

Burton Dassett Parish Council

Information Technology Policy

Update Schedule

	Adoption date
Adopted by Burton Dassett Parish Council	18 th May 2026
Next review due May 2027	

1. Purpose

This policy sets out how Burton Dassett Parish Council, “Parish Council” will use and manage its Information Technology (IT) systems and information.

It aims to:

- Protect Council data and equipment.
- Support Councillors and staff in carrying out their roles.
- Ensure compliance with relevant laws, including data protection.

2. Scope

This policy applies to:

- All Councillors and staff who use Parish Council computers, email accounts, cloud storage, or other IT resources.
- Any personal devices used for Council business (e.g. laptops, tablets, or phones).

3. Acceptable Use

- Parish Council IT systems and accounts must only be used for Council business.
- Personal use of Parish Council-provided equipment should be minimal and must not interfere with Council work.
- Inappropriate, offensive or unlawful activity is strictly prohibited.

4. Data Protection and Confidentiality

- Councillors and staff must handle all personal data in line with UK GDPR and the Data Protection Act.
- Councillors and staff must comply with the Data Protection Policy.
- Confidential information must not be shared outside the Council unless authorised.
- Personal devices used for Council business must be secured with a password or PIN.

5. Email and Communication

- Parish Council email accounts must be used for all Council business.
- Emails must be written professionally and treated as public records.
- Care must be taken not to open suspicious links or attachments.

6. Security

- Strong passwords must be used.
- Devices must be locked when unattended.
- Antivirus and software updates must be kept up to date.
- Cloud services or online storage must be approved by the Council.

7. Social Media and Website

- Only authorised Councillors or staff may post on the Council's website or social media accounts.
- Posts must reflect official Council decisions and maintain a professional tone.
- Personal opinions should not be posted from Council accounts.

8. Backup and Records

- Important Council documents must be stored in the official shared drive or approved system.
- Regular backups must be taken to prevent data loss.
- Records must be retained and disposed of in line with the Council's Document Retention Policy.

9. Breaches and Reporting

- Any suspected IT security breach (e.g. lost device, data leak, hacking attempt) must be reported to the Clerk immediately.
- The Council will investigate breaches and take appropriate action.

10. Review

This policy will be reviewed annually or when significant changes in technology or legislation occur.