Brightling Parish council

INFORMATION TECHNOLOGY (IT) POLICY

Adopted March 2026
Review Annually

---

1. Purpose

This policy sets out how Brightling Parish Council manages its use of information technology (IT), including email, to support its work and communications. It helps to ensure the council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

This policy applies to all individuals who use Brightling Parish Council's IT resources, including computers, networks, software, website, data, email and cloud-based systems and accounts.

3. Governance and Oversight

The Clerk is the designated Data Protection Officer (DPO) and IT Systems Administrator working in conjunction with the council member with responsibility for the website.

4. Data Protection & Security

All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as set out in the council's data protection policy available on the council website.

All data collection, processing, and subject rights are governed by the council's Privacy Policy, available on the council website.

4.1 Access and Storage: Data is stored securely, with access granted only to authorised personnel based on necessity. Personal data will be retained in accordance with the council's Document Retention Scheme and securely deleted when no longer needed. See separate Document Retention Policy.

4.2 Security Controls:

4.2.1 Strong password protection with multi-factor authentication should be used for systems where possible. Users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security and should be

unique to the BPC systems – users must not use logins associated with non-council systems.

4.2.2 Regular security updates and anti-malware software are required on all council-owned and personal devices and backups of essential data must be stored in a secure location. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary

4.3 Access Control: when staff or members leave the Council, the Clerk (or instructed council member) will stop access to all council systems for the leaving person. This includes changing login details / passwords and freezing any email account(s) and access to council systems (including cloud storage and website admin). All council owned IT hardware must be returned securely on the last day with the council. If a personal device has been used for council business all council data must be removed.

5. Acceptable use of IT resources

Brightling Parish Council IT resources and email accounts are to be used for official council-related activities and tasks only. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Councillors and staff may use personal devices for council business only if explicitly authorised and subject to compliance with this policy. This includes the use of council-owned domain-based email and access to the council's accounting system and website administration. 2-factor or multi-factor authentication is required where supported.

Data Separation: Council data must be kept separate from personal data using dedicated apps or storage areas.

Where possible, authorised devices, software, and applications will be provided by Brightling Parish Council. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

6. Use of Email

Gov.uk email accounts provided by Brightling Parish Council to councillors and the clerk are for official communication only. Confidential or sensitive information must not be sent via email unless encrypted / password protected. Attachments and links should be handled with caution – users should try and verify the source before opening any attachments or clicking on links.

The use of personal email accounts for council business is prohibited. All council correspondence must be conducted through official council-provided email

addresses. Council emails must not be shared or forwarded outside of approved data areas, such as forwarding to a non council-owned domain or personal email.

Email Retention: All council emails will be stored in compliance with the GDPR, DPA and Freedom of Information requirements.

7. Data Breach Protocol

The Parish Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR and DPA requirements.

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

7.1 Actions to take following a data breach:

a. Immediate Notification: Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer).

b. Initial Response: The Clerk in consultation with Council will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA). Technical fixes or security upgrades will be prioritised to prevent recurrence

c. Investigation: A full investigation will be conducted by the Clerk within 72 hours of the breach being discovered. The breach will be logged, including:

- Date and time of breach
- Type of data affected
- Cause and extent of the breach
- Actions taken to address the breach

d. Reporting: If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours. If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay.

8. Monitoring and Compliance

All council-owned hardware will be recorded on the asset register. All devices must be regularly updated and checked for compliance with this policy along with

recommended software updates and both strong password with multi-factor authentication enabled where possible. Any breaches of this policy will be investigated, and appropriate measures taken in line with the council's disciplinary or governance procedures. Councillors and staff will be offered regular training on IT systems, cybersecurity, data handling, and transparency responsibilities.

Review: This policy will be reviewed annually, or sooner if legislation changes.