BICKLEIGH PARISH COUNCIL
INFORMATION TECHNOLOGY (IT) POLICY
Adopted by Bickleigh Parish Council: March 2026
Review Date: March 2027

1. Introduction

The purpose of this Information Technology (IT) Policy is to ensure that all councillors, employees, contractors and volunteers using Bickleigh Parish Council's IT systems and equipment understand their responsibilities and use Council technology securely, lawfully and appropriately.

The policy is designed to:

- Protect the Council's information and systems from unauthorised access, misuse, loss or damage;
- Ensure compliance with relevant legislation including the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Freedom of Information Act 2000 and Copyright legislation;
- Promote safe and efficient use of Council IT resources;
- Reduce cyber security risks to the Council.

2. Scope

This policy applies to:

- All Parish Councillors;
- Employees and contractors;
- Volunteers acting on behalf of the Council;
- Any third party given access to Council systems or data.

The policy covers:

- Computers and laptops;
- Mobile phones and tablets;
- Email systems;
- Cloud storage and shared drives;
- Websites and social media accounts;
- Printers and removable media;
- Internet access and Wi-Fi;
- All Council-owned data and records.

3. Acceptable Use

Council IT equipment and systems are provided for official Council business.

Limited personal use may be permitted provided that it:

- Does not interfere with Council duties;
- Does not incur additional cost to the Council;
- Does not breach security requirements;
- Is lawful and appropriate.

Users must not:

- Access, store or distribute offensive, discriminatory or illegal material;
- Use Council systems for political campaigning;
- Download unauthorised software;
- Circumvent security measures;
- Share confidential information without authority;
- Use another person's login credentials.

4. Passwords and Access Security

All users must:

- Use strong passwords containing a combination of letters, numbers and symbols;
- Keep passwords confidential;
- Not share passwords with others;
- Change passwords if compromise is suspected;
- Enable multi-factor authentication where available.

Devices should be locked when unattended.

Access to Council systems shall only be granted where necessary for Council duties.

5. Email Use

Council business should only be conducted through authorised Council email accounts.

Users must:

- Take care when opening attachments or clicking links;
- Be alert to phishing or scam emails;
- Avoid sending personal or confidential information unless necessary and secure;
- Use professional and respectful language.

Emails relating to Council business may constitute official records and may be subject to Freedom of Information or Subject Access Requests.

6. Data Protection and Confidentiality
All users must comply with UK GDPR and the Data Protection Act 2018.

Personal data must:
• Be processed lawfully, fairly and transparently;
• Only be used for legitimate Council purposes;
• Be kept secure;
• Not be retained longer than necessary.

Confidential information must not be shared with unauthorised individuals.

Paper records containing sensitive information should be securely stored and shredded when no longer required.

7. Remote Working and Personal Devices
Where personal devices are used for Council business:
• Devices must be password protected;
• Security software and updates must be maintained;
• Council information must be deleted when no longer required;
• Users must take reasonable precautions to prevent unauthorised access.

Where possible, Council business should be undertaken using Council-issued devices and email accounts.

8. Software and Updates
Only authorised software may be installed on Council devices.

All devices must:
• Have up-to-date antivirus protection;
• Install security updates promptly;
• Use supported operating systems and software.

Users must not disable security settings or install unapproved applications.

9. Backup and Storage
Important Council files must be stored in approved locations and backed up regularly.

Where cloud services are used, they should:
• Be reputable and secure;
• Comply with UK data protection requirements;
• Restrict access to authorised users only.

Critical records should not be stored solely on individual devices.

10. Social Media and Website Use
Only authorised persons may publish content on behalf of the Council.

Content published online must:
• Be accurate and lawful;
• Respect confidentiality and copyright;
• Not bring the Council into disrepute.

Official Council social media accounts remain the property of the Council.

11. Incident Reporting
Any suspected security breach, phishing attempt, data loss or unauthorised access must be reported immediately to the Parish Clerk.

Incidents may include:
• Lost or stolen devices;
• Malware or ransomware attacks;
• Accidental disclosure of personal information;
• Suspicious emails or login activity.

Where necessary, the Council will report breaches to the Information Commissioner's Office (ICO).

12. Monitoring
The Council reserves the right to monitor use of its IT systems where lawful and proportionate in order to:
• Maintain security;
• Investigate misuse;
• Ensure compliance with this policy.

Monitoring will be carried out in accordance with relevant legislation.

13. Training

Appropriate IT and cyber security awareness training will be provided periodically to councillors and staff.

Users are expected to keep themselves aware of current cyber security risks and guidance.

14. Breaches of Policy

Failure to comply with this policy may result in:

- Withdrawal of access to Council systems;
- Disciplinary action;
- Referral to law enforcement authorities where appropriate.

15. Policy Review

This policy shall be reviewed every two years or sooner if legislation, technology or Council procedures change.

Approved by: Bickleigh Parish Council

Signed: _____

Position: Chair / Clerk

Date: _____