BUCKLAND PARISH COUNCIL

Buckland Parish Council, Village Hall, New Road, Buckland, HP22 5JB
Tel. 01296 630962
email: clerk@buckland-pc.gov.uk www.buckland-pc.gov.uk

Review	Date	Amendments
Adopted by Full Council	**February 2026**	

Information Technology (IT) Policy

1. Introduction

Buckland Parish Council relies on information technology (IT) to carry out its business efficiently and securely. This policy sets out how the council manages and protects its IT systems, in compliance with the 2025 Practitioners' Guide, UK GDPR, the Data Protection Act 2018, and relevant accessibility standards.

The policy also aims to protect council systems, digital assets, and reputation from cyber threats, misuse, and security breaches.

2. Scope

This policy applies to all councillors, employees, volunteers, and other authorised users who access or use the council's IT systems, devices, email, documents, or communications, regardless of their working location or pattern, including those who are home based, office based or work on a flexible part time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

IT resources include:

- Council-owned desktops, laptops;
- Council email accounts
- Cloud-based systems and shared digital storage
- Council website and social media accounts
- Personal devices used under Bring Your Own Device (BYOD) provisions

3. Roles and Responsibilities

Clerk: Acts as the Data Protection Officer (DPO) and IT lead, responsible for:

- Granting and rescinding access to council systems
- Liaison with IT providers

- Ensuring data protection and IT security compliance

IT Provider (Cloudy IT):

- Provides secure IT support, system maintenance, updates, and backups

Councillors, Staff, and Other Users:

- Must comply with this policy
- Report technical issues, security concerns, or breaches to the Clerk immediately

4. Council IT Equipment

4.1 Use of Council Devices

- Council-owned devices (laptops, desktops) are for council business only. Personal use is strictly prohibited.
- Devices must be treated with care; any damage or loss should be reported immediately to the Clerk.
- Devices must be locked when not in use.
- Equipment must not be dismantled, modified, or used to install non-council software.

4.2 Portable Equipment and Security

- Portable devices must be securely stored when not in use.
- Laptops and tablets must be encrypted, and mobile devices must be PIN-protected.
- Multi-factor authentication (MFA) must be enabled where possible.
- Lost or stolen devices must be reported to the Clerk immediately.

5. Bring Your Own Device (BYOD)

- Personal devices may only be used to access council systems via a secure web browser.
- No files, apps, or council data may be downloaded to personal devices unless explicitly authorised.
- Personal devices must be password-protected and not shared with others.
- Council data must be kept separate from personal data using dedicated apps or storage areas.

6. Passwords and Authentication

- Strong passwords are required for all council accounts, following NCSC guidance (e.g., three random words).
- MFA is mandatory for email and cloud-based systems where supported.
- Passwords are personal and must not be shared.
- All default passwords must be changed upon first use.
- Administrative credentials are only accessible to authorised personnel and stored securely.
- A back up copy of passwords are given to the Chair of Buckland Parish Council in a signed and sealed envelope. These should only be opened by the chair and one other councillor in extreme emergency.

7. Email Use

- All council business must use official council email accounts.
- Personal email accounts are strictly prohibited for council business.
- Council emails must not be forwarded to personal accounts.
- Councillors must copy the Clerk on all email correspondence related to council business.

8. Internet Use

- Internet access via council devices or BYOD must be for council purposes only.
- Downloading illegal or copyrighted material is prohibited.
- Users must not access sites that could compromise the council's reputation.

9. Social Media

- Only authorised users may post on council social media accounts.
- Personal social media use must not bring the council into disrepute.
- Councillors and staff must adhere to the Council's Code of Conduct and Social Media Policy.
- Content related to council business or events must not disclose confidential information.

10. Cybersecurity

- All council devices must have up-to-date antivirus, firewall protection, and software updates.
- Suspicious emails, attachments, or links must be reported to the Clerk immediately.
- Council data must be backed up regularly to secure cloud storage or encrypted devices.

11. Remote Working

- Council data must not be left unattended when working outside the office.
- Public Wi-Fi may only be used with a secure VPN.
- Screen privacy filters should be used where confidential information may be visible.
- Documents must be returned to council systems; no local storage of council data is permitted.
- Devices should be secured and encrypted during travel or when working offsite.

12. Data Protection and Security

- All council data is processed in accordance with UK GDPR and the Data Protection Act 2018.
- Sensitive or confidential documents must never be stored on personal devices unless authorised.
- Access to council systems is granted on a need-to-know basis.

13. Data Breaches

13.1 Reporting

- Any suspected breach must be reported immediately to the Clerk.

13.2 Investigation

- The Clerk will investigate breaches within 72 hours, documenting:
  - Date and time of breach
  - Type and extent of data affected
  - Cause of the breach
  - Actions taken to mitigate risk

13.3 Notification

- If a breach risks individuals' rights or freedoms, the ICO must be notified within 72 hours.
- Affected individuals will be informed promptly if risk is high.

13.4 Remediation

- Lessons learned will inform updated policies, training, and technical safeguards.

14. Training

- All councillors, staff, and authorised users receive induction training on IT security and data protection.
- Refresher training will be provided as required.

15. Policy Review

- This policy will be reviewed annually or sooner if legislation, council systems, or technology practices change.

Appendix A – Approved Systems

- Email and file storage: Microsoft 365 or council-approved cloud services
- IT provider Cloudy IT
- Supported access: Web browser (Edge, Chrome, Firefox, Safari – latest versions)
- Backup: Secure cloud storage or encrypted drives

Appendix B – Security Standards

- MFA enabled for all accounts
- Council data not stored locally on personal or council devices without authorisation
- Council laptops/devices strictly for council business only
- Passwords must follow NCSC best practice and be changed if compromised