IT Security 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 St Peter's seeks to manage IT security risks connected with digital technology, church systems, devices, accounts and data.

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

As disciples of Jesus Christ, we seek to be faithful in all that we say and do. That includes protecting confidential information, guarding against avoidable harm, stewarding church resources wisely, and using technology responsibly in the service of the gospel.

This policy is intended to help staff, clergy, PCC members, officers, volunteers and others protect St Peter's systems and data from loss, misuse, unauthorised access, accidental disclosure, cyber attack and other security risks.

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, ChurchSuite, website admin, shared storage or data;
- use of personal devices where they are used to access church systems or church data.

This policy covers:

- computers, laptops, tablets and phones;

- church email accounts;
- ChurchSuite;
- website administration;
- Dropbox or other shared storage;
- WiFi;
- livestreaming and online services;
- messaging systems, including WhatsApp;
- passwords and authentication;
- software, updates and malware protection;
- storage, sharing and transfer of data;
- backups and continuity;
- loss, theft, incidents and data breaches.

3. Introduction

Digital technology is now part of St Peter's ordinary church life. It supports mission, communication, administration, giving, pastoral care, rotas, events, records, safeguarding, finance and public engagement.

These tools bring real benefits, but they also bring risks. Poor IT security could expose personal data, safeguarding information, finance records, pastoral information, staff or volunteer records, photographs, church systems, or the reputation and witness of St Peter's.

St Peter's will therefore seek to manage IT security risks in a way that is practical, proportionate and consistent with current data protection, safeguarding and cyber security expectations.

4. General principles

St Peter's will seek to ensure that:

- access to systems is limited to those who need it;
- accounts are protected by strong authentication;
- devices are secured against unauthorised access;
- personal and confidential data is stored in approved locations;
- systems and software are kept up to date;
- suspicious emails, links and attachments are treated with caution;
- important data is backed up where appropriate;
- access is removed when no longer needed;
- incidents, breaches, loss or theft are reported promptly;
- users receive guidance appropriate to their role.

IT security should support ministry and administration, not prevent them. The aim is to make safe practice normal, simple and sustainable.

5. Responsibilities

The PCC is responsible for ensuring that appropriate IT security arrangements are in place.

The Data Protection Lead, Church Administrator, Vicar, churchwardens, PCC Risk and Governance group and any delegated IT support should work together to ensure that IT risks are identified and managed.

Those using church systems are responsible for:

- following this policy;
- using systems only for authorised purposes;
- protecting passwords and devices;
- reporting suspicious activity;
- reporting lost or stolen devices;
- reporting actual or suspected data breaches;
- asking for advice where unsure.

6. Device security

All devices used to view, store, access or edit church data should be secured using an appropriate authentication method, such as a password, PIN, fingerprint, face recognition or other suitable protection.

Unattended devices should be locked.

Devices should, where possible, be set to lock automatically after no more than 15 minutes of inactivity.

On shared devices:

- browsers must not be configured to store passwords;
- "stay logged in" options should normally be disabled;
- users must log out of email, ChurchSuite, website admin and other church systems after use;
- confidential files should not be left visible or stored locally unless necessary and authorised.

Devices used for church work should be kept physically secure and should not be left unattended in public places, vehicles or unlocked rooms.

7. Passwords and authentication

Passwords must be kept confidential and must not be shared except where there is an agreed and secure church process for shared administrative access.

Passwords should be strong, not easily guessed, and not reused across unrelated accounts.

Where available and appropriate, multi-factor authentication should be used for important church systems, including email, ChurchSuite, website admin, finance systems and shared storage.

Default passwords must be changed.

Where someone leaves a role, changes responsibilities, or no longer needs access, their access should be removed or amended promptly.

Any suspected password compromise must be reported immediately.

8. Email security

A stpeterscolchester.org email address should be used for church-related email wherever one has been provided.

Replies to church-related email should normally come from a stpeterscolchester.org address.

Users should access church email by logging into their St Peter's Church mailbox. Church emails should not be forwarded automatically to personal email addresses for ease of access, because this may allow others to read the emails or create unmanaged copies of church data.

On shared devices, users must not leave the device logged into their mailbox.

Email is not always a secure method of communication. Sensitive information should be sent with care. Where sensitive information must be attached, users should consider using password-protected files, secure links, or another appropriate method. Passwords should be communicated separately from the file where needed.

Users should take care with:

- phishing emails;
- suspicious links;
- unexpected attachments;
- requests for money;
- requests for bank details;
- requests for passwords or login details;
- urgent or unusual requests appearing to come from clergy, staff, treasurers, wardens or church officers.

No legitimate organisation should ask for passwords by email.

Suspicious emails should be reported to the appropriate church contact and should not be forwarded casually.

9. Software, updates and malware protection

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

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

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

Church devices should use appropriate antivirus, malware protection or built-in security controls.

Users must not disable, bypass or weaken security controls.

Any suspected virus, malware, ransomware, unusual device behaviour or unauthorised access should be reported immediately.

Although some devices, including Apple devices, may use built-in security features rather than separate antivirus software, they must still be kept up to date.

10. Storage of data

Church data should be stored in approved church systems and agreed locations.

This may include:

- ChurchSuite;
- church email;
- approved shared storage;
- finance or payroll systems;
- safeguarding systems or files;
- agreed archive locations;
- approved secure devices or storage media.

Church data should not normally be kept only as a local copy on an individual device.

Where flash drives or other external storage are used, they should be provided or approved by St Peter's and kept securely.

Personal data and confidential information should not be stored in unmanaged personal cloud accounts, personal email accounts, informal folders, personal devices or messaging apps unless specifically authorised and appropriate.

Important records should be stored where other authorised users can access them if needed and where backup or continuity arrangements are in place.

11. ChurchSuite and website security

ChurchSuite contains a large amount of personal data. Full access must be restricted to those who have a genuine need for the information and who have been approved by the PCC or those acting under delegated authority.

Access to ChurchSuite should be role-based and proportionate.

Information from ChurchSuite must not be shared informally. If someone asks for another person's phone number, address or contact details, the normal approach should be to contact

the individual concerned and ask them to give the information to the enquirer, unless there is a proper authorised reason to share it.

Access to admin or editing facilities for St Peter's websites, ChurchSuite and other public-facing systems should be restricted to trained and authorised users only.

Website and ChurchSuite admin access should be reviewed periodically.

12. WiFi security

Only authorised users should be given the password to St Peter's WiFi network where that network provides access to church systems or internal resources.

Guest WiFi, where available, should be separated from administrative systems where reasonably practicable.

WiFi passwords should be changed where there is a security concern or where access has become too widely shared.

13. WhatsApp and messaging

WhatsApp and similar messaging tools can be useful for quick communication, but they carry risks.

Users should take particular care to check that they are sending messages to the correct person or group. It is easy to reply to the wrong person or to send a message to a group that was intended for an individual.

Confidential safeguarding, employment, finance, complaints, governance or sensitive pastoral information should not normally be sent by WhatsApp or similar messaging platforms unless specifically authorised and appropriate.

Where important church information is received by WhatsApp, text message or another informal channel, it may need to be transferred to an appropriate church record system.

When setting up the Sunday service WhatsApp livestream or sharing a livestream link, users must follow St Peter's livestream sharing instructions so that privacy is protected and the link is shared in the intended non-editable form.

14. Projectors, screens and public display

When connecting devices to projectors, livestream systems or public screens, users must ensure that the screen is not showing personal, confidential or inappropriate information.

Before connecting to a projector or public display, users should close or hide:

- emails;
- messages;
- personal data;
- pastoral or safeguarding information;

- finance information;
- browser tabs;
- notifications;
- private documents.

Notifications should be disabled where needed during services, meetings, livestreams or presentations.

15. Backups and continuity

Important church data should be stored in systems or locations where appropriate backup or recovery arrangements are in place.

Where data is stored locally or on removable media, users should consider whether it is adequately backed up and accessible to authorised people if the device is lost, damaged or unavailable.

Backups should be protected against unauthorised access.

St Peter's should periodically consider whether its most important systems and records could be restored or accessed if a device, account or service failed.

16. Lost or stolen devices

Any lost or stolen device that contains, stores, syncs or accesses church data must be reported immediately.

This includes:

- laptops;
- tablets;
- phones;
- memory sticks;
- hard drives;
- paper records;
- notebooks;
- keys or passwords;
- any device logged into church systems.

The report should be made to the Church Administrator, Data Protection Lead, Vicar or another appropriate person.

St Peter's will consider whether access needs to be disabled, passwords changed, data remotely wiped, the incident recorded, the ICO notified, or affected individuals informed.

17. Data breaches and incidents

An IT security incident may also be a data breach.

Any actual or suspected breach must be reported promptly to the Data Protection Lead.

Examples include:

- email sent to the wrong recipient;
- unauthorised access to ChurchSuite or email;
- lost device or file;
- phishing attack;
- malware or ransomware;
- accidental publication of personal data;
- sharing personal data in the wrong WhatsApp group;
- website admin compromise;
- loss of photos or records;
- unauthorised disclosure of safeguarding, pastoral, employment or financial information.

The Data Protection Policy sets out further data breach arrangements.

18. Related policies and documents

This policy should be read alongside, where applicable:

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

19. 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 cyber security risks change quickly, practical IT security 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 and IT practice.

Short public-facing summary

IT Security Policy

St Peter's uses digital systems for church administration, communication, safeguarding, finance, giving, rotas, records, website, livestreaming and ministry.

Everyone using church systems must help keep them secure.

Devices used for church data should be password-protected, kept up to date and locked when unattended.

Church email should normally be sent from a stpeterscolchester.org address. Church emails should not be automatically forwarded to personal email accounts.

Passwords must be kept confidential. Multi-factor authentication should be used for important systems where available.

ChurchSuite, website admin, email, shared storage and finance systems should only be accessed by authorised users.

Personal or confidential church data should be stored only in approved church systems or agreed secure locations.

Suspicious emails, lost devices, unauthorised access, accidental disclosure or other suspected data breaches must be reported promptly.