Bovingdon Parish Council

Parish Council Office
Memorial Hall
High Street
Bovingdon
Herts HP3 0HJ

Tel: 01442 833036
Email: office@bovingdonparishcouncil.gov.uk
Website: www.bovingdonparishcouncil.gov.uk

Information Technology Policy

Contents

Bovingdon Parish Council

Parish Council Office
Memorial Hall
High Street
Bovingdon
Herts HP3 0HJ

Tel: 01442 833036
Email: office@bovingdonparishcouncil.gov.uk
Website: www.bovingdonparishcouncil.gov.uk

1. Introduction

Bovingdon Parish Council ("the Council") recognises the importance of effective and secure information technology and this policy outlines how the Council manages, protects and uses its information technology systems.

It aims to ensure that all IT resources are used securely, efficiently and lawfully, supporting the Council's operations and obligations under data protection and transparency legislation.

2. Scope

This policy applies to:

- All staff, councillors, volunteers and contractors who use the Council's IT equipment, systems or data.
- All hardware, software, email, and digital platforms provided or managed by the Council, including those hosted by Microshade and other approved providers.
- Any personal devices used to access Council systems or data.

3. Responsibilities

The Parish Clerk is responsible for ensuring compliance with this policy and for reporting breaches to the Council or the Data Protection Officer (DPO) as appropriate.

Councillors, employees, and volunteers must use IT systems responsibly, maintain confidentiality, and follow security guidance.

Microshade is responsible for providing and maintaining the Council's secure hosted environment, including data backup, firewall protection and user authentication. Microshade are also responsible for maintaining software, ensuring updates, and providing technical support as required.

4. Acceptable Use

Council IT systems must be used **only for legitimate Council business**. Users must:

- Use Council email addresses (e.g. @bovingdonparishcouncil.gov.uk) for all official correspondence.

Parish Council Office
Memorial Hall
High Street
Bovingdon
Herts HP3 0HJ

Tel: 01442 833036
Email: office@bovingdonparishcouncil.gov.uk
Website: www.bovingdonparishcouncil.gov.uk

- Keep login details confidential and never share passwords.
- Lock or log out of devices when unattended.
- Use only authorised software and Council-approved cloud storage.
- Avoid accessing, storing or distributing any inappropriate or unlawful material.
- Not use Council IT for personal gain, political activity, or private business.

Limited personal use of Council devices may be permitted, provided it does not interfere with Council work, security, or system performance.

5. Data Management and Security

The Council stores and processes personal data in compliance with the **UK GDPR** and **Data Protection Act 2018**.

- All data and documents must be stored on the **Microshade hosted platform**, not on local or personal drives.
- Data must not be copied to personal devices, USB sticks or unapproved storage systems.
- Only authorised users may access the hosted environment.
- Confidential data must never be shared via personal email or unencrypted channels.
- Any suspected data breach must be reported immediately to the Parish Clerk.

The Council's IT systems are backed up daily by **Microshade**, with backups stored securely in line with their data protection protocols.

6. Passwords and Access Control

Passwords must contain at least 12 characters and a mix of upper/lowercase letters, numbers and symbols. They must not be shared or reused across personal accounts.

Two-factor authentication (2FA) must be enabled for access to Microshade and Office 365 accounts.

Accounts will be disabled immediately when a user leaves the Council or no longer requires access.

7. Email and Communication

- All official Council correspondence must be sent using Council email accounts.

Parish Council Office
Memorial Hall
High Street
Bovingdon
Herts HP3 0HJ

Tel: 01442 833036
Email: office@bovingdonparishcouncil.gov.uk
Website: www.bovingdonparishcouncil.gov.uk

- Emails should be written professionally and comply with the Council's Code of Conduct and Data Protection Policy.
- Users must be cautious of phishing emails and avoid clicking on suspicious links or attachments.
- Personal or sensitive information must only be sent using secure and encrypted email methods
- All emails and documents are potentially subject to Freedom of Information (FOI) and Data Subject Access requests.

8. Remote Working and Access

The Council recognises the need for flexible and remote working.

- Remote access is provided through Microshade's secure hosted platform and authorised connections only.
- Users must ensure that home or remote devices have up-to-date antivirus software and are password-protected.
- Council data must not be downloaded to or stored on personal computers.

9. Software and Equipment

- All software must be properly licensed and installed only by authorised personnel.
- Automatic updates and security patches must be enabled at all times.
- Council-owned devices (desktops, laptops, printers, etc.) remain the property of the Council and must be returned when no longer required.
- Installation of personal software or applications is strictly prohibited due to security concerns.
- Equipment faults must be reported promptly to the Parish Clerk or IT provider.

10. Social Media and Internet Use

- Use of Council social media accounts must comply with the Council's Social Media and Communications Policy.
- Users must not post or share content that could damage the Council's reputation or disclose confidential information.
- Access to the internet must be for Council related activity only.
- Streaming, gaming or other high-bandwidth activities unrelated to Council business are prohibited.

Parish Council Office
Memorial Hall
High Street
Bovingdon
Herts HP3 0HJ

Tel: 01442 833036
Email: office@bovingdonparishcouncil.gov.uk
Website: www.bovingdonparishcouncil.gov.uk

11. Monitoring and Compliance

The Council reserves the right to monitor its IT systems to ensure compliance with this policy, prevent misuse, and safeguard data. Any misuse of IT systems may result in disciplinary action and, if necessary, referral to law enforcement.

Compliance with this policy will be reviewed periodically in line with internal audit requirements.

12. Incident Reporting

All IT-related incidents, including security breaches, system failures, or suspected cyberattacks, must be reported immediately to:

- The **Parish Clerk**, and
- **Microshade**

An incident log will be maintained, and serious incidents will be reported to the Council and, if required, to the **Information Commissioner's Office (ICO)** within 72 hours.

13. Policy Review

This policy will be reviewed at least **every two years**, or earlier if there are significant changes to legislation, technology, or Council operations.