CAPEL PARISH COUNCIL

IT and Cyber Security Policy

Using Council systems, email, devices and information safely

Status	Final	**Policy owner**	Parish Clerk
Adopted	November 2026	**Minute reference**	Item 18, 16/11/2026
Last reviewed	November 2026	**Next review**	November 2027
Review cycle	Annual	**Applies to**	Councillors, employees, volunteers and contractors using Council systems or information

1. Purpose and scope

This policy protects the Council's information, money and reputation from loss, error, fraud and cyber-attack. It applies to everyone who uses Council email, accounts, websites, devices or information, including on personal devices. It supports the Information Governance Policy, the Financial Regulations (sections 2.7, 7.9 to 7.12) and the Staff Handbook. For employees it forms part of the standards set out in their contract of employment.

2. Responsibilities

- **The Council** approves this policy, funds proportionate security and receives a short report on incidents at least once a year.
- **The Clerk** is the system owner. The Clerk keeps the list of approved systems and users, arranges back-ups, updates and leaver removal, and records incidents. IT support is provided by Helpdesq.
- **Every user** follows this policy, completes the induction briefing and an annual refresher, and reports problems at once.

3. Accounts and access

- Everyone uses their own account. Never share a login or password.
- All councillors use a Council email address (for example name@capel-pc.gov.uk) for Council business. Personal email must not be used. Emails cannot contain councillors' personal opinions unless that is clarified in the text of the email.
- Use long, unique passwords (three or more random words) and a password manager. Turn on **multi-factor authentication** wherever it is offered, and always for email, the website, banking and the accounting package.
- Access is limited to what each person needs. The Clerk removes a leaver's or former councillor's access, and recovers devices and records, within one working day.

4. Devices

- Council-owned devices are preferred for staff.

- Personal devices may be used only if they have a screen lock, up-to-date software, encryption switched on, and no Council files saved locally (use the approved cloud storage). The Council may require remote wiping of Council data from a lost device.
- Do not use devices running software that no longer receives security updates.
- Lock your screen when away. Take care with public Wi-Fi (use a VPN or your mobile data).
- Report a lost or stolen device to the Clerk immediately.

5. Email and internet

- Use Council email for Council business only, with limited, reasonable personal use by staff that does not interfere with work.
- Do not send or store unlawful, discriminatory, offensive or defamatory material.
- Check recipients and attachments before sending. Use "bcc" when recipients should not see each other's addresses. Do not set up automatic forwarding to a personal account.
- Be alert to phishing. Do not click unexpected links or open unexpected attachments; do not approve unexpected sign-in prompts.
- Emails are Council records and may have to be disclosed under the Freedom of Information Act or as personal data.

6. Software, services and payments

- Use only approved systems (Council email and storage, the accounting package named in the Financial Regulations, online banking). New systems or apps need the Clerk's approval and a data protection check.
- Online banking must be done on a secure, up-to-date device, with no remembered passwords, and with two authorised people for every payment (Financial Regulations section 7).
- Never change a supplier's bank details because of an email or call. Check using a known phone number and follow Financial Regulations 7.9.

7. Artificial intelligence (AI) tools

- Do not enter personal data, confidential information or draft decisions into public AI tools or chatbots.
- Only AI tools approved by the Council (after a data protection check) may be used with Council information.
- AI output must be checked for accuracy, bias and copyright. The person who uses it remains responsible for the document.
- Do not record or transcribe meetings with AI tools unless the Council has agreed this and told attendees.

8. Protecting data

- Keep software, apps and operating systems up to date; install critical security updates promptly (within 14 days).
- Use anti-virus and firewalls. Encrypt laptops, phones and removable media.
- Back up essential records regularly to a separate location and test restoring them at least once a year.
- Store Council records only in approved places. Paper records are kept locked away.
- Wipe and securely dispose of old devices.

9. Website, domain and social media

The Clerk and one other named person hold the administrator access to the website, domain name and official social media accounts, with multi-factor authentication. The website is kept accessible and up to date. See the Communications and Social Media Policy.

10. Cyber incidents

Report any suspected incident (phishing click, lost device, odd account activity, ransomware, unexpected payment request) to the Clerk at once, or to the Chair if it involves the Clerk.

1. Disconnect the affected device from the network and do not delete anything. Do not pay any ransom.

2. The Clerk records the incident, changes passwords, and contacts IT support, the bank and insurers if needed.

3. If personal data may be involved, the data protection officer is told and the ICO is informed within 72 hours where required (see the Information Governance Policy).

4. Report fraud to Action Fraud (and the police if it is urgent).

11. Monitoring and privacy

The Council may check use of its systems where it is lawful, necessary and proportionate (for example to investigate a breach). Users will be told what is monitored in the Privacy Notices.

12. Training, insurance and review

The Clerk gives new councillors and staff a short IT briefing and an annual refresher. The Council reviews its cyber insurance cover each year and will consider working towards Cyber Essentials certification [CONFIRM]. This policy is reviewed annually.

13. Breaches of this policy

Serious or repeated breaches by employees may be dealt with under the Disciplinary Procedure in the Staff Handbook. Breaches by councillors may be a breach of the Code of Conduct.