Brympton Parish Council
Serving our community

Clerk: Julie Ferguson **E-mail:** clerk@brymptonparishcouncil.gov.uk **Tel:** 01935 571008

Adopted: April 26
Review: Annually

1. Purpose
   This policy sets out how Brympton Parish Council manages its digital systems, information, and communication tools to ensure security, transparency, and compliance with legal responsibilities.

2. Who and what this policy applies to.
- Councillors
- The Clerk **(designated authorised user)** and Council staff.
- Contractors and volunteers using council systems.
- All devices, software and digital services used for Council business.

3. IT Governance
- The Clerk is responsible for day-to-day IT management and liaising with external IT providers.
- The Council will ensure appropriate budget provision for IT maintenance, upgrades, and cybersecurity.
- All IT purchases must be approved by the Council and comply with procurement procedures.

4. Acceptable Use
- Council IT systems and devices must be used only for official Council business.
- Personal use of Council devices is discouraged and must not compromise security or data integrity.
- Users must not install unauthorised software or access inappropriate content.
- All communications via Council email or social media must be professional and in line with Council values and the Nolan Principles.

5. Email and Communication
- All council business must be conducted using official council email addresses.
- Personal email accounts must not be used for council matters.
- Email passwords must be strong and changed regularly.

6. Data Protection
- All personal data must be handled in accordance with the UK GDPR and Data Protection Act 2018.
- The Clerk is the designated Data Protection Officer (DPO) and responsible for ensuring compliance.
- Personal data must be stored securely on council-approved systems and only accessed by authorised user.
- Data breaches must be reported immediately to the Clerk and documented.

7. Website and Accessibility
- The council website must comply with WCAG 2.2 AA standards.
- Required documents and information must be published and kept up to date.
- The Clerk will be responsible for website management and regular checks.

8. Cybersecurity
- All devices used for council business must have up-to-date antivirus software and security updates.
- Devices must be password-protected and updated regularly.
- Two-factor authentication should be enabled wherever possible.
- Councillors and staff must report any suspicious emails or IT issues immediately (to DPO).
- Access to sensitive data and systems must be restricted to authorised users.
- Remote access must be secured via VPN or encrypted connections.

Clerk: Julie Ferguson **E-mail:** clerk@brymptonparishcouncil.gov.uk **Tel:** 01935 571008

9. Social Media and Public Communication

- **Authorisation:** The Clerk and Chair serve as the sole authorised publishers for official Council accounts. All content must be approved by the Clerk or the Chair to ensure that it accurately reflects the formal Council decisions and adopted policies.
- **Official Voice:** Posts are restricted to factual, Council-related information. Personal opinions, political commentary, or unofficial advocacy by members or staff are strictly prohibited on official platforms.
- **Broadcast only:** The Council's social media presence is a **non-interactive broadcast channel.** To ensure transparency and reliable record-keeping, the Council does not monitor "comments," "tags," or "direct messages" (DMs).
- **Official Correspondence:** Social media is not a platform for public inquiry or formal grievance. All official correspondence, questions, or feedback must be directed to the **Clerk via email**, which remains the sole medium for documented Council communication.

10. Backups and Disaster Recovery

- The Council uses real-time cloud backup via Microsoft Onedrive, which can be accessed via another device if necessary in a disaster recovery situation.

11. Training and Review

- Councillors and staff are encouraged to attend training on IT security and data protection at least every 3 years.
- This document shall be kept under review and updated as necessary, at least annually.