

IT Acceptable Use Policy

St Peter's, Colchester

Adopted by the PCC: [tbc]

Review date: [3 years]

Policy owner: The Parochial Church Council

1. Purpose

This policy explains how IT systems, devices, email, internet access, mobile phones and digital tools provided or used for St Peter's should be used.

Its purpose is to ensure safe, lawful, responsible and appropriate use of technology, protecting individuals, the church, church systems, personal data, safeguarding responsibilities and the reputation and witness of St Peter's.

The Parochial Church Council has responsibility for the governance and oversight of St Peter's, including data protection, IT security, safeguarding, staff, volunteers, communications, records and church administration.

As disciples of Jesus Christ, we seek to be faithful in all that we say and do. That includes using technology truthfully, wisely, lawfully and with care for others.

2. Scope

This policy applies to:

- clergy;
- licensed staff;
- employees;
- PCC members;
- churchwardens;
- Ministry Area Leaders;
- volunteers;
- anyone using church-owned devices;
- anyone accessing church IT systems, networks, email, internet access, ChurchSuite, website admin or data;
- use of personal devices where they are used to access church systems or church data.

This policy applies to:

- computers, laptops, tablets and phones;
- church email;

- internet access;
- ChurchSuite;
- website administration;
- Dropbox or other shared storage;
- livestreaming and media systems;
- WhatsApp or other messaging tools used for church purposes;
- personal devices used for church work.

3. General principles

Church IT systems, mobile phones and digital tools are provided primarily for church business, ministry, administration, governance and communication.

Limited personal use may be permitted where it is reasonable, lawful, occasional, appropriate, and does not interfere with work, ministry, safeguarding, security or the reputation of St Peter's.

Users are responsible for their conduct when using church IT systems.

Users must use IT systems in a way that is:

- lawful;
- respectful;
- secure;
- honest;
- consistent with St Peter's policies;
- consistent with safeguarding requirements;
- consistent with the values, mission and witness of the church.

4. Fair and acceptable use

Users must:

- use church IT systems responsibly and appropriately;
- comply with relevant law, including data protection, safeguarding, copyright, equality and communications law;
- comply with St Peter's policies and procedures;
- protect personal and confidential information;
- respect others when communicating online;
- avoid bringing St Peter's into disrepute;
- follow instructions about security, passwords, updates and storage;
- report concerns, breaches or misuse promptly.

Users must not use church systems in a way that is dishonest, abusive, unlawful, unsafe, sexually inappropriate, discriminatory, harassing, intimidating, malicious, reckless or inconsistent with church responsibilities.

5. Prohibited use

Church IT systems, internet access, email, devices and mobile phones must not be used to:

- access, view, download, store or distribute pornographic, sexually explicit or indecent material;
- access illegal material;
- access the dark web, illegal marketplaces, or anonymising services intended to conceal unlawful activity;
- access extremist, hateful, abusive, discriminatory or otherwise unlawful material;
- engage in gambling;
- engage in illegal downloading or copyright infringement;
- harass, intimidate, bully, exploit or harm others;
- send abusive, threatening, discriminatory or malicious messages;
- impersonate others;
- deliberately damage or disrupt systems;
- bypass security controls;
- share passwords without authorisation;
- unlawfully disclose personal, confidential, safeguarding, financial or pastoral information;
- conduct private commercial activity without permission;
- use church systems in a way that could bring St Peter's into disrepute.

Deliberate access to illegal or seriously inappropriate material may result in disciplinary action, removal of access, safeguarding action and, where appropriate, referral to statutory authorities.

6. Mobile phone use and driving

Church-provided mobile phones must not be used while driving.

This includes:

- calls;
- texting;
- emailing;
- social media;
- messaging;
- using apps;
- reading notifications.

Phones may only be used when the vehicle is safely parked and the engine is switched off.

Users are responsible for complying with road traffic law at all times.

Where urgent church communication is needed, the user should stop safely before responding.

7. Email, messaging and communication

Church-related email should normally be sent from a stpeterscolchester.org email address where one has been provided.

Users should communicate in a way that is courteous, truthful, careful and appropriate.

Users should remember that emails and messages may be forwarded, copied, disclosed, misdirected, retained or requested as records.

Confidential, safeguarding, employment, finance, complaints, governance or sensitive pastoral matters should be handled with particular care and should not normally be discussed through informal messaging unless specifically authorised and appropriate.

Users should check recipients carefully before sending messages or attachments.

8. IT security

Users must take reasonable steps to keep church systems secure, including:

- keeping passwords confidential;
- using strong passwords;
- using multi-factor authentication where required or available;
- locking screens when devices are unattended;
- not allowing unauthorised people to use church devices or accounts;
- installing updates promptly when requested;
- not disabling security controls;
- not downloading software or files from untrusted sources;
- reporting lost or stolen devices immediately;
- reporting suspicious emails, links, messages or system behaviour promptly.

Further requirements are set out in St Peter's IT Security Policy.

9. Downloads, software and updates

Only authorised software and apps may be installed on church-owned devices.

Users must not download software, apps or files from untrusted or unofficial sources.

Copyrighted material must not be downloaded, copied, shared or used unlawfully.

Operating systems, apps, browsers and security updates must be installed promptly when requested.

Users must not attempt to bypass licensing, subscription, security or access restrictions.

10. Viruses, malware and security controls

Church devices must use approved antivirus, malware protection or built-in security controls as appropriate.

Users must not disable or bypass security controls.

Any suspected virus, malware, ransomware, unusual behaviour, unauthorised access or security warning must be reported immediately.

11. Data protection and confidentiality

Personal and confidential information must be handled in accordance with St Peter's Data Protection Policy, Data Privacy Notice and Data Retention and Records Management Policy.

Sensitive information must not be stored insecurely or shared without authorisation.

Church data should only be stored on approved systems and devices.

Images, photographs and video may only be taken, stored, shared and used in accordance with St Peter's Data Privacy Notice, Safeguarding Policy and Social Media Policy.

Users should not access personal data unless they need it for their role.

Users must not share contact details, pastoral information, safeguarding information or other personal data casually or informally.

12. Personal devices

Personal devices may be used for church work only where this is necessary, appropriate and consistent with St Peter's policies.

Personal devices used for church work should:

- be password-protected;
- be kept up to date;
- be locked when unattended;
- use appropriate security settings;
- not be shared in a way that exposes church data;
- avoid unnecessary local downloads of church data;
- be reported promptly if lost or stolen and if church data may be affected.

Personal devices should not be used to store long-term church records unless specifically authorised.

13. Monitoring and privacy

St Peter's reserves the right to monitor use of its IT systems where necessary for security, safeguarding, legal, operational, governance or policy reasons.

Monitoring will be proportionate and lawful.

Users should have no expectation of complete privacy when using church systems, church devices, church email accounts or church internet access.

Any monitoring will be handled in accordance with data protection law and St Peter's policies.

14. Breaches of this policy

Failure to comply with this policy may result in:

- advice, training or reminder of expectations;
- withdrawal or restriction of access to IT systems;
- removal from a role or responsibility;
- disciplinary action under relevant church or employment procedures;
- safeguarding action;
- data breach investigation;
- referral to the PCC, diocese, insurer, police, local authority, ICO or other statutory authority where required.

The response will depend on the seriousness, circumstances, risk and whether the breach was accidental, careless, repeated or deliberate.

15. Related policies and documents

This policy should be read alongside, where applicable:

- IT Security Policy;
- Data Protection Policy;
- Data Privacy Notice;
- Data Retention and Records Management Policy;
- Social Media Policy;
- Safeguarding Policy;
- Handling of DBS Information Policy;
- Code of Conduct;
- Volunteer Policy;
- Volunteer Agreement;
- Staff Handbook and employment policies;
- Complaints Policy;
- Whistleblowing Policy;
- Governance and Risk Management Policy;
- ChurchSuite terms and acceptable use requirements;
- relevant NCSC and ICO guidance.

16. Review

This policy will be reviewed by the PCC every three years, or sooner if required by changes in law, ICO guidance, cyber security guidance, systems, suppliers, parish practice, staffing, governance need or IT security risk.

Because technology and digital risks change quickly, practical acceptable-use arrangements may be reviewed more frequently than the policy itself.

The PCC is responsible for ensuring that this policy remains legally responsible, practically useful and consistent with St Peter's data protection, safeguarding, records management, IT and ministry practice.

Short public-facing summary

IT Acceptable Use Policy

Church IT systems, devices, email, internet access and digital tools should be used safely, lawfully, responsibly and appropriately.

Church IT is provided primarily for church business, ministry, administration and communication. Limited personal use may be allowed where reasonable and appropriate.

Users must not use church systems to access illegal, pornographic, extremist, hateful, abusive, discriminatory or otherwise inappropriate material.

Users must protect passwords, lock devices, use church systems responsibly, avoid unsafe downloads, and report suspicious emails or security concerns promptly.

Church-related email should normally be sent from a stpeterscolchester.org address where one has been provided.

Personal and confidential information must be handled carefully and in accordance with St Peter's data protection, safeguarding and IT security policies.

Church-provided mobile phones must not be used while driving.

Misuse of church IT may lead to withdrawal of access, disciplinary action, safeguarding action or referral to statutory authorities where required.