

Halstead Parish Council Information Technology (IT) Policy

Approved: Full Council – 9th February 2026

For review: February 2028

1. Purpose

This policy sets out the council's expectations for the safe, lawful and appropriate use of its IT systems and equipment. It aims to:

- Protect council data and digital assets
- Reduce security, legal and reputational risks
- Clarify acceptable and unacceptable use
- Support compliance with data protection legislation

2. Scope

This policy applies to all councillors, employees and other authorised users of council IT systems, equipment and email accounts.

3. Use of Council IT Equipment

- Council IT equipment is provided to the Clerk for council business only unless otherwise authorised.
- Users must take reasonable care of all equipment and keep it secure.
- Computers and devices must be locked when left unattended.
- Equipment must not be altered, repaired, or replaced without approval.
- Unauthorised software or storage devices must not be used.
- Loss, damage or theft of equipment must be reported immediately.

4. Portable and Personal Devices

- Portable devices must be protected by strong passwords or PINs and encrypted where possible.
- Personal devices must meet council security requirements.
- Users must keep council and personal data separate wherever possible.

5. Passwords and Security

- Strong passwords must be used and kept confidential.
- Passwords must not be shared or recorded insecurely.
- Multi-Factor Authentication should be enabled where available.
- Suspected security breaches must be reported immediately.

6. Monitoring

The council reserves the right to monitor use of its IT systems, including email and internet usage, where lawful, necessary and proportionate. Monitoring will be carried out in accordance with data protection and privacy legislation.

7. Remote Working

When working remotely, users must:

- Prevent unauthorised access to council information
- Keep screens and documents out of public view
- Log out of systems when not in use
- Store and dispose of information securely

8. Email and Internet Use

- Council email is for council business only unless otherwise authorised.
- Users must take care with attachments, links and unknown senders.
- Copyright and intellectual property laws must be respected.
- Accessing illegal, offensive or inappropriate material is prohibited.

9. Social Media

- Users must not post confidential information or material that could damage the council's reputation.
- Personal views must not be presented as council views.
- Media enquiries must be referred to the Clerk.

10. Breaches of Policy

Failure to comply with this policy may result in disciplinary action, withdrawal of IT access, or other appropriate action.

11. Review

This policy will be reviewed by the council at least every two years.