Sandgate Parish Council

Information and Communications Technology (ICT) Usage Policy

Policy Title: Information and Communications Technology (ICT) Usage Policy
Council: Sandgate Parish Council (SPC)
Adopted by: Sandgate Parish Council
Adoption Date 30th March 2026
Next Review Date: 30th March 2027
Responsible Officer: Parish Clerk

1. Purpose and Scope

The purpose of this policy is to ensure that the Parish Council's ICT and email facilities are used appropriately and in compliance with all relevant legislation, including the General Data Protection Regulation (GDPR) 2018 and the Data Protection Act 2018.

This policy provides clear guidance for the safe and responsible use of IT systems, devices, and Parish Council-owned email accounts. It ensures compliance with UK law and recognised best practice, including the JPAG Practitioners' Guide (2025), sections 5.121–5.122.

The policy applies to all hardware, software, applications, and data owned, leased, or used by the Parish Council.

This policy will be reviewed annually or biennially to reflect evolving cyber threats, legislative changes, and guidance from relevant sector bodies.

This policy applies to all staff, councillors, and contractors who access the Parish Council's IT systems or data.

2. Restrictions on the Use of Parish Council Computer Equipment

Employees and councillors must not use any of the Parish Council's ICT facilities to send, solicit, or download unauthorised or inappropriate material via any medium including, but not limited to:

* the internet
* email
* social media platforms
* networking platforms
* other connected devices

Employees and councillors must ensure that their workstations are protected from potential physical hazards.

No software may be installed on or removed from the Parish Council's ICT systems without prior authorisation from the Parish Clerk.

All portable equipment and software must be stored securely when not in use.

Limited personal use of Parish Council computer equipment may be permitted provided that:

a) It has been authorised by the Parish Clerk.
b) It is reasonable, occasional, and kept to a minimum.

3. Confidentiality

Employees and councillors must not upload, download, or otherwise transmit commercial software or copyrighted materials belonging to third parties without the explicit permission of the Parish Clerk.

Employees must not reveal or disclose confidential or proprietary information to any third party. This includes, but is not limited to:

* Personal or sensitive data as defined under the General Data Protection Regulation (GDPR) 2018 and Data Protection Act 2018
* Software source codes
* System logins
* Passwords

Such disclosure may only occur with the express permission of the Parish Clerk.

Access to the Parish Council's ICT facilities, applications, and data will be granted on a need-to-know basis.

Authorisation for the granting, suspension, or removal of access privileges is restricted to individuals with administrative privileges, namely the Parish Clerk and authorised IT support staff.

All access privileges for staff or members who leave the Parish Council will be revoked immediately.

Passwords must be:

* strong and unique
* changed periodically
* kept confidential

All Parish Council-owned equipment and email accounts may be audited for compliance by the IT Support Contractor in collaboration with the Parish Clerk.

Anti-virus protection and security updates must be enabled on all devices used for Parish Council business.

---

4. Use of Email, Internet and Social Networking Facilities

This section applies to all Parish Council staff and councillors and covers the use and potential misuse of the Parish Council's internet, email, and social media platforms.

All use of internet, email, and social media must comply with:

* this policy
* the Parish Council's Code of Conduct
* relevant legislation

Access to these facilities is provided primarily for Parish Council business purposes.

Limited personal use may be tolerated provided that it:

* does not interfere with Parish Council duties or operations
* has been authorised by the Parish Clerk

Any unacceptable use may be addressed through the Parish Council's disciplinary procedures.

Serious misuse may result in dismissal or criminal prosecution.

5. Legal Risks

Email is a business communication tool and must be used in a polite, responsible, effective, and lawful manner.

Although email may appear less formal than other written communications, the same professional standards apply.

Users should:

* Avoid using BLOCK CAPITALS, as this may be interpreted as shouting.
* Use appropriate salutations such as "Dear".
* Write emails with the same care as formal letters.

Users must be aware of the legal risks associated with email communications.

If users send or forward emails containing libellous, defamatory, offensive, racist, or obscene content, both the user and the Parish Council may be held liable.

Similarly:

* Unlawful disclosure of confidential information may result in legal liability.
* Forwarding messages without permission may constitute copyright infringement.
* Sending attachments that contain viruses may result in liability.

Users must follow the guidelines set out in this policy to minimise legal risks.

6. Cybersecurity Awareness and Training

The Parish Council will provide regular training and resources to educate users about:

* IT security best practices
* privacy and data protection requirements
* technology updates
* emerging cyber threats

All employees and councillors must undertake cybersecurity training, including:

* email security
* phishing awareness
* incident reporting
* secure data handling

Training is mandatory and will be refreshed at least annually. The current training provider is *…*.

7. Handling Personal Data Safely

Where there is a need to share personal data, parish council staff and councillors should ensure that precautions are taken to prevent a data breach.

Suitable precautions include:

* sharing the minimum amount of data required.
* password protecting data prior to sharing it and sending the password via different means.
* anonymising data where possible.

8. Incident Reporting and Data Breach Procedure

All staff and councillors must report any suspected IT security incident or data breach immediately to the Parish Clerk.

Examples include:

* lost or stolen devices
* accidental disclosure of personal data
* suspected phishing emails
* virus or malware alerts
* unauthorised access to systems

The Parish Clerk will investigate the incident and take appropriate action.

Where personal data is involved, the Parish Clerk will determine whether the incident must be reported to the Information Commissioner's Office (ICO) within 72 hours, as required under the Data Protection Act 2018 and UK GDPR.

9. Remote Working and Mobile Device Security

Where Parish Council systems are accessed remotely or via mobile devices, appropriate security measures must be followed.

Users must ensure that:

* devices are protected with passwords or PINs
* devices are kept secure at all times
* devices are not left unattended in public places
* unsecured public Wi-Fi networks are avoided when accessing Council systems

Loss or theft of any device used for Parish Council work must be reported immediately to the Parish Clerk.

10. Bring your own device (BYOD)

Parish council staff and councillors may at times use their own devices in the completion of their duties. This may also includes accessing the council's Wi-Fi and internet connection.

Users must ensure that:

* devices are protected from viruses and malware and have security software installed such as Windows Security.
* storage devices are encrypted where possible.
* devices are only used to access software or websites relevant to the council's functions when using the council's Wi-Fi.

11. Monitoring and Policy Compliance

The Parish Council reserves the right to monitor the use of its ICT systems to ensure compliance with this policy.

Monitoring may include:

* reviewing email usage
* monitoring internet activity
* auditing user access to systems
* reviewing security logs

Monitoring will be carried out in accordance with the Data Protection Act 2018 and UK GDPR.

Breaches of this policy may result in disciplinary action, dismissal, or legal proceedings.

12. Policy Acceptance

All Parish Council staff, councillors, and contractors who access Parish Council ICT systems must comply with this policy.

Failure to comply may result in disciplinary action.

Policy Approval

Adopted by:Sandgate Parish Council

Chair of the Council:

Name: ____Councillor Tim Prater_____

Date: _____30th March 2026_____

Parish Clerk:

Name: ___Gaye Thomas_____

Date: _____30th March 2026_____