

BOLNEY PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) POLICY

Version: 1 Adopted: Tuesday 21st October

1. Purpose

This policy sets out how Bolney Parish Council manages and secures its information technology (IT) systems and data. It ensures;

- The security and integrity of Council information.
- Compliance with UK GDPR and the Data Protection Act 2018.
- Responsible and consistent use of IT systems by councillors and staff.

2. Scope

This policy applies to the Clerk using the council-owned laptop and the nine councillors, who use their own personal computers to access Council information, .gov.uk email addresses and any associated digital storage.

3. Responsibilities

The Council

- Provide and maintain one secure, up-to-date laptop for the Clerk.
- Provide secure cloud-based storage for Council data (Google Workspace).
- Ensure the Council device has anti-virus protection, encryption, and regular updates.

The Clerk

- Use the Council-owned laptop for official council related activities and tasks. Personal use should be limited and should not interfere with Bolney Parish Council work responsibilities.
- Keep passwords confidential and change them regularly.
- Report any IT incidents or suspected data breaches to the Chair immediately.

Councillors

- Use personal devices responsibly when accessing Council information.
- Keep devices updated and protected with anti-virus software.
- Use Council-provided email accounts for all official business.
- Avoid storing Council documents on personal devices, unless they are available publicly on the Council website. Use the Council's approved cloud storage.
- Report any data loss or breach promptly to the Clerk.

4. Data Storage and Backup

- All Council documents must be stored with the approved cloud system.

- The Clerk will perform regular backups (at least monthly).
- No confidential or personal data should be permanently stored on personal devices.

5. Security and Passwords

- All users must use strong passwords (mixed case, numbers, and symbols).
- Devices must lock automatically after inactivity.
- The Clerk's laptop must be encrypted and password protected.
- Passwords must be changed if compromise is suspected.

6. Software and Updates

- Only licensed and authorised software may be used on the Council laptop.
- Councillors must ensure their personal computers are updated regularly
- Installation of software on the Council Laptop must be authorised by the Council.

7. Email and Communication

- All Council business must be conducted using official Council email accounts.
- Personal email addresses must not be used for Council matters.
- Emails and Documents must not be shared externally unless authorised.

8. Data Protection and Confidentiality

- All users must comply with the Council's **Data Protection Policy** and **Privacy Notice**.
- Personal data must be handled lawfully, securely, and only for legitimate Council purposes.
- Confidential information (including HR, legal, or financial data) must not be disclosed outside the Council.

9. Incident Reporting

- Any data breach, equipment loss, or IT incident must be reported to the Clerk immediately.
- The Clerk will assess and, if necessary, report serious breaches to the Information Commissioner's Office (ICO) within 72 hours.

10. Review

This policy will be reviewed annually, or sooner if there are significant IT or staffing changes, or relevant guidance from NALC, SLCC, or the ICO is updated.