Loughton and Great Holm Parish Council

Information Technology (IT) Policy

Purpose

This policy sets out how Loughton and Great Holm Parish Council will use and manage its information technology (IT) systems to ensure they are secure, reliable, and used appropriately in support of council business.

The policy aims to protect council data and systems, ensure compliance with legal and regulatory requirements (including GDPR) and promote responsible and effective use of IT.

Scope

This policy applies to all councillors, employees, contractors and volunteers acting on behalf of the Council

It covers all IT systems and data, including computers, laptops, tablets, and mobile phones, email systems and cloud storage, the Parish Council website, social media platforms and any personal devices used for council business.

Acceptable Use

Council purchased IT systems must primarily be used for official council business.

Limited personal use is permitted provided as long as it does not interfere with council duties, does not incur any additional cost and does not breach this policy or any laws.

Users must not access, store, or share inappropriate or unlawful material, use council systems for political campaigning (unless formally authorised) or download or install unauthorised software

Email and Communications

Councillors and staff should use **official council email accounts** for all council business and we should bear in mind that council emails are considered official records and may be subject to FOI requests. Personal email accounts should not be used for council business.

Users must take care when opening attachments or links. avoid sharing sensitive information unless secure and maintain professional standards in all communications.

Data Protection and Security

All users must comply with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

Key principles detailed in these documents state that individuals must:

- Only access data necessary for your role
- Keep personal data secure and confidential
- Do not share data without proper authority
- Report any data breaches immediately to the Clerk

Sensitive information must be stored securely (password-protected where appropriate) and not be stored on personal devices unless necessary and secure

Passwords and Access

Strong passwords must be used and kept confidential. These Passwords must not be shared, devices should be locked when unattended and multi-factor authentication should be used where available

Use of Personal Devices (BYOD)

Where personal devices are used for council business they must be kept secure and password protected, Council data must be separated from personal data where possible and data must be deleted when no longer required.

Software and Updates

- Only authorised software may be installed on council devices
- Systems must be kept up to date with security updates
- Antivirus protection should be in place where applicable

Social Media and Website Use

Only authorised individuals may post on official council social media platforms. The Clerk and the Community Engagement Officer are currently authorised in this capacity.

Content must be accurate, appropriate, and non-political and personal opinions must not be presented as council views

Incident Reporting

All users must report the following immediately to the Clerk who is the Data Protection Officer.

- Suspected data breaches
- Lost or stolen devices
- Cybersecurity incidents (e.g. phishing emails)

Monitoring

The Council reserves the right to monitor use of its IT systems to ensure compliance with this policy and legal obligations.

Responsibilities

- **Clerk**: Overall responsibility for implementation and compliance
- **Councillors and users**: Responsible for adhering to this policy
- **Chair**: Oversight and governance

Review

This policy will be reviewed every 3 years or sooner if required due to changes in legislation or technology

Approved and Implemented: May 2026

Next Due for Review: May 2029