

Little Malvern & Welland Parish Council

IT & Data Governance Policy

Version	Date	Author	Changes Made	Approved By	Next Update
0.1	09/06/2026	Paul Riordan	Initial Draft		
0.2	14/06/2026	Paul Riordan	Updates following Councillor Comments		

1. Purpose

This policy sets out how Little Malvern & Welland Parish Council manages information technology, personal data and digital communication. It ensures compliance with UK GDPR, the Data Protection Act 2018, the Freedom of Information Act 2000, and NALC governance guidance. The Council does not routinely provide IT equipment; councillors therefore use their own devices.

2. Scope

This policy applies to all councillors, the Clerk/Responsible Financial Officer (RFO), volunteers, and contractors. It covers:

- Email and digital communication
- Storage and processing of personal data
- Use of councillors' personal devices
- Freedom Of Information compliance
- Cybersecurity
- Retention and disposal of information

3. Roles & Responsibilities

The Council

- Provides governance oversight
- Approves and reviews this policy annually
- Acts as Data Controller under UK GDPR

The Clerk

- Manages day-to-day information governance
- Maintains official records and retention schedules
- Coordinates FOI responses
- Ensures councillors understand their obligations

Councillors

- Use councillors' personal devices securely
- Protect council information

- Use official council email only
- Report data breaches or lost devices immediately (including councillors' personal devices holding council information such as WhatsApp messages and emails)

4. Use of Councillors' Personal Devices (BYOD)

Devices used for council business must have:

- Password, PIN, or biometric lock
- Up-to-date operating system and security patches
- Antivirus/antimalware (where applicable)
- Device encryption enabled (most modern iPhones, iPads and newer Macs are encrypted by default; older Macs may require FileVault)

Councillors must:

- Use the official council email account
- Avoid storing council documents in councillors' personal cloud accounts
- Not forward council emails to councillors' personal email addresses
- Report lost or stolen devices immediately

5. Email & Communication

All formal council business, and anything involving personal data, must be conducted using official council email accounts.

Councillors and the Clerk must not use councillors' personal email accounts for council business.

WhatsApp may be used for routine coordination and operational messages, provided no personal data or sensitive information is included.

SMS and social media may be used only for non-personal-data communication (e.g., "running late", "meeting moved", "please check your email").

Councillors must not delete emails relating to council business unless instructed under the retention schedule.

The Clerk maintains the official record of correspondence.

Volunteers and contractors (e.g., Sue and Barbara) must send emails to official council email addresses when communicating with the Council. Communication between volunteers themselves may use their normal methods unless personal data is being exchanged.

6. Data Protection & GDPR

Lawful basis

The Council processes personal data under:

- Public Task

- Legal Obligation
- Consent (only where explicitly required)

Storage

Personal data must be stored:

- In council-approved cloud storage
- On encrypted devices where possible but documents must be at least password or PIN protected
- In structured folders accessible to the Clerk

Sharing

Personal data must not be shared via:

- Councillors' personal email
- Social media
- Messaging apps (including WhatsApp) when the message contains personal data

Retention

The Clerk maintains the retention schedule. Councillors must not retain or delete data outside this schedule.

Data breaches

Any suspected breach must be reported to the Clerk immediately. The Clerk will determine whether the ICO must be notified within 72 hours.

7. Freedom of Information (FOI)

Council information held on councillors' personal devices may be subject to FOI disclosure.

Deleting information to avoid disclosure is unlawful.

The Clerk coordinates all FOI responses.

Councillors must forward relevant correspondence to the Clerk for filing.

8. CyberSecurity

The Council follows NCSC "Small Organisation Guidance", including:

- Strong passwords
- Multifactor authentication where available
- Regular software updates
- Avoiding public Wi-Fi for accessing council email or personal data where possible, use a VPN when using public Wi-Fi
- Public Wi-Fi may be used for posting public information (e.g., website updates, Facebook posts, newsletters)

- Reporting phishing attempts

9. Social Media

Councillors must:

- Not post personal data on social media without consent
- Not conduct council business via councillors' personal accounts
- Refer residents to official channels where appropriate

10. Use of Artificial Intelligence (AI) and AI Chatbots

Artificial Intelligence tools may assist with drafting text, summarising information, and improving efficiency. However, their use must be carefully controlled to protect personal data, maintain confidentiality, and ensure compliance with UK GDPR and council governance standards.

Permitted Use

AI tools may be used for:

- Drafting non-confidential documents
- Summarising publicly available information
- Improving clarity or structure of council documents
- Generating templates or administrative content

Use of AI must always be supplementary. Councillors and the Clerk remain responsible for the accuracy, legality, and appropriateness of all outputs.

Prohibited Use

AI tools must not be used for:

- Processing, storing, or entering personal data
- Drafting responses to individual residents that contain personal or sensitive information
- Uploading or pasting internal council documents that are not already public
- Handling confidential matters
- Making decisions or recommendations that should be made by the Council or Clerk

Data Protection and Privacy

When using AI tools, councillors and the Clerk must ensure:

- No personal data is entered into AI systems
- No confidential or unpublished documents are uploaded
- Outputs are checked for accuracy and bias
- AI-generated content is reviewed and approved before publication

11. Retention & Disposal

The Clerk maintains the master retention schedule.

Councillors should delete local copies of documents once the Clerk confirms they are archived.

Paper records containing personal data must be securely destroyed. Public documents (e.g., agendas, minutes) do not require shredding.

12. Compliance

Failure to comply with this policy may result in:

- Additional guidance being provided
- Referral to the Monitoring Officer
- Reporting to the ICO in the event of a data breach

13. Review

This policy will be reviewed annually or sooner if:

- There are major legislative changes
- The Council adopts new IT systems
- A data breach or FOI issue highlights a need for revision



20th July 2026