

SHERFIELD ENGLISH PARISH COUNCIL

Information Technology (IT) Policy

1. Purpose

This policy sets clear, practical rules for the safe and appropriate use of council IT systems and equipment. It aims to:

- Protect council data and systems
- Support efficient working
- Reduce security, legal and reputational risks
- Clarify acceptable and unacceptable use

2. Scope

This policy applies to all councillors, employees, contractors and other authorised users who access council IT systems or data, whether working remotely or on personal devices (where permitted).

3. Acceptable Use of IT Equipment

3.1 Council Equipment

- Council IT equipment is provided for council business only.
- Devices must be locked when unattended.
- Equipment must be handled with care and kept clean.
- Only authorised hardware, software and storage devices may be used.
- Faults, loss or damage must be reported to council promptly.

3.2 Portable Devices

- Portable devices holding council data (laptops, tablets, smartphones) must be kept secure at all times and never left unattended in public places or vehicles.
- Devices holding council data must be protected by strong passwords/PINs and encryption where possible.
- Lost or stolen devices must be reported to council immediately.
- Public computers must not be used to access Council systems.

3.3 Use of Personal Devices (BYOD)

- Council data must be kept separate from personal data and stored securely.
- Personal devices used for Council business must be locked when unattended.
- The Council may require access to devices for legal or security reasons.
- Secure networks must be used and logged out of systems when finished.
- The same security and conduct standards apply as for council equipment.
- The council may require access to devices for legal or security reasons.
- Screens must be protected from being overlooked.

4. Information Security

4.1 Passwords and Authentication

- Strong passwords must be used (e.g. three random words).
- Passwords must not be shared or written down insecurely.
- Multi-Factor Authentication (MFA) must be used where available.
- Passwords must be changed immediately if compromised.

4.2 Data Protection

- Council data must only be stored on approved systems.
- Confidential or personal data must not be saved to personal cloud services.
- Data must be securely deleted when no longer required.

5. Monitoring

- The Council may monitor IT usage, including email and internet access, where lawful, necessary and proportionate.
- Monitoring is carried out to protect systems, investigate incidents and ensure compliance with this policy.
- Data obtained through monitoring will be handled in accordance with data protection law.

6. Email and Internet Use

- It is preferable that Council emails are sent from Council accounts with the domain sherfieldenglish-pc.gov.uk
- Emails sent from Council email addresses to recipients outside of the Parish Council must contain the following footer at the start of an email chain:

“This email and any attachments to it may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed may not necessarily represent those of Sherfield English Parish Council. If you are not the intended recipient of this email, you must neither take any action based upon its contents, nor copy or show it to anyone. The copying or distribution of this transmission or any information it contains, by anyone other than the addressee, is prohibited. Please contact the sender if you believe you have received this e-mail in error. All communication sent to or from Sherfield English Parish Council may be subject to recording and or monitoring in accordance with UK legislation, are subject to the requirements of the Freedom of Information Act 2000 and may therefore be disclosed to a third party on request. If you are not the named addressee, you must destroy the original.”
- Emails should be professional, accurate and lawful.
- Copyright laws must be respected when downloading or sharing material.
- Internet use must not expose the council to security, legal or reputational risks.

7. Social Media

- Councillors and staff must not post content that could damage the council's reputation or breach confidentiality.
- Views expressed online must not be presented as council views unless authorised.
- Council information, personal data and confidential matters must never be shared on social media.
- Media enquiries must be referred to the Parish Clerk and the Chairman.

9. Health and Safety

- Appropriate workstations must be used.
- Display Screen Equipment (DSE) requirements must be followed.
- Any concerns about workstations or equipment should be discussed with the Chairman.

10. Misuse and Breaches

- Misuse of IT systems may result in disciplinary action or termination of access.
- Serious breaches may lead to dismissal or legal action.

11. Review

This policy will be reviewed periodically and updated as required to reflect changes in legislation, technology or council practices.