



Document Name: Information Security Policy

Approved by Council on: 24.10.2018

Reviewed by Council on: 24.11.2021

Next Review Date: 22.09.2026

Information Security Policy

Contents

1. Purpose
2. Scope
3. Policy statements
4. Implementation
5. Responsibilities
6. Physical and environmental security
7. Communications and operations management
8. Compliance measurement
9. Custodian
10. Ensuring equality of treatment

1. Purpose

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 following three aspects should be considered carefully in the working environment and procedures can be put in place to reduce the risk of insecure information:

- Physical Security can be increased by considering the layout of the working environment, for instance, placing filing cabinets away from easy access such as doorways, positioning computer screens appropriately so that they cannot be easily overlooked and, in some cases, considering CCTV
- Computer Security risks can be reduced, for example, by ensuring that password protected screensavers are utilised and ensuring that removable media (e.g., floppy disks, CDs, USB devices etc.) are not left unattended. Individual responsibilities are discussed later in this document
- Backup of electronically stored data is essential to good security

1.3 The main objectives of the policy are:

- To ensure that Llandeilo Town Council's assets, staff (permanent, temporary and contracted), councillors, data and equipment are adequately protected against any action that could have an adverse effect in relation to Information & Communications Technology (ICT) and the security of information
- To ensure that staff and councillors 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 held by Llandeilo Town Council whether held electronically or in paper format.

2.2 All users of the Council's ICT equipment are responsible for reading, understanding and complying with this policy.

2.3 This policy applies to:

- All employees and elected members (councillors) of the Council.
- All employees and agents of other organisations or volunteers who directly or indirectly support or use the Council's ICT resources.
- 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 views information security as a key to efficiency within day-to-day activities across the organisation. Any breaches of this policy may lead to disciplinary action being taken against those who commit any breach.

3.2 This policy is applicable to all information held by the Council whether held electronically or in paper format. All users of the Council's ICT equipment are responsible for reading, understanding and complying with this policy. In ensuring the security of information, the Council will adhere to all applicable laws and regulations.

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

4. Implementation

4.1 Asset management

The Council keeps documentary evidence of all computer equipment and software. It is the responsibility of the Operations Officer to ensure that these records are accurate and continuously maintained.

- 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 the Operations Officer.
- No equipment should be installed on the Council's network without prior consent of the Operations Officer.
- All disposal of equipment will be made by the Operations Officer and recorded. The Council actively supports a policy on recycling ICT equipment.
- An annual audit of ICT equipment should be carried out by the Operations Officer.
- ICT equipment must not be relocated or re-allocated without prior agreement with the Operations Officer.

4.2 Human resources

Security must be addressed at the recruitment stage and included in job descriptions, contracts and induction courses. Job descriptions should define security roles and 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. Responsibilities

5.1 The Operations Officer will:

Oversee the implementation and monitoring of all IT Security issues within this policy, and also advise on the development of future strategies.

5.2 Each member of staff is responsible for:

- Assisting in the protection of the Council's paper based and electronic data, 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 staff ever disclose their passwords to anyone. Each user will use login credentials unique to them.
- Informing the Clerk of the Council when a suspected breach of security is detected.
- Ensuring that all Council data is stored on the appropriate network drive or business system and not on the hard disk drive of the computer, or the storage device of a tablet or phone.
- Ensuring that portable devices and removable media holding personal or otherwise confidential information are suitably encrypted, stored and carried securely.
- On suspecting the presence of a computer virus, bringing the issue to the attention of the IT Helpdesk without delay.
- Ensuring that no Council computer is used for personal or any other improper purpose.
- Ensuring that they are aware of and understand all Information governance policies and associated guidance. Ensuring that the Council's email system is used in accordance with the Internet use, social media and electronic communication policy.
- Ensuring that any access to the internet is in accordance with the Council's Internet Use, social media and electronic communication policy.
- Ensuring that personal data is dealt with in accordance with the Data Protection Act. • Ensuring that only authorised software runs on Council systems.

5.3 Line Managers, in this case the Clerk, 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 in legal requirements such as the Data Protection Act. Each line manager shall arrange training for each new employee and periodic training for all their personnel, to respond to changing procedures and legislation. Each member of staff shall receive training at a level appropriate to their position that allows them to be aware of their security responsibilities and become proficient in the use of security systems required for the protection of automated and manual information systems, applications, and sensitive information (e.g. personal information).
- Ensuring that on leaving the authority or transferring to another section, employees' access rights are reviewed and revoked when appropriate.

6. Physical and environmental security

6.1 Secure areas

ICT equipment supporting sensitive information (e.g. personal data) must be based in secure areas. Physical protection from unauthorised access, damage and interference must exist (e.g. locked doors).

Approved by CTC 24.10.18, reviewed 24.11.21

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 data). Personal computer screens must also be clear of information when desk and offices are unattended. 'Locking' the computer screen will restrict unauthorised access to computer-based information.

7. Communications and operations management

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, startup and shutdown procedures, backups and maintenance.

8. Compliance measurement

8.1 Compliance with this Information Security Policy is mandatory.

9. Custodian

9.1 It is the responsibility of the Clerk of the Town Council to ensure that this policy is regularly reviewed and updated.

10 Ensuring equality of treatment

10.1 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, parental or marital status.

Approved by LTC _____