CYNGOR TREF
LLANFYLLIN
TOWN COUNCIL

IT INFRASTRUCTURE & INFORMATION SECURITY POLICY

DOCUMENT REFERENCE: LTC-19A V2

ADOPTED DATE: 24-MAR-2026

REVIEW DATE: MAR-27

Document Control

Version	Date	Notes
v2	2026	Full policy update including security, confidentiality, encryption and incident management

1 Introduction

Llanfyllin Town Council recognises the importance of secure, reliable and well-managed information technology systems in supporting the delivery of its services and the effective operation of the Council.

This policy establishes the framework for the safe use, management and protection of the Council's IT systems and information assets.

The Council must comply with statutory obligations including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004

All individuals who access Council systems share responsibility for maintaining information security and protecting Council data.

2 Scope

This policy applies to all councillors, employees, contractors, volunteers and authorised users who access Council IT systems or process Council information.

The policy applies whether systems are accessed from Council premises, remotely, or via authorised personal devices.

This includes:

- computers and laptops
- mobile devices and tablets
- cloud systems and online platforms
- network infrastructure
- data storage systems
- backups and archives

3 Information Security Principles

The Council will take appropriate and proportionate measures to ensure the confidentiality of information, the integrity of data and the availability of systems.

Users must ensure Council information is protected against unauthorised access, loss or theft, accidental disclosure and malicious damage or misuse.

4 Responsibilities

Maintaining effective information security is a shared responsibility.

- The Council is responsible for establishing governance and policy.
- The Town Clerk is responsible for implementation, oversight and incident reporting.
- Councillors, staff and authorised users must comply with this policy and handle information securely.

5 Password Management

Strong passwords must be used for all Council systems. Passwords be a minimum of 10 characters

- include upper and lower case letters, numbers, and special characters
- not be reused within the previous 12 passwords
- not contain easily guessable information
- Passwords must not be shared.
- Passwords must not be written down insecurely.
- Passwords must be changed immediately if compromise is suspected.
- Multi-factor authentication (MFA) must be used where available.

6 Access Control

Access to Council systems will be granted only where required for Council duties.

- Access is based on a need-to-know principle.
- Permissions will be reviewed periodically.
- Access must be removed promptly when individuals leave their role.
- Users must not attempt to access unauthorised systems or data.

7 Use of IT Equipment

All IT equipment supplied or owned by Llanfyllin Town Council remains Council property.

- Devices must be protected against loss or theft.
- Only authorised software may be installed.
- System configurations must not be altered without permission.
- Council equipment must not be used for unlawful activity.

Users must not

- install unauthorised software
- alter system configurations without permission
- access or distribute illegal or inappropriate material

8 Data Protection and Information Handling

All users must handle personal and confidential information in accordance with UK GDPR and the Data Protection Act 2018.

- Personal data must only be accessed where necessary.
- Information must be stored securely.
- Data must only be shared with authorised recipients.

8.1 Confidential Council Information

Confidential information includes, but is not limited to:

- matters discussed in confidential Council or committee sessions
- personal data relating to individuals
- financial, contractual or commercially sensitive information

Such information must:

- only be accessed on a need-to-know basis
- not be shared with unauthorised third parties
- not be forwarded to personal email accounts
- not be stored outside approved Council systems

Unauthorised disclosure of confidential information may constitute a data breach and will be subject to investigation and potential disciplinary action.

8.2 Encryption Requirements

Where information contains personal or confidential data, it must be protected using appropriate safeguards.

Encryption must be applied where data:

- contains personal or confidential information
- is stored on portable devices
- is transmitted externally

Where possible:

- secure systems should be used for sharing sensitive data
- email attachments containing sensitive data should be password protected
- printing of sensitive information should be restricted or avoided

9 Incident Reporting

Any suspected or actual information security incident must be reported immediately to the Town Clerk.

This includes:

- data breaches or accidental disclosure
- lost or stolen devices
- suspected cyber-attacks
- unauthorised system access

10 Incident Management

The Council will maintain an appropriate response to IT and information security incidents.

This includes:

- recording and assessing incidents
- taking steps to contain and mitigate risks
- restoring systems and data where necessary
- reporting incidents in accordance with legal and regulatory requirements
- communicating with relevant parties where appropriate

11 System Maintenance and Backups

Council IT systems will be maintained and updated to ensure reliability and security.

- Security updates will be applied as necessary.
- Backups are performed daily.
- Backups will be stored securely in our cloud hosting partner.
- Backup restoration will be tested periodically.
- Users must report faults or system concerns promptly.

The Council will periodically review backup arrangements and retention periods in line with operational and legal requirements. See LTC-18 for IT Data Retention Policies.

12 Third-Party Systems and Suppliers

Where external providers are used to store, process or manage Council data:

- Appropriate security measures must be in place.
- Data must only be processed in accordance with Council requirements.
- Access must be controlled and reviewed.
- Providers must comply with relevant data protection obligations.

13 System Monitoring and Access

All Council IT systems, email accounts and devices remain the property of Llanfyllin Town Council.

The Council reserves the right to:

- access Council systems where necessary
- investigate misuse or security concerns
- ensure continuity of Council business
- comply with legal or regulatory requirements

System use may be monitored for security, audit and compliance purposes.

14 Compliance

All users must comply with this policy.

Failure to comply may result in:

- removal of system access
- investigation under Council procedures
- further action where appropriate

15 Policy Review

This policy will be reviewed annually to ensure it remains effective, proportionate and compliant with legislation and best practice. All users must acknowledge and adhere to its provisions.