Data Retention & Records Management 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 records and data held by St Peter's should be created, stored, accessed, retained, reviewed, archived and disposed of.

The Parochial Church Council has responsibility for the governance and oversight of St Peter's, including data protection, records management, safeguarding, finance, employment, buildings, governance, risk management and church administration.

As disciples of Jesus Christ, we seek to be faithful in all that we say and do. That includes keeping truthful and accurate records, protecting confidential information, preserving records that need to be kept, and disposing of records securely when they are no longer required.

This policy is intended to help St Peter's manage records lawfully, securely, proportionately and consistently.

2. Scope

This policy applies to all records and data created, received, stored, used, archived or disposed of by St Peter's.

This includes records held in:

- paper files;
- email;
- ChurchSuite;
- Dropbox or other cloud storage;
- finance, payroll, banking and Gift Aid systems;
- safeguarding records;
- personnel and volunteer files;
- PCC and committee papers;
- parish registers;
- building, insurance and faculty records;
- photographs, video and livestreaming records;
- website and communications systems;

- laptops, desktops, phones, tablets and removable media;
- archive storage.

This policy applies, as relevant, to:

- clergy;
- licensed staff;
- employed staff;
- PCC members;
- churchwardens;
- PCC officers;
- Ministry Area Leaders;
- safeguarding officers and teams;
- volunteers;
- anyone who creates, handles, stores, accesses or disposes of records on behalf of St Peter's.

3. Relationship with other documents

This policy should be read alongside:

- Data Protection Policy;
- Data Privacy Notice;
- IT Security Policy;
- IT Acceptable Use Policy;
- Safeguarding Policy;
- Handling of DBS Information Policy;
- Complaints Policy;
- Whistleblowing Policy;
- Governance and Risk Management Policy;
- Risk Assessment Procedure;
- Staff Handbook and employment policies;
- Volunteer Policy;
- Church of England Records Retention Schedule;
- Church of England Safeguarding Records Retention Schedule.

The Church of England Records Retention Schedule and Safeguarding Records Retention Schedule should be treated as the primary reference documents for retention periods.

Where this policy gives examples of retention periods, those examples should be checked against the current Church of England schedules before records are destroyed.

4. General principles

St Peter's will seek to manage records according to the following principles:

- records should be accurate, necessary and proportionate;

- records should be stored in appropriate locations;
- records should be accessible to those who need them for their role;
- access should be restricted where records are confidential or sensitive;
- records should be retained for as long as required by law, guidance, safeguarding need, governance need, financial requirement, archival value or legitimate church purpose;
- records should not be kept for longer than necessary;
- records should be reviewed periodically;
- records should be archived where they need to be preserved;
- records should be securely disposed of when no longer required;
- disposal decisions should be made carefully and recorded where appropriate.

The level of security required should reflect the sensitivity and confidential nature of the material.

Any record containing personal data should be treated as confidential.

5. Active, inactive and archived records

Records may be active, inactive or archived.

Active records are still needed for current church administration, ministry, employment, safeguarding, governance, finance, buildings or operational purposes. They should be stored where they can be accessed safely by those who need them.

Inactive records are no longer used regularly but may still need to be kept for legal, safeguarding, financial, governance, insurance, historical or reference reasons. They should be stored securely and reviewed according to the relevant retention schedule.

Archived records are records that should be preserved long-term or permanently because of their legal, historical, safeguarding, governance, property or ecclesiastical significance.

Inactive or archived records should not be left scattered across personal devices, inboxes, informal folders or unmanaged shared drives.

6. Storage and security

Records should be stored in the most convenient and appropriate location, having regard to:

- the retention period required;
- how often access is needed;
- the sensitivity of the information;
- confidentiality requirements;
- safeguarding or legal significance;
- practical access by authorised people;
- security against loss, damage, misuse or unauthorised disclosure.

Paper records should be stored securely, especially where they contain personal, safeguarding, employment, financial or confidential information.

Electronic records should be stored in approved church systems or agreed storage locations. Access should be controlled and limited to those who need it.

Personal data and confidential records should not normally be stored on personal devices, personal cloud accounts, personal email accounts or informal messaging systems.

Records should not be moved, copied or downloaded unnecessarily.

7. Retention and review

Records should be retained in accordance with the Church of England Records Retention Schedule and the Church of England Safeguarding Records Retention Schedule.

St Peter's will review records periodically to identify:

- records that remain active;
- records that should be archived;
- records that should be retained for a further period;
- records that can be securely disposed of;
- records that need further advice before a decision is made.

The Data Protection Lead will co-ordinate periodic data and records review, using the Church of England record review template or equivalent process where appropriate.

Records should not be destroyed without checking whether they are needed for:

- safeguarding;
- legal obligations;
- financial or tax requirements;
- employment matters;
- governance and trustee responsibilities;
- insurance;
- property, faculty or building matters;
- complaints, disputes or investigations;
- historical or archival purposes;
- ongoing pastoral or operational reasons.

8. Secure disposal

Records that no longer need to be kept should be disposed of securely.

Paper records containing personal, confidential, safeguarding, employment, financial or sensitive information should be shredded or destroyed securely.

Electronic records should be deleted securely from relevant systems, folders, downloads, devices and backups as far as reasonably practicable.

Special care must be taken when disposing of data stored on electronic media, including laptops, phones, tablets, memory sticks, hard drives, external drives or old equipment.

Records should not be placed in ordinary waste or recycling if they contain personal or confidential information.

Where records are disposed of in bulk or where the records are sensitive, a record of disposal may need to be kept.

9. Records that should not be deleted casually

Some records should normally be archived rather than deleted, even if they are old or no longer actively used.

This includes records relating to:

- safeguarding;
- children's and youth work;
- pastoral concerns involving risk;
- PCC minutes and governance decisions;
- finance, Gift Aid, accounts and payroll;
- employment and volunteer management;
- complaints, whistleblowing and conduct concerns;
- accidents, incidents and near misses;
- buildings, fabric, quinquennial reports, faculties and insurance;
- risk assessments and risk registers;
- legal matters;
- parish registers and official records;
- disputes or possible disputes;
- records with historical or archival value.

Records should not be deleted simply because they are embarrassing, inconvenient, critical, outdated, disputed, or difficult to manage.

10. Emails, messaging and informal records

Email and messaging systems can create church records.

Where an email, attachment or message records a significant decision, concern, safeguarding matter, complaint, agreement, instruction, financial matter, employment matter, pastoral risk, building issue or governance matter, it should be saved or filed in the appropriate church system or record location.

Important church records should not remain only in personal inboxes, WhatsApp chats, text messages or informal threads.

WhatsApp and similar messaging platforms should not normally be used for confidential safeguarding, employment, finance, complaints, governance or sensitive pastoral records unless specifically authorised and appropriate. Where such information is received, it should be transferred into the correct record system where necessary.

Routine emails and messages may be deleted when no longer needed.

11. ChurchSuite and other systems

ChurchSuite and other church systems may hold current operational and pastoral data.

Records in ChurchSuite should be kept accurate, proportionate and up to date.

Where people leave, stop attending, withdraw consent or no longer need to be contacted, ChurchSuite records should be reviewed and updated in accordance with St Peter's Data Protection Policy, Data Privacy Notice and the relevant retention schedule.

Deletion or archiving of ChurchSuite records should be considered carefully where records relate to safeguarding, children's and youth work, pastoral concerns, giving, Gift Aid, attendance history, volunteer service, consent, or unresolved matters.

The same principles apply to other church systems, including finance, payroll, website, email, storage and communications systems.

12. Photographs, video and livestreaming records

Photographs, video and livestreaming material may be personal data.

Such material should be retained only where there is a lawful basis and legitimate church purpose, such as publicity, communications, safeguarding, historical record, training, worship archive or agreed ministry use.

Images of children, young people and vulnerable adults should be reviewed with particular care and handled in accordance with safeguarding and consent arrangements.

Old images should be reviewed periodically and deleted where no longer needed, unless they have historical, safeguarding, legal or other proper reason to be retained.

13. Safeguarding records

Safeguarding records must be handled with particular care.

Safeguarding records should be retained in accordance with Church of England safeguarding records retention guidance and diocesan safeguarding advice.

Safeguarding records may need to be retained for long periods and should not be deleted simply because the person has left the church, moved away, died, stopped volunteering, or because a matter appears closed.

Safeguarding records should be stored securely, with access restricted to authorised people.

Where there is uncertainty about whether a safeguarding record should be retained, archived, disclosed or destroyed, advice should be sought from the Parish Safeguarding Officer, diocesan safeguarding team or another appropriate adviser.

14. DBS and safer recruitment records

DBS certificate information should be handled in accordance with St Peter's Handling of DBS Information Policy and safer recruitment arrangements.

DBS certificate information should not normally be copied or retained once the relevant recruitment or role-suitability decision has been made, except for the limited period and purposes allowed by DBS guidance.

St Peter's may keep appropriate safer recruitment records, including records of checks completed, dates, certificate numbers, role decisions, training and renewal dates, in accordance with the relevant retention schedule.

Safer recruitment records relating to roles involving children, young people or vulnerable adults may need to be retained for longer than ordinary volunteer records.

15. Retention examples

The following examples are drawn from St Peter's current working draft and have been checked against the Church of England Records Retention Schedule and Safeguarding Records Retention Schedule where possible. The Church of England schedules remain the controlling reference documents and should be checked before significant disposal decisions are made.

Record type	Retention period / action
Personnel files of employees and voluntary workers who have not worked with children or vulnerable adults, including training and health records	6 years from the end of employment or term of service
Clergy personnel records where there are no safeguarding allegations or investigations	75 years from the end of employment or ministry appointment
Statutory Maternity Pay records and calculations	3 years after the end of the tax year to which they relate
Statutory Sick Pay records and calculations	6 years from the end of employment, where retained as part of employment/payroll records
Application forms and interview notes for unsuccessful applicants	6 months from interview / recruitment decision, unless there is a dispute, complaint, safeguarding concern or other reason to retain longer

Record type	Retention period / action
Application forms and interview notes for successful applicants	Transfer to personnel file and retain according to the relevant personnel-file retention period
Church member information	Review when the person ceases active connection with St Peter's; retain only while needed for church administration, pastoral care, safeguarding, finance, Gift Aid, governance or legitimate church purposes; delete or archive according to the Church of England schedules
Risk assessments for events not involving children, young people or vulnerable adults	6 years; longer if connected to an accident, complaint, claim, insurance matter, safeguarding concern or unresolved risk
Risk assessments for events involving children, young people or vulnerable adults	Retain according to the Church of England Safeguarding Records Retention Schedule; do not apply the ordinary 6-year event-risk-assessment period
Payroll records, including HMRC, Pensions Regulator and payroll correspondence	6 years
Accident books, records and reports – adults	6 years after the date of the last entry
Accident books, records and reports – children	Until the child reaches 21 years and 3 months; longer where safeguarding, serious injury, claim, insurance or legal advice requires it
PCC, Standing Committee, Buildings, Risk and Governance and other committee minutes	Permanently
Church registers, including marriage, baptism and other official records	Permanently
Subject access request records	3 years following completion of the request, unless complaint, ICO involvement, litigation, safeguarding or other legal issue requires longer retention

Record type	Retention period / action
Whistleblowing documents – substantiated investigation	6 years following the outcome; longer where the concern relates to safeguarding, serious misconduct, legal, insurance, employment or governance risk
Whistleblowing documents – unsubstantiated investigation	Review promptly after outcome; remove or anonymise unnecessary personal data where appropriate, but retain a proportionate record where needed for safeguarding, legal, governance, employment, complaint, insurance or accountability reasons

16. Access to records

Access to records should be limited to those who need access for their role.

Confidential or sensitive records should only be accessed by authorised people.

This may include, where appropriate:

- the Vicar;
- Church Administrator;
- Data Protection Lead;
- PCC officers;
- churchwardens;
- Parish Safeguarding Officer or Safeguarding Team;
- Treasurer or finance officers;
- staff with line-management responsibilities;
- relevant Ministry Area Leaders;
- diocesan officers or advisers;
- professional advisers;
- statutory authorities where required.

Access should be proportionate. Not everyone involved in church life needs access to all records.

17. Records during disputes, complaints or investigations

Where there is a complaint, dispute, safeguarding concern, legal issue, insurance matter, employment matter, whistleblowing concern, accident, data breach or investigation, relevant records must not be destroyed while the matter is active or reasonably foreseeable.

A temporary hold may need to be placed on relevant records until the matter is resolved and appropriate advice has been taken.

18. Responsibilities

The PCC is responsible for ensuring that St Peter's has appropriate records management and retention arrangements.

The Data Protection Lead is responsible for co-ordinating periodic data and records review and advising on day-to-day records management issues.

The PCC Risk and Governance group supports trustee-level oversight of information risk and records management.

The Vicar, churchwardens, staff, PCC members, Ministry Area Leaders, safeguarding officers and volunteers are responsible for creating, storing, using and disposing of records appropriately within their roles.

Anyone unsure whether a record should be retained, archived or deleted should ask the Data Protection Lead before taking action.

19. Related policies and documents

This policy should be read alongside, where applicable:

- Data Protection Policy;
- Data Privacy Notice;
- IT Security Policy;
- IT Acceptable Use Policy;
- Cookies Policy;
- Safeguarding Policy;
- Handling of DBS Information Policy;
- Safer Recruitment arrangements;
- Staff Handbook and employment policies;
- Volunteer Policy;
- Volunteer Agreement;
- Complaints Policy;
- Whistleblowing Policy;
- Governance and Risk Management Policy;
- Risk Assessment Procedure;
- Finance Policy and financial procedures;
- Buildings, Fabric and Development documents;
- Health and Safety Policy;
- Accident and incident reporting arrangements;
- Church of England Records Retention Schedule;
- Church of England Safeguarding Records Retention Schedule;

- ICO guidance.

20. Review

This policy will be reviewed by the PCC every three years, or sooner if required by changes in law, ICO guidance, Church of England guidance, diocesan guidance, safeguarding requirements, records retention schedules, systems, parish practice, staffing, governance need or records management risk.

Because retention guidance may be updated, retention periods should be checked against the current Church of England schedules when making significant disposal decisions.

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

Short public-facing summary

Data Retention & Records Management Policy

St Peter's keeps records for church administration, safeguarding, finance, employment, governance, buildings, pastoral care, legal responsibilities and historical purposes.

Records should be accurate, secure, proportionate and kept only for as long as needed.

St Peter's follows the Church of England Records Retention Schedule and the Church of England Safeguarding Records Retention Schedule.

Some records should be kept permanently or for long periods, including parish registers, PCC minutes, safeguarding records, building records, finance records and records relating to legal, insurance or governance responsibilities.

Records containing personal or confidential information must be stored securely and accessed only by those who need them for their role.

Records should not be deleted simply because they are old, embarrassing, inconvenient, critical, disputed or difficult to manage.

When records are no longer needed, they should be securely disposed of. Paper records should be shredded or securely destroyed. Electronic records should be deleted securely as far as reasonably practicable.

Anyone unsure whether a record should be retained, archived or deleted should ask the Data Protection Lead before taking action.