.

4.6 Human Resources

Security must be addressed at the recruitment stage and included in job descriptions, contracts and all induction courses. Job descriptions should define security responsibilities as laid down in the Council's Information Security Policy. This should include any general responsibilities for implementing or maintaining

the Council's Information Security Policy, as well as any specific responsibilities for the protection of particular systems or for the execution of security processes.

5. Access Control

5.1 User identification and authentication

Access to information assets must be restricted to authorised users and must be protected by appropriate controls.

These will include, but will not be limited to:

- Physical restrictions to Council buildings such as swipe card entry systems
- Robust authentication process to access the Council's network by validating user identity
- Enforcement of access permissions to electronic data, operating to the principle of least privilege

5.2 User access

Information Asset Owners must ensure that access to information assets are restricted according to the users' specific job function. Access must be based on the minimum privileges required to perform the function.

Users must only access information assets when they need to do so in order to fulfil their job role or specific task assigned to them. Intentional access to information assets outside of these situations is considered as being unauthorised and without the consent of the Council.

Unauthorised access to information is a breach of this policy and may result in disciplinary action being taken.

This may also constitute a breach of the General Data Protection Regulation and Computer Misuse Act 1990, and be reportable to the Information Commissioner and result in criminal prosecution of the user concerned.

5.3 Password management

All passwords used to access information assets must be kept confidential and be changed at regular intervals as per the password guidance below:

http://intranet/our-people/it-support/manage-your-password/.

5.4 Access termination, modification or revocation

Any changes to an individual's job function that affect their requirements for access to information must be noted by their line managers and reported to ICT Services immediately.

Users also have a responsibility to notify ICT Services and their line manager of any known conflict of interest that may arise, which would affect their job role and access to information.

Where staff leave the employment of the Council, including where employees are suspended, the Human Resources team will without undue delay ensure that the Council's ICT Services are notified to ensure that access permissions are terminated.

Line Managers are responsible for ensuring that system administrators of systems (e.g. Ohms, CareFirst etc) are notified to remove terminated/suspended access accounts.

5.5 Third Party Access

All third party access (contractors, business partners, consultants, vendors, customers) must be appropriately authorised and monitored. Third party access to information assets will be granted in increments of 6 months or less. In cases where access is needed for longer periods, the business owners must specify access timeframes and justification for such access.

5.6 Data Processors

Access by any third party to personal data to be processed on behalf of the Council will only take place after sufficient guarantees that the requirements of the General Data Protection Regulation are to be met and the rights of data subjects protected. The Processors must only act on the documented instructions of the Council, under a binding written contract (Data Processing Agreement). Service delivery by third parties must include agreed security arrangements, service definitions and service delivery agreements.

5.7 System monitoring

Access to and use of critical systems will be logged to detect non-compliance with the access control measures defined in this policy , and to record evidence in case of breaches/security incidents.

Records must be reviewed on a regular basis.

5.8 Audits

Periodic audits are to be performed within the Council to validate the levels of access and to ensure compliance.

6. Physical and environmental security

6.1 Secure areas

Any media, including ICT equipment, supporting sensitive information (e.g. personal information) must be based in secure areas. Physical protection from unauthorised access, damage and interference must exist (e.g. locked doors). These will be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security barriers (e.g. partition for desks/walls, card control entry, etc.).

6.2 Clear screen and clear desk

To ensure the security of information, desk and offices must be cleared of sensitive information (for example, personal information). Personal computer screens must also be clear of information when desk and offices are left unattended and should. Users should not leave themselves logged in to ICT equipment if it is left unattended.

7. Operational Security Controls

7.1 Documented operating procedures

To ensure the correct and secure operation of information processing facilities, procedures will be prepared for system activities such as, but not limited to, start up and shutdown, backups, recovery and maintenance.

7.2 ICT Equipment Asset Management

ICT Services keeps documentary evidence of all computer equipment and software. These records must be maintained for accuracy.

- Each inventory item must clearly identify each ICT asset by an identity tag detailing its unique asset number
- ICT equipment and software can only be purchased through ICT Services
- No equipment should be installed on the Council's network without prior consent of ICT Services
- All disposals of equipment must be done through ICT Services and recorded.

7.3 Change management

ICT Services will follow documented change control procedures to enable the identification and recording of significant changes. The procedure must consider planning and testing of changes, assessment of potential impacts, a formal approval procedure for proposed changes, communication of change details to relevant parties and back-out procedures.

7.4 Segregation of duties

Wherever practical and possible duties should be segregated. For example, the initiation of an event should be separated from its authorisation.

7.5 System planning and acceptance

To minimise the risk of system failures, controls will be implemented for capacity management and system acceptance.

7.6 Protection against malicious and mobile code

To protect against damage from malicious and mobile code such as computer viruses, the authority will implement systems and controls to prevent the execution of unauthorised code on systems. These controls include, but are not limited to, removal of administrative rights, endpoint anti-virus, email and internet filtering and Intrusion Prevention/Detection Systems at our internet gateway

7.7 Backup

Backups of critical data will be taken, recorded and tested to ensure that all essential information and software can be recovered following a disaster or media failure.

7.8 Network security management

IT Services will implement controls to ensure the security of information in networks and the protection of connected services from unauthorised access.

To ensure the secure installation, maintenance and use of WiFi access and, where there is a business need, approved Wireless networking equipment will be installed by ICT Services or approved third parties.

Wireless access to the corporate network will be restricted to corporate devices and require authentication.

Wireless networking equipment and management interfaces must be adequately secured to prevent unauthorised access.

Regular audits of wireless networks will be undertaken and any unauthorised access points will be removed.

7.9 Information systems acquisition, development and maintenance

Information Systems should not be acquired without the explicit consent from ICT Services to ensure that systems are safe, secure and compatible with our ICT Infrastructure. This includes operating systems, infrastructure, business applications, off-the-shelf products, services and user-developed applications that support the business process. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

8. Compliance measurement

Compliance with this Information Security Policy is mandatory

9. Sponsor

This Policy is owned by the Corporate Information Governance Group

10. Custodian

It is the responsibility of the Digital Security Officer to ensure that the policy is regularly reviewed and updated.

11. Ensuring equality of treatment

This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, age, gender, gender reassignment, sexual orientation and parental or marital status.

Policy approved by Executive Board:	22nd Oct 2018
Policy review:	22nd Oct 2020
Policy written by:	Richard R Williams & John M Williams (CISMP)