Berryfields Parish Council

IT and Information Security Policy

1. Introduction

Berryfields Parish Council recognises that information, digital systems, and IT equipment are critical assets. Protecting them ensures service continuity, legal compliance, and the safeguarding of personal data.

This policy sets out the mandatory rules for councillors, employees, and contractors in line with:

- UK GDPR and the Data Protection Act 2018
- Freedom of Information Act 2000 (FOIA)
- Local Government Transparency requirements
- The Procurement Act 2023 and related regulations
- National Association of Local Councils (NALC) good practice guidance.

2. Objectives

- Preserve Confidentiality, Integrity, and Availability of information
- Protect Council IT assets from theft, misuse, or damage
- Ensure compliance with date protection, procurement, and employment law
- Promote resilience, accountability, and public trust.

3. Scope

This policy applies to:

- All councillors, employees, (permanent, temporary, or casual), and contractors
- All Council-owned or personal devices used for Council business
- All premises, information systems, and cloud platforms used for council work.

4. User Responsibilities

- All users are personally responsible for safeguarding Council data and IT equipment
- Users must comply with this and all related council policies (e.g. Data Protection, Data Retention, Social Media, Disciplinary Rules)
- Misuse of IT systems may result in disciplinary or legal action.

5. Acceptable Use

- IT facilities are provided for Council business. Limited personal use is permitted if it does not interfere with duties, security, or reputation
- Prohibited use includes bypassing security, installing unauthorised software, accessing offensive/illegal material, or using systems abusively
- Emails and texts must be professional and may be disclosable under FOI or Data Protection law.

6. Access Control & Authentication

Users must use strong passwords, enable multi-factor authentication where available, and ensure accounts are unique and disabled when users leave.

7. Device and Asset Protection

All Council-owned equipment must:

- Be locked or shut down when unattended
- Be taken home or secured in a locked office overnight
- Be recorded against a serial number in the Council's asset register

8. Office and Physical Access

Offices containing confidential data or IT equipment must be locked when unoccupied and visitors must not be left unsupervised where confidential information is accessible.

9. Cloud Systems, Storage & Backup

All cloud accounts must use appropriate access controls and permissions must be reviewed periodically. Sensitive folders are accessible only to authorised staff.

10. Business Continuity & Disaster Recovery

- The Clerk/RFO will maintain a Business Continuity Plan (BCP) covering:
  - Loss of IT systems (email, website, finance)
  - Cyberattack or ransomware
  - Loss of key personnel

11. Data Retention & Disposal

- All information must be managed in line with the Council's Data Protection Policy and Data Retention Policy
- Personal confidential data must be securely stored, retained only as long as necessary, and securely destroyed (e.g. shredding paper, secure digital deletion).

12. Social Media & Online Participation

- Users must not disclose personal or confidential information without authorisation
- Personal views expressed online must be clearly identified as such, not official Council policy
- Social media use must remain professional, lawful, and consistent with Council values.

13. Training & Awareness

- All councillors and staff must complete annual cyber security training, covering phishing, password hygiene, and device security
- Refresher sessions will be arranged as needed.

14. Monitoring

- The Council reserves the right to monitor use of its IT systems, internet, and email, where there is a legitimate business reason
- Monitoring will always be proportionate and lawful, and staff will be made aware.

15. Incident Reporting

All users must immediately report to the Clerk (or Chair if Clerk unavailable):

- Suspected data breaches or security incidents
- Lost or stolen equipment
- Malware infections or unauthorised access attempts

The Clerk will log, investigate, and report incidents, and notify the ICO if required.

16. Governance & Review

- The Parish Clerk has overall responsibility for policy implementation and compliance
- The policy will be reviewed annually by full council, or earlier if legislation or risks change
- Compliance will be evidenced in the Annual Governance Statement (Assertion 10).

Document History

Approved and adopted	May 2021	(version 1)
Reviewed by the Clerk	June 2023	(version 1)
Reviewed and amended by Deputy Clerk/checked by Clerk	September 2025	(version 2)

Policy reviewed and updated to incorporate NALC IT Policy Guidelines, reflect new legislation (UK GDPR, Data Protection Act 2018, Procurement Act 2023), and include updated best practice on IT security and governance.

Approved by Parish Council	September 2025