Data Protection Policy

St Peter's, Colchester

Adopted by the PCC: [tbc]

Review date: [3 years]

Policy owner: The Parochial Church Council

Charity number: 1163262

Church address: St Peter's Church, North Hill, Colchester, CO1 1DZ

Data Controllers:

- The PCC of St Peter's Church, Colchester;
- the Vicar of St Peter's Church, Colchester.

Data Protection Lead:

- Lizzie Wallace, Church Administrator
- Email: office@stpeterscolchester.org
- Phone: 07947 136048

---

1. Purpose

This policy explains how St Peter's seeks to protect personal data and comply with data protection law.

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

As disciples of Jesus Christ, we seek to be faithful in all that we say and do. That includes handling information truthfully, carefully, lawfully and confidentially; protecting people's privacy; safeguarding the vulnerable; and using personal data only for proper purposes.

This policy is intended to help staff, clergy, PCC members, officers, volunteers and others acting on behalf of St Peter's understand their responsibilities when handling personal data.

2. Scope

This policy applies to personal data handled by St Peter's in connection with the life, ministry, governance and administration of the church.

This may include personal data relating to:

- church members, attenders, visitors and enquirers;
- children, young people and families;
- staff, clergy, volunteers and applicants;
- PCC members, officers and trustees;
- donors, Gift Aid donors and supporters;
- pastoral contacts;
- safeguarding matters;
- hirers, contractors and suppliers;
- event participants;
- website, email, ChurchSuite and online users;
- members of the public who contact St Peter's.

This policy applies to personal data held in any format, including:

- paper records;
- email;
- ChurchSuite;
- Dropbox or other shared storage;
- finance and accounting systems;
- safeguarding records;
- personnel and volunteer records;
- photographs, videos and livestreaming material;
- website and online forms;
- WhatsApp or other messaging systems;
- laptops, desktops, phones, tablets and removable media.

This policy applies to:

- clergy;
- employed staff;
- PCC members;
- churchwardens;
- Ministry Area Leaders;
- volunteers;
- safeguarding officers and teams;
- those with access to church systems;
- anyone processing personal data on behalf of St Peter's.

3. Legal framework

St Peter's will seek to comply with applicable data protection and privacy law, including:

- the UK General Data Protection Regulation;
- the Data Protection Act 2018;
- the Privacy and Electronic Communications Regulations;

- the Data (Use and Access) Act 2025;
- other relevant legislation and guidance, including ICO guidance.

The Data (Use and Access) Act 2025 came into law in June 2025. ICO guidance is being updated, and this policy may need further review as guidance develops.

This policy should be read alongside St Peter's Data Privacy Notice, Data Retention Policy, IT Security Policy, IT Acceptable Use Policy, Safeguarding Policy, Safer Recruitment arrangements and other relevant policies.

4. Data protection principles

St Peter's will seek to uphold the data protection principles.

Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept only for as long as necessary;
- handled securely and confidentially;
- processed in a way that demonstrates accountability.

In practice, this means St Peter's should:

- use personal data only where there is a proper lawful basis;
- be clear with people about how their data is used;
- collect only the information that is needed;
- avoid reusing personal data for unrelated purposes;
- keep records accurate and up to date;
- store information securely;
- restrict access to those who need it;
- delete, archive or retain records in accordance with retention guidance;
- keep appropriate records of decisions, processes and policies.

5. Lawful basis for processing

St Peter's will identify and use an appropriate lawful basis when processing personal data.

The lawful basis may differ depending on the purpose and type of data. The lawful basis may include:

- consent – where a person has given clear consent for a specific use;
- contract – where processing is necessary for a contract or proposed contract;
- legal obligation – where St Peter's is required by law to process the data;
- vital interests – where processing is necessary to protect someone's life or safety;
- public task – where processing is necessary for a task carried out in the public interest;

- legitimate interests – where processing is necessary for St Peter's legitimate interests, provided those interests are not overridden by the rights and freedoms of the individual.

St Peter's may rely on different lawful bases for different activities, including worship, pastoral care, safeguarding, administration, employment, volunteering, finance, Gift Aid, rotas, events, communications and building use.

If the lawful basis for processing changes, St Peter's will consider whether individuals need to be informed.

6. Special category data and criminal conviction data

Some personal data is especially sensitive. This includes information about health, ethnicity, religious belief, sex life, sexual orientation, biometric data and other special category data.

St Peter's may process special category data where necessary, for example in relation to:

- church membership and religious affiliation;
- pastoral care;
- safeguarding;
- health and accessibility needs;
- children's and youth ministry;
- employment and volunteering;
- emergency contact and medical information;
- equal opportunities monitoring where appropriate;
- prayer, support or pastoral records where appropriate.

St Peter's must identify both a lawful basis and an additional condition for processing special category data.

Criminal conviction data, DBS information and safeguarding-related information must be handled with particular care and only where lawful and necessary.

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

Safeguarding records must be handled in accordance with safeguarding policy, diocesan guidance, Church of England guidance and appropriate retention requirements.

7. People's rights

St Peter's recognises that people have rights in relation to their personal data.

These rights may include the right to:

- be informed about how their data is used;
- access their personal data;
- obtain a copy of their personal data;
- have inaccurate data corrected;

- ask for data to be deleted in certain circumstances;
- ask for processing to be restricted in certain circumstances;
- object to certain processing;
- object to direct marketing;
- data portability where applicable;
- complain about how their data is handled.

These rights are not absolute and may depend on the legal basis for processing, safeguarding needs, legal obligations, retention requirements, pastoral responsibilities, employment responsibilities or the rights of others.

Requests relating to personal data should be referred promptly to the Data Protection Lead.

8. Subject access requests and individual rights requests

A person may ask to see personal data St Peter's holds about them. This is known as a subject access request.

A person may also ask St Peter's to correct, delete, restrict or stop using their data, or may object to certain processing.

Anyone receiving such a request should pass it promptly to the Data Protection Lead.

St Peter's will respond to valid requests within the timescales required by law, unless an extension is permitted.

Before responding, St Peter's may need to:

- confirm the identity of the person making the request;
- clarify the request;
- search relevant records;
- consider whether exemptions apply;
- protect the rights and privacy of others;
- seek advice where safeguarding, legal, employment or confidentiality issues arise.

Requests involving safeguarding, pastoral records, employment records, complaints, DBS information, legal privilege or third-party information should be handled with particular care.

9. Data protection complaints

St Peter's will provide a clear route for people to raise data protection complaints.

Data protection complaints may be sent to:

Data Protection Lead

- St Peter's Church, c/o The Vicarage, Balkerne Close, Colchester, CO1 1DZ
- Email: office@stpeterscolchester.org

St Peter's will normally acknowledge data protection complaints within 30 days of receipt.

St Peter's will take appropriate steps to consider and respond to the complaint, including making enquiries where needed and keeping the complainant informed.

St Peter's will communicate the outcome of the complaint without undue delay.

If a person remains dissatisfied, they may complain to the Information Commissioner's Office.

10. Data security and confidentiality

Personal data must be handled securely and confidentially.

Those handling personal data on behalf of St Peter's should:

- access only the data they need for their role;
- keep passwords secure;
- use church systems responsibly;
- avoid unnecessary downloads or copies;
- store paper records securely;
- keep personal data out of public view;
- avoid discussing confidential information inappropriately;
- use secure methods when sharing sensitive information;
- take care when emailing personal data;
- check recipients before sending;
- avoid using WhatsApp or informal messaging for confidential, safeguarding, employment, finance or sensitive governance matters unless specifically authorised and appropriate;
- report suspected data breaches promptly.

Personal data should not be stored on personal devices unless this is necessary, authorised and appropriately protected.

Additional requirements are set out in St Peter's IT Security Policy and IT Acceptable Use Policy.

11. Photographs, video and livestreaming

Photographs, video and livestreaming may involve personal data.

St Peter's will seek to use photographs and video responsibly, with particular care for children, young people, vulnerable adults and those who may be at risk.

St Peter's should be clear where photography, filming or livestreaming is taking place.

Consent or another lawful basis may be required depending on the context and use.

Images should not be used in ways that are intrusive, misleading, unsafe or inconsistent with safeguarding requirements.

Images of children and young people must be handled in accordance with safeguarding policy, parental consent arrangements, photography guidance and any relevant ChurchSuite records.

12. Sharing personal data

St Peter's will share personal data only where there is a proper reason and lawful basis.

Personal data may be shared, where appropriate, with:

- clergy, staff, officers and volunteers who need it for their role;
- PCC members or trustees where necessary for governance;
- diocesan officers;
- safeguarding advisers or statutory safeguarding agencies;
- police, local authority or emergency services;
- HMRC or other public authorities;
- payroll, finance, accounting or Gift Aid service providers;
- IT, ChurchSuite, website, email, cloud storage or database providers;
- insurers, professional advisers or legal advisers;
- contractors or processors providing services to St Peter's.

Where third-party processors are used, St Peter's should seek appropriate assurances that personal data is handled securely and lawfully.

Personal data should not be shared casually, unnecessarily, or outside agreed purposes.

13. International transfers and online systems

Some systems used by St Peter's may store or process data outside the UK.

Where this occurs, St Peter's will seek to ensure that appropriate safeguards are in place, either through the provider's arrangements or other lawful transfer mechanisms.

This may apply to cloud storage, email, website, ChurchSuite, finance systems, communications tools, video platforms or other online services.

The Data Protection Lead should be involved where new systems are introduced that process personal data.

14. Data retention and deletion

St Peter's will keep personal data only for as long as necessary.

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

Data will be reviewed and cleansed periodically by the Data Protection Lead, using the Church of England record review template or equivalent process where appropriate.

Some records may need to be retained for long periods, including safeguarding records, governance records, financial records, employment records, building records, insurance records and legal records.

Other records should be deleted, archived or anonymised when no longer needed.

Records should not be deleted simply because they are embarrassing, inconvenient, critical or relate to a dispute, complaint, safeguarding matter, insurance matter or possible legal issue.

Superseded records should normally be archived rather than deleted where they relate to safeguarding, governance, finance, buildings, risk, complaints, employment, accidents or legal responsibilities.

15. Data breaches

A data breach is a security incident that affects the confidentiality, integrity or availability of personal data.

This may include:

- sending personal data to the wrong person;
- losing a paper file, laptop, phone or memory stick;
- unauthorised access to ChurchSuite, email, Dropbox or other systems;
- accidental deletion or alteration of records;
- phishing or malware;
- unauthorised disclosure of safeguarding, pastoral, employment or financial information;
- loss of photographs, records or contact lists;
- personal data being made public by mistake.

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

The Data Protection Lead, with appropriate support, will consider:

- what happened;
- what data is affected;
- who is affected;
- whether there is risk to individuals;
- what immediate action is needed;
- whether the ICO must be notified;
- whether affected individuals must be told;
- what records should be kept;
- what lessons should be learned.

Serious data breaches may need to be reported to the ICO within the statutory timescale.

16. Accountability and governance

St Peter's will seek to demonstrate accountability by keeping appropriate records, policies and processes.

This may include:

- Data Protection Policy;
- Data Privacy Notice;
- Data Retention Policy;

- IT Security Policy;
- IT Acceptable Use Policy;
- Handling of DBS Information Policy;
- Safeguarding Policy;
- records of processing activities where appropriate;
- data breach records;
- subject access request records;
- data protection complaint records;
- retention and deletion records;
- processor and system records;
- training or guidance records.

The Data Protection Lead is responsible for day-to-day organisational management of data protection and is the first point of contact for data protection issues, subject access requests, data protection complaints and data review.

The Senior Information Risk Owner trustee role provides trustee-level assurance that information risk is being managed appropriately and effectively across St Peter's.

At St Peter's, the SIRO function is exercised through the PCC Risk and Governance group.

17. Training and awareness

Those who handle personal data on behalf of St Peter's should receive appropriate guidance or training according to their role and level of access.

This may include guidance on:

- confidentiality;
- secure storage;
- ChurchSuite use;
- email and messaging;
- safeguarding records;
- photographs and consent;
- data breaches;
- subject access requests;
- retention and deletion;
- use of church and personal devices;
- phishing and cyber security.

Those with access to sensitive personal data, safeguarding records, employment records, DBS information, finance records or significant church systems may need more detailed guidance.

18. Responsibilities

The PCC and Vicar are the Data Controllers for St Peter's.

The PCC is responsible for ensuring that appropriate data protection arrangements are in place.

The Data Protection Lead is responsible for day-to-day organisational management of data protection, responding to data issues, co-ordinating subject access requests and complaints, and supporting periodic data review.

The PCC Risk and Governance group acts as the Senior Information Risk Owner trustee function, working with the Data Protection Lead to provide assurance to the PCC.

Staff, clergy, PCC members, officers, Ministry Area Leaders and volunteers are responsible for handling personal data appropriately and following this policy.

Anyone who is unsure about how to handle personal data should seek advice from the Data Protection Lead.

19. Related policies and documents

This policy should be read alongside, where applicable:

- Data Privacy Notice;
- Data Retention Policy;
- IT Security Policy;
- IT Acceptable Use Policy;
- Cookies Policy;
- Safeguarding Policy;
- Safer Recruitment arrangements;
- Handling of DBS Information Policy;
- Staff Handbook and employment policies;
- Volunteer Policy;
- Volunteer Agreement;
- Code of Conduct;
- Social Media Policy;
- Complaints Policy;
- Whistleblowing Policy;
- Governance and Risk Management Policy;
- Risk Assessment Procedure;
- 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, systems, parish practice, staffing, governance need or data protection risk.

Because data protection law and guidance are developing following the Data (Use and Access) Act 2025, this policy should be reviewed sooner if updated ICO guidance requires changes.

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 IT practice.

Short public-facing summary

Data Protection Policy

St Peter's seeks to handle personal data lawfully, fairly, securely and transparently.

The Data Controllers are the PCC of St Peter's Church, Colchester and the Vicar of St Peter's Church, Colchester. The Data Protection Lead is Lizzie Wallace, Church Administrator.

St Peter's may hold personal data about church members, attenders, visitors, families, children, young people, staff, volunteers, donors, hirers, contractors, safeguarding matters, events and church administration.

Personal data should only be used for proper purposes, kept secure, accessed only by those who need it, kept up to date, and retained only for as long as necessary.

People have rights in relation to their personal data, including the right to understand how their data is used, request access, ask for correction, object to some uses, and complain.

Data protection requests, complaints or concerns should be sent to:

office@stpeterscolchester.org

St Peter's will normally acknowledge data protection complaints within 30 days and will consider and respond to them appropriately.

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

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