Corscombe Halstock and District Parish Council

IT and Cyber Security Policy

1. Introduction

This policy sets out the standards for the secure, lawful, and effective use of information technology (IT) and email systems by Corscombe, Halstock and District Parish Council. Its aim is to protect council data, ensure continuity of operations, and promote responsible use of digital resources. It covers acceptable use, security, data management, password safety, email monitoring, training, and compliance for all users.

2. Scope

This policy applies to all individuals who use Corscombe, Halstock and District Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

The authority endeavours to provide digital devices but acknowledges that some councillors may be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Acceptable use of IT resources and email

Corscombe, Halstock and District Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it

- does not interfere with council duties
- does not incur cost to the council
- does not breach this policy or any applicable law

All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

- Where possible, authorised devices, software, and applications will be provided by Corscombe, Halstock and District Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns. Installation of unauthorised software on council devices is prohibited. Personal devices used for council work must have up-to-date security patches, antivirus protection, and password/biometric access controls.

IT Governance

- The Clerk is responsible for day-to-day IT management and liaising with external IT providers.
- The Council will ensure appropriate budget provision for IT maintenance, upgrades, and cyber security.
- All IT purchases must be approved by the Council and comply with procurement procedures.

5. Data management and security

All sensitive and confidential Corscombe, Halstock and District Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Data Protection and Privacy

- All personal data must be handled in accordance with the UK GDPR and Data Protection Act 2018.
- The Clerk is the designated Data Protection Officer (DPO) and responsible for ensuring compliance.
- Personal data must be stored securely and only accessed by authorised personnel.

- Data breaches must be reported immediately to the Clerk and documented.

6. Network and internet usage

Council network and internet access must be used responsibly and for legitimate council purposes. Users must not:

- Corscombe, Halstock and District Parish Council's network and internet connections should be used responsibly and efficiently for official purposes.
- Downloading and sharing copyrighted material without proper authorisation is prohibited. Attempt to bypass security controls
- Engage in activities that compromise network performance or security

7. Email communication

Email accounts provided by Corscombe, Halstock and District Parish Council are for official communication only.

Emails should be professional and respectful in tone.

Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Corscombe, Halstock and District Parish Council 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.

Multi-factor authentication (MFA) should be used where available.

9. Mobile devices and remote work

Mobile devices provided by Corscombe, Halstock and District Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Corscombe, Halstock and District Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR and be proportionate and lawful.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Users should regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

13. Training and awareness

Corscombe, Halstock and District Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on

- Cyber security
- data protection
- safe email practices
- updates to IT systems or procedures

All councillors and staff must participate in mandatory training.

14. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

16. IT related enquiries or assistance

Clerk and councillors are responsible for the safety and security of Corscombe, Halstock and District Parish Council's IT and email systems. By adhering to this IT and Email Policy, Corscombe, Halstock and District Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

This policy was adopted at a meeting on 8th April 2026, minute reference 8.4.26 and will be reviewed every year.

Related Parish Council Documents:

Data Protection and Privacy Notice

General Data Protection Regulatory Policy

Press and Media policy