Charsfield Parish Council

IT and Cyber Security Policy

This policy was adopted by the Council at its meeting held on the 29th September 2025.

Contents

1. Introduction

Charsfield Parish Council has a duty to ensure the proper security and privacy of its computer systems and data. All users are responsible for protecting these assets.

The Parish Clerk is responsible for implementing and monitoring this policy.

2. General Principles

The Parish Clerk and all members should remain vigilant about cybersecurity threats. Suspicious activity or emails should be reported to the Parish Clerk. Users should never share passwords via email and should be cautious of odd or inconsistent language in communications.

All users must comply with the council's Data Protection & Information Management Policy.

Council devices must have up-to-date antivirus software, which must not be disabled.

Unauthorised use, modification, or interference with computer systems or data breaches this policy and may also be an offence under the Computer Misuse Act 1990.

Only properly licensed software may be installed on council devices.

3. Training and Guidance

The Parish Clerk will receive appropriate cybersecurity training to suit the duties of the role.

Members will be provided with a basic overview of cybersecurity measures when they join and may receive further guidance if required.

4. IT Policy Parish Clerk:

- The Parish Clerk will either be assigned a council email address for official correspondence.

- Limited personal use of council IT is permitted, provided it does not interfere with council duties.

- The Parish Clerk is responsible for safeguarding any council devices, data, or systems under their control.

Members:

- Members will be issued council email addresses for all council-related communications (preferred) or alternatively must create and use an email address dedicated to their Charsfield Parish Councillor role, which is separate from their personal email.

- Emails relating to council business are considered council data and may be subject to disclosure under the Data Protection Act or Freedom of Information Act, even when sent from personal accounts.

- Incoming emails to member accounts must be stored per the Data Protection and Information Management Policy.

- Members not using webmail should configure email clients to retain copies of sent messages on the server.

- When using social media in a personal capacity, members must make it clear they are not representing the Parish Council.

- Members must follow the Council's Code of Conduct when using social media.

- Personal devices used to access council systems must be password-protected and accessible only by the member.

5. Websites and Social Media

The Parish Clerk shall ensure that the council website is accurate, up-to-date, and secure.

Council social media accounts may be managed by the Parish Clerk and, where applicable, by the Chair of the Council.

Posts on council-operated social media must remain non-political, factual, and in the interests of the parish.

Creation of new websites or social media accounts for council use requires Parish Clerk approval.

6. Password Protection

All council systems must be secured with passwords.

Two-factor authentication should be enabled where possible.

Unattended devices must be locked or require password re-entry.

Passwords must:

- Be at least eight characters long

- Include uppercase and lowercase letters, a number, and a special character

Generic/shared accounts should be avoided.

Access credentials must not be shared between users.

Unique passwords should be used across different systems and devices.

Passwords should be changed periodically.

Passwords must not be written down or stored in unsecured locations.

7. Portable Devices

All mobile devices (phones, tablets, laptops) used for council business must be protected using passcodes, passwords, or biometric locks.

Passwords and passcodes must be strong and not easily guessed.

Two factor authentication should be used where possible.

Removable media (such as USB drives) must be encrypted or password protected when containing sensitive council data.

8. Incident Reporting

Any incidents that may compromise council data or systems must be reported to the Parish Clerk without delay.

This includes:

- Lost or stolen devices

- Phishing attempts

- Shared or compromised passwords

- Suspected unauthorised access

9. Misuse of IT

Misuse of IT systems is prohibited and may result in disciplinary or legal action.

Misuse includes but is not limited to:

- Accessing, creating or sending offensive or inappropriate content

- Sending defamatory or infringing material

- Distributing spam or malware

- Interfering with others' data or work

- Changing system settings without permission

- Using council devices for gaming during work-related activities

Unauthorised access to or distribution of council systems, data or information is strictly prohibited.