

Ufford Parish Council

Information Technology (IT) Policy

Adopted: 13th January 2026

Review date: January 2027

1. Purpose

This policy sets out how Ufford Parish Council manages and uses information technology to support its statutory functions. It aims to ensure that the council's use of IT is secure, proportionate, transparent, and compliant with data protection legislation and best practice for smaller authorities.

The policy should be read alongside the Council's Data Protection Policy

Data-Protection-Policy

and other governance documents.

2. Scope

This policy applies to:

- All councillors
- The Clerk
- Any volunteers or contractors with access to council information

It covers:

- Email communication
- Use of personal devices and email accounts
- Storage and handling of electronic information
- Website management
- Data security and breaches

3. Governance and Responsibility

The Clerk is responsible for the day-to-day management of the council's IT arrangements and acts as the Data Protection Lead.

Ufford Parish Council does not have a dedicated IT committee or sub-committee.

Overall responsibility for compliance rests with the full council.

4. IT Systems and Equipment

The council owns one laptop, used by the Clerk for council business.

The Clerk uses a Microsoft 365 account provided and managed by Peterborough City Council, which is subject to their security controls and policies.

Councillors do not have council-owned IT equipment or council email accounts.

5. Use of Email

i. Councillor Email Use

- Councillors use personal email addresses for council business.
- Councillors should only send and receive council business emails via the Clerk, unless expressly authorised.
- Councillors should not forward council emails to third parties without the Clerk's knowledge and authority.
- Reply-all should be used only where necessary and with care, ensuring no confidential or personal data is shared inappropriately.
- Councillors are reminded that emails relating to council business may be subject to Freedom of Information requests and data protection legislation, regardless of the email account used.

ii. Clerk Email Use

The Clerk conducts council business through their official Microsoft 365 email account.

Council records and correspondence are retained within the council's controlled systems in line with data protection and retention requirements.

6. Use of Personal Devices (BYOD)

Councillors and the Clerk may use personal devices (e.g. laptops, tablets, smartphones) for council business.

Devices must be:

- Password protected
- Kept up to date with software and security updates
- Used responsibly to avoid unauthorised access to council information
- Council information should not be stored unnecessarily on personal devices and should be deleted when no longer required.

7. Website and Digital Publishing

The council website is managed solely by the Clerk.

Councillors do not have login access to the website or other digital publishing platforms.

All published information must comply with the Transparency Code for Smaller Authorities and data protection requirements.

8. Data Protection and Security

All personal data is processed in accordance with the UK GDPR and the Data Protection Act 2018.

The council follows the principles and procedures set out in its Data Protection Policy.

Reasonable technical and organisational measures are in place to protect data from loss, misuse, or unauthorised access.

9. Data Breaches

A data breach includes any incident resulting in the loss, unauthorised access to, or disclosure of personal data.

Any councillor or officer who becomes aware of a potential data breach must inform the Clerk immediately.

The Clerk will assess the breach, take appropriate mitigation action, and record it.

Where required, breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours and affected individuals informed in line with legal requirements.

10. Training and Awareness

The Clerk undertakes GDPR and data protection training as required.

Councillors are expected to familiarise themselves with this policy and the council's Data Protection Policy.

Guidance will be provided to councillors where necessary to support compliance.

11. Monitoring and Review

This policy will be reviewed annually or sooner if there are changes to legislation, guidance, or the council's working arrangements.

Any significant changes will be approved by the full council.

This policy was adopted by Ufford Parish Council on [insert date].

—