BIRDINGBURY PARISH COUNCIL
Information Technology & Data Policy

Status	Adopted 21.09.26
Version	2.0
Date Prepared	2026
Review Due	Annually
Policy Owner	The Clerk

1. Introduction

Birdingbury Parish Council recognises the importance of effective, secure, and lawful use of information technology (IT) in supporting its operations and communications. This policy sets out the obligations and responsibilities of all those who use the Council's IT resources or handle its data.

This policy reflects current best practice, including the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and guidance from the National Cyber Security Centre (NCSC). It supersedes any earlier version.

2. Scope

This policy applies to all councillors, the Clerk, any employees, volunteers, and contractors who access or process Birdingbury Parish Council data or use IT resources in connection with Council business. It covers:

- Personal devices used for Council work (Bring Your Own Device – BYOD)
- Email accounts and communication platforms
- Cloud storage and document management
- Internet and network access
- Passwords and account security
- Data handling, retention, and disposal
- Incident reporting and disaster recovery

3. Acceptable Use

Council IT resources and data must only be used for official Council business. Limited and incidental personal use is permitted provided it does not:

- Interfere with Council duties or responsibilities
- Involve accessing, creating, or distributing offensive, illegal, or inappropriate content
- Compromise the security or reputation of the Council
- Breach copyright, intellectual property rights, or any applicable law

Users must not use Council data or IT resources to conduct personal business, solicit, advertise, or engage in political activities unrelated to Council duties.

4. Bring Your Own Device (BYOD)

As the Council does not currently provide dedicated hardware, the Clerk and councillors may use personally owned devices (computers, tablets, smartphones) for Council work. The following requirements apply to all such devices:

4.1 Device Security Requirements

- Devices must be protected by a strong password, PIN, or biometric lock
- Operating systems and applications must be kept up to date with security patches
- Reputable antivirus/anti-malware software must be installed and kept current
- Device encryption must be enabled where the operating system supports it (e.g. BitLocker on Windows, FileVault on macOS)
- Automatic screen lock must be enabled after a short period of inactivity

4.2 Data Handling on Personal Devices

- Council data should not be stored permanently on local device drives; use approved cloud storage (see Section 5)
- If Council data is temporarily held on a device, it must be deleted securely when no longer needed
- Personal devices used for Council work must not be shared with other household members without taking precautions to prevent unauthorised access to Council data

4.3 Lost or Compromised Devices

- If a device used for Council work is lost, stolen, or compromised, the Clerk must be notified immediately
- Where possible, remote wipe or account revocation steps should be taken without delay
- The incident must be logged and assessed for potential data breach notification obligations under UK GDPR

5. Email Communication

Email is the primary means of formal Council communication. The following standards apply:

5.1 Council Email Accounts

Where council email addresses are provided (e.g. clerk@birdingburyparishcouncil.gov.uk or equivalent), these must be used for all official Council correspondence. Personal email accounts should not be used to conduct formal Council business where a Council address is available.

5.2 Email Standards

- Do not forward Council emails to personal accounts unless strictly necessary and in compliance with this policy

- Be vigilant against phishing: verify the sender before opening attachments or clicking links; if in doubt, do not open

5.3 Email Monitoring

The Council reserves the right to monitor email communications conducted on Council accounts to ensure compliance with this policy and relevant legislation. Monitoring will be conducted proportionately and in accordance with the Data Protection Act 2018 and UK GDPR.

6. Cloud Storage and Software

The Clerk currently uses Microsoft 365 (Word, Excel, and cloud storage via OneDrive/SharePoint) for Council work. The following applies:

- Council documents and records must be stored in the approved cloud platform, not solely on local device storage
- Access to cloud accounts must be protected by a strong, unique password and multi-factor authentication (MFA) where available
- Sharing permissions on cloud-stored documents must be reviewed regularly; documents should not be shared publicly unless specifically intended for publication

7. Data Protection and UK GDPR Compliance

Birdingbury Parish Council is a Data Controller under the Data Protection Act 2018 and UK GDPR. All users who handle personal data on behalf of the Council must comply with the following principles:

7.1 Data Protection Principles

- Personal data is processed lawfully, fairly, and transparently
- Data is collected for specified, explicit, and legitimate purposes only
- Only the minimum necessary personal data is collected and held (data minimisation)
- Data is kept accurate and up to date
- Personal data is not retained longer than necessary (see Section 9)
- Personal data is kept secure against unauthorised access, loss, or destruction

7.2 Data Subject Rights

Individuals have rights under UK GDPR, including the right to access their data, correct inaccuracies, and in some cases request erasure. Any request relating to personal data held by the Council should be directed to the Clerk without delay.

7.3 Privacy Notices

The Council must maintain an up-to-date Privacy Notice describing what personal data it holds, why, and how individuals can exercise their rights. This should be published on the Council's website or made available on request.

7.4 Data Sharing

Personal data must not be shared with third parties without a lawful basis for doing so. Where data is shared with contractors or service providers, an appropriate data processing agreement must be in place.

8. Data Retention and Disposal

Council data must be retained in accordance with the retention schedule recommended by the National Association of Local Councils (NALC) and the Information and Records Management Society (IRMS) Local Government Classification Scheme. Key principles:

- Documents and records must not be kept longer than necessary for their purpose
- Emails should be reviewed regularly; irrelevant or time-expired emails should be deleted
- Personal data must be securely deleted when no longer required – simply deleting a file is not sufficient; use secure deletion tools or overwrite methods
- Paper records containing personal data must be shredded
- The Clerk is responsible for maintaining a basic record of what data the Council holds and for how long

9. Password and Account Security

- All accounts used for Council work must be protected by a strong, unique password
- A strong password is typically at least 12 characters and includes a mix of letters, numbers, and symbols; alternatively, a three-word passphrase approach (as recommended by the NCSC) may be used
- Passwords must not be shared with any other person
- Multi-factor authentication (MFA) must be enabled on all accounts where it is available, including email and cloud storage
- Passwords must be changed immediately if there is any suspicion of compromise
- Use of a reputable password manager is encouraged to manage multiple unique passwords securely

10. Network and Internet Usage

The Council does not operate its own network. Users access the internet via their own home or mobile connections. The following precautions apply:

- Avoid conducting Council business on public or unsecured Wi-Fi networks (e.g. in cafes or libraries) where possible unless using a VPN
- Home routers used for Council work should be kept updated with current firmware
- Do not use Council credentials on shared or public computers

11. Security Incident Reporting

A security incident includes any actual or suspected: unauthorised access to data, loss or theft of a device containing Council data, phishing attack, malware infection, or accidental disclosure of personal data.

11.1 Reporting Procedure

- Any suspected incident must be reported to the Clerk immediately
- The Clerk will assess the incident and determine whether it constitutes a personal data breach requiring notification to the ICO
- Under UK GDPR, reportable breaches must be notified to the ICO within 72 hours of the Council becoming aware
- Where a breach is likely to result in a high risk to individuals, those individuals must also be notified without undue delay
- All incidents must be documented, including details of what occurred, what data was affected, and what steps were taken

12. Disaster Recovery and Business Continuity

Although the Council is a small organisation, it is important to ensure that operations can continue following a significant IT failure or data loss event.

12.1 Data Backup

- Council data stored in Microsoft 365 / OneDrive benefits from automatic cloud backup; the Clerk should verify that version history and recycle bin features are enabled

12.2 Recovery Planning

- If the Clerk's primary device or account becomes unavailable, the Council Chair or a nominated councillor should have sufficient access (or knowledge of how to recover access) to critical accounts and data to maintain essential communications
- Account recovery options (e.g. backup email addresses, recovery codes) must be recorded securely and kept up to date
- The Clerk should maintain a brief IT register noting key accounts, services used, and recovery contacts – this should be stored securely and separately from the accounts themselves

13. Social Media and Online Presence

Where the Council uses social media or a website to communicate with residents:

- Only authorised users (as agreed by the Council) may post on behalf of the Council
- Content must be accurate, appropriate, and in keeping with the Council's public role
- Personal data of residents or councillors must not be published online without consent
- Account credentials for Council social media accounts must be held securely and not tied solely to a personal account; handover arrangements must be in place

14. Training and Awareness

The Council will ensure that the Clerk and all councillors receive appropriate guidance on IT security and data protection. This includes:

- Awareness of this policy and their responsibilities under it

- Basic cyber security awareness (phishing, password hygiene, safe browsing)
- UK GDPR awareness relevant to their role

Free resources are available from the National Cyber Security Centre (ncsc.gov.uk) and the ICO (ico.org.uk). The Clerk should draw these to the attention of councillors as relevant guidance is updated.

15. Compliance and Consequences

All users are expected to comply with this policy. Failure to do so may result in:

- Withdrawal of access to Council IT systems or data
- Disciplinary action in accordance with the Council's disciplinary procedures
- In serious cases, referral to relevant authorities

The Council takes its obligations under UK GDPR seriously. Deliberate or reckless mishandling of personal data may constitute a criminal offence and could expose both the individual and the Council to regulatory action by the ICO.

16. Policy Review

This policy will be reviewed annually, or earlier if required by changes in legislation, technology, or Council practice.

17. Related Documents and References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- NCSC Cyber Essentials guidance – ncsc.gov.uk
- ICO guidance for local councils – ico.org.uk
- NALC / SLCC Data Protection guidance for parish and town councils

— End of Policy —