CAWTHORNE PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) POLICY

Document Control

Title	**Information Technology (IT) Policy**
Policy Owner	The Clerk to the Council
Approved by	Cawthorne Parish Council
Version	1.0
Adoption Date	5th March 2026
Minute Reference	Minute No 197
Review Date	March 2027 (or earlier if legislation or guidance changes)

---

1. Policy Statement

Cawthorne Parish Council recognises that effective management of information technology is essential to the efficient operation of the Council and the protection of public information.

This policy establishes the standards for the secure use, management and governance of the Council's information technology systems and digital information.

The Council is committed to:

- protecting Council information and personal data;
- maintaining secure and resilient IT systems;
- complying with all relevant legislation;
- supporting the requirements of the Annual Governance and Accountability Return (AGAR), including Assertion 10;
- promoting good cyber security practices.

---

2. Scope

This policy applies to:

- all elected members;
- the Clerk and Responsible Financial Officer;
- employees;
- contractors or volunteers who have authorised access to Council information.

It covers:

- Council email accounts;
- computers and mobile devices;
- cloud storage;
- electronic documents;
- websites;
- social media;
- software;
- internet access.

---

3. Relevant Legislation

This policy should be read alongside:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Act 1972
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990

---

4. Roles and Responsibilities

Full Council

The Council shall:

- approve this policy;
- review it annually;
- ensure adequate resources are available for secure IT provision;
- include cyber security within the Council's Risk Management arrangements.

Clerk

The Clerk is responsible for:

- implementing this policy;
- maintaining user accounts;

- ensuring secure storage of Council information;
- reporting cyber incidents where appropriate;
- maintaining software licences and subscriptions.

Councillors

Councillors must:

- comply with this policy;
- use Council systems responsibly;
- protect confidential information;
- report any suspected security incidents immediately.

---

5. Council Email

Cawthorne Parish Council provides councillors and officers with official Council email addresses using the Council's **.gov.uk domain**.

These accounts shall be used for all official Council business.

Personal email accounts must not be used for Council correspondence except in exceptional circumstances authorised by the Clerk.

Council email accounts shall:

- remain the property of the Council;
- be protected by strong passwords;
- use Multi-Factor Authentication where available;
- not be shared with other users;
- be retained as Council records.

When a councillor or officer leaves office, access shall be removed promptly and any Council information retained in accordance with the Council's Retention Policy.

---

6. Passwords and Authentication

Users must:

- create passwords containing at least twelve characters;
- avoid using easily guessed information;
- use different passwords for different systems;
- never disclose passwords to another person;
- change passwords immediately if compromise is suspected.

Where available, Multi-Factor Authentication (MFA) shall be enabled.

---

7. Council Devices

Council-owned devices shall:

- be password protected;
- receive automatic security updates;
- have appropriate anti-malware protection installed;
- be locked when left unattended.

Only authorised software may be installed.

---

8. Personal Devices

Where councillors or officers use personal devices for Council business they must ensure that:

- the device is password protected;
- operating systems remain up to date;
- Council information is stored securely;
- confidential information is protected from unauthorised access.

Council information must be removed from personal devices when an individual ceases to hold office.

---

9. Cyber Security

The Council recognises cyber security as an essential governance responsibility.

The Council will:

- maintain official **.gov.uk** email accounts;
- use secure cloud-based systems where appropriate;
- ensure regular software updates;
- maintain secure backups;
- review user accounts annually;
- remove unnecessary accounts promptly;
- encourage councillors and officers to undertake cyber awareness training.

Any suspected cyber incident must be reported immediately to the Clerk.

---

10. Data Protection

All personal information shall be processed in accordance with:

- UK GDPR;
- Data Protection Act 2018;
- the Council's Data Protection Policy;
- the Council's Privacy Notice.

Personal information shall only be accessed by authorised persons.

---

11. Cloud Storage

Council electronic records shall be stored only in approved locations.

Cloud services used by the Council should:

- provide secure authentication;
- support encrypted data transfer;
- permit controlled user access;
- support Multi-Factor Authentication where available.

---

12. Website

The Council website shall:

- comply with accessibility regulations;
- publish statutory information;
- be maintained securely;
- be reviewed regularly.

Only authorised users may update website content.

---

13. Social Media

Official social media accounts represent Cawthorne Parish Council.

Only authorised administrators may publish content.

Posts must:

- remain factual and respectful;
- not disclose confidential information;
- comply with the Members' Code of Conduct.

---

14. Software

Only properly licensed software shall be installed.

Unauthorised downloads or software installation are prohibited.

---

15. Backups

Important Council records shall be backed up using secure methods.

The Clerk shall periodically confirm that backups remain available for restoration if required.

---

16. Information Sharing

Electronic information shall only be shared where:

- authorised;
- legally permitted;
- necessary for Council business.

Sensitive information should only be transferred using secure methods.

---

17. Leaving Office

When a councillor or employee leaves office:

- Council email accounts shall be disabled;
- website access removed;
- cloud storage access removed;
- passwords changed where necessary;
- Council equipment returned;
- Council documents deleted from personal devices.

The Clerk shall maintain a register of user accounts to support orderly handover.

---

18. Training

Councillors and officers are encouraged to undertake regular cyber security and data protection training.

New councillors should receive basic guidance on:

- use of Council email;

- information security;
- data protection responsibilities;
- cyber awareness.

---

19. Monitoring

The Council reserves the right to monitor its IT systems where necessary to:

- protect Council assets;
- investigate security incidents;
- comply with legal obligations.

Monitoring will be proportionate and compliant with data protection legislation.

---

20. Breaches of this Policy

Failure to comply with this policy may result in:

- withdrawal of access to Council systems;
- investigation by the Council;
- referral to appropriate authorities where necessary.

---

21. Review

This policy shall be reviewed annually by Full Council or sooner if:

- legislation changes;
- National Association of Local Councils (NALC) guidance changes;
- AGAR requirements change;
- significant changes are made to the Council's IT systems.
