BETCHWORTH PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

Adopted by Council on 1st September 2025

1. Purpose and Scope

This policy sets out the expectations and responsibilities for the use of Information Technology (IT) and communication systems within Betchworth Parish Council.

Who does this policy apply to?

This policy applies to:

- All employees (permanent, temporary, and contract)
- Elected members (Councillors)
- Volunteers
- Contractors and third-party users granted access to council systems

2. Equipment and Systems Covered

This policy covers the use of all IT and communication equipment and services provided or supported by the Parish Council, including:

- Desktop and laptop computers
- Internet access and broadband connections
- Remote access tools (VPN, remote desktops)
- Email systems and webmail
- File storage (local and cloud)
- Telephones and mobile phones
- Council websites and social media
- Printers, scanners, and other peripherals

3. Responsibility for the Policy

The Parish Clerk is responsible for:

- Monitoring and reviewing the IT Policy annually
- Providing advice and training to staff and councillors
- Enforcing compliance and investigating potential breaches

4. Related Policies

This policy should be read alongside the following policies:

- General Data Protection Policy
- Social Media Policy
- Records Retention Policy

5. Monitoring

The Parish Council reserves the right to monitor the use of its IT and communication systems. This includes, but is not limited to:

- Internet usage
- Emails sent and received
- Phone call logs

Monitoring will only be carried out for legitimate reasons such as security, legal compliance, or policy enforcement. Staff using council devices for personal purposes must be aware that usage may still be monitored.

6. Password Management

- Passwords must be a minimum of 8 characters and include upper and lowercase letters and numbers.
- Passwords must not be shared except with the Parish Clerk in specific authorised situations (e.g. absence or emergency access).
- If a password is suspected to be compromised, it must be changed immediately and reported to the Clerk.
- If password-protected documents are emailed, passwords must be sent via a separate channel (e.g., by phone).

7. Computer and System Usage

- All computers must be shut down at the end of each working day.
- Users must lock their screen or log out when away from their desk.
- Files must be saved in designated folders accessible for regular backups.
- If in areas accessible to the public, screens must be locked when unattended, and sensitive documents secured.
- As well as cloud back up storage provided by designated 3rd party, an off site backup will be provided to the Chair at month end via approved USB device.

8. Bring Your Own Device (BYOD)

It is understood that Personal devices are required for the functioning of the Parish Council by Elected members (Councillors), Volunteers, Contractors and third-party users granted access to council systems

These devices must:

- Have up-to-date antivirus software

- Use secure passwords or biometric locks
- Not store council data locally (Provision for cloud storage has been made)

9. Data Protection (See also General Data Protection Policy)

All staff must comply with the UK GDPR and Data Protection Act 2018. This means:

- Only collecting personal data where lawful and necessary
- Storing data securely (password protection, encryption)
- Disclosing data only to authorised parties
- Retaining data only as long as needed
- Disposing of data securely (e.g., shredding paper, deleting digital files)

Failure to comply may result in disciplinary action and legal consequences.

10. Mobile Phone Use and Texting (see also Social Media Policy)

Text messaging may be used for urgent, work-related communication, but should:

- Avoid abbreviations or slang
- Never include illegal, discriminatory, or offensive content
- Be treated with the same care as email or letters
- Not be used to share confidential information

11. Email Use

- Council email should be used for all official communication.
- Emails must be professional, respectful, and accurate.
- Staff must not use council email to enter into contracts or agreements without proper authority.
- Phishing or suspicious emails should be reported and not opened or replied to.

12. Internet Use

- Internet access is for work purposes only, with reasonable limited personal use permitted outside working hours.
- Access to inappropriate, offensive, or illegal content is strictly prohibited.
- Use of chat rooms, messaging services, or personal blogs during work time is not permitted.

13. Software

- Only authorised software may be installed on council devices.
- Downloading or installing software without the Clerk's permission is prohibited.
- Regular updates must be installed promptly to maintain system security.

14. Training and Support

- All new staff and councillors will receive basic IT and information security training during induction.
- Ongoing guidance is available from the Parish Clerk.
- Refresher training may be provided when policies are updated or when needed.

15. Misuse of IT Systems

Misuse of IT systems may lead to disciplinary action. Examples of misuse include:

- Breaching this policy
- Attempting to guess or steal passwords
- Accessing or distributing offensive or illegal content
- Circumventing security systems
- Installing unapproved software
- Leaving devices unattended in public places
- Using IT systems for bullying, harassment, or discrimination

16. Policy Review

This policy will be reviewed **every 2 years** by the Parish Clerk or earlier if significant changes to legislation or technology occur.

End

Clerk to Betchworth Parish Council Email: clerk@betchworth-pc.gov.uk

Disclaimer: Hardcopies of this document are considered uncontrolled. For the latest version please refer to www.betchworth-pc.gov.uk

Next Review September 2028