



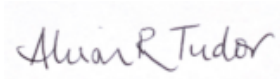
Data Protection and Retention Policy

Version – 1.2

Date of publication – 27.06.2025

Date of review – 30.06.2028

Published by Alison Tudor
Church Administrator

Signed  Date 27.06.2025

Approved by Mark Inglis
on behalf of Seagate Elders

Signed  Date 27.06.2025

Approved by Dave Tudor
on behalf of Seagate Trustees

Signed  Date 27.06.2025

1. Overview

Seagate Church takes the security and privacy of personal data seriously. As part of our activities we need to collect and use personal information about a variety of people including members, former members, adherents, employees, volunteers, office-holders, enquirers and other people who are in contact with us for a variety of reasons. The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 govern the way in which organisations can collect, process, store, access or transfer personal information about living individuals. We are committed to processing personal data appropriately and lawfully.

This policy explains the provisions that we will adhere to when any personal data belonging to or provided by the individuals listed above are collected, processed, stored, accessed or transferred on behalf of Seagate Church. It applies to all personal data whether stored electronically, on paper or on other materials. We expect everyone processing personal data on behalf of Seagate Church to comply with this policy and our Data Privacy Notice. Any deliberate or negligent breach of this policy or our Data Privacy Notice by an employee or volunteer may result in disciplinary action being taken.

Our Data Privacy Notice is available on the Seagate Church website and can be found on the noticeboard in the church building. The individuals from whom we collect personal data should be provided with our Data Privacy Notice prior to the collection of data.

This policy does not form part of any contract of employment (or contract for services if relevant) and can be amended by the Trustees at any time.

2. Definitions

Personal data is any information, held either on paper, electronically or on other materials, relating to a living person ("data subject") that directly or indirectly identifies them personally. It can be factual (such as a name, address, email address, telephone number, photograph or video) or an opinion (such as a performance appraisal) or a statement of intention about them.

Special category personal data includes personal data revealing religious beliefs. A significant amount of personal data held by Seagate Church will be classed as special category personal data, either specifically or by implication, as it could be indicative of a person's religious beliefs. Additional rules apply to the processing of personal information which falls in this category.

Criminal offence data is personal data relating to criminal convictions and offences. The processing of this data also has additional legal safeguards.

Processing means any operation which is performed on personal data, such as collecting, recording, accessing, organising, structuring, storing, editing, retrieving, viewing, listening to, disclosing, transferring, sharing, archiving, erasing, deleting, destroying etc.

The **Data Controller** for the purposes of GDPR is identified as the Trustees of Seagate Church collectively, because they decide how personal data is processed and for what purposes.

Where individuals (employees, trustees, volunteers) are processing personal data on behalf of Seagate Church and in accordance with their paid or voluntary role within the church, this processing will be deemed to be by the Data Controller entity. This also applies to those doing work on behalf of the church from home and who are processing individual's personal data there.

3. Data Protection Principles

Personal data will be processed in accordance with the following 'Data Protection Principles'. It must:

- Be processed fairly, lawfully and transparently
- Be collected and processed only for specified, explicit and legitimate purposes
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Be accurate and, where necessary, kept up to date. Any inaccurate data must be deleted or rectified without delay.
- Not be kept for longer than is necessary for the purposes for which it is processed and
- Be processed securely, with protection against unauthorised or unlawful processing and against accidental loss or damage, using appropriate technical or organisational measures

4. Processing Personal Data

Personal data should only be accessed by those who need it for the work they do for or on behalf of Seagate Church. Data should be used only for the specified lawful purpose for which it was obtained. Unnecessary copies of personal data should not be made.

We process personal information on one or more of the following legal bases, which are also set out in our Privacy Notice, where:

- Processing is necessary for the purposes of Seagate Church's legitimate interests, unless these are overridden by interests, fundamental rights and freedoms of the data subject
- Processing is necessary for the performance of a contract with the data subject
- Processing is necessary for us to comply with a legal obligation
- Processing is necessary to protect someone's life (vital interests)
- Processing is necessary for us to perform a task in the public interest and the task has a clear basis in law
- The data subject has given consent

We may also process personal data relating to criminal convictions and offences or related security measures in a safeguarding context where the processing meets a condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018.

Processing of special category data is only lawful when one of the legal bases in UK GDPR and the DPA 2018 Act applies. This includes the following:

- The individual has given explicit consent to the processing of the personal data for one or more specified purposes; and/or

- The processing is carried out in the course of our legitimate activities with appropriate safeguards in place by Seagate Church, as a not-for-profit body with a religious aim, where the processing relates solely to the members, former members or people who have regular contact with us in connection with our purposes and that the personal data are not disclosed outside Seagate Church without the consent of the data subjects.

Where personal data is to be held with a third party (for example ChurchSuite), Seagate Church will only do so with the consent of the data subject or where there is a lawful basis for doing so.

Information relating to criminal proceedings or offences or allegations of offences may be processed for the protection of children or adults who may be at risk and shared with Seagate's Safeguarding Team or with statutory agencies. We will only do so in compliance with the law and at all times respecting the rights and freedoms of the data subjects.

When mentioning pastoral concerns or requesting prayer for identifiable individuals, reasonable steps will be taken to ensure that the individual is willing for this to happen.

In the UK, children aged 13 or over are able to provide their own consent, so for children under this age, where processing of their data is based on consent (and not on some other lawful basis, as set out in this policy), it will be necessary to obtain this from whoever holds parental responsibility for the child.

5. Keeping Personal Data Secure

Personal data should not be shared with those who are not authorised to receive it.

Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use.

Confidential paper waste should be disposed of securely by shredding.

Any computers or other devices being used in a shared area should be shut down, or the user should log off, when leaving them unattended.

Passwords and PINs should be kept secure. They should be strong, changed regularly and not written down or shared with others.

Particularly sensitive electronic data should be password protected or encrypted before transfer.

The 'bcc' rather than the 'cc' or 'to' fields should be used when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group.

6. Data Retention

Data should only be held for as long as necessary for the purposes for which it is collected. Data protection law does not set specific time limits for the retention of different types of personal information. It is up to data controllers to set and justify their own retention periods. Retention periods are determined taking into account the type of information that is collected and the purpose for which it is collected, bearing in mind the requirements applicable to the situation and the need to destroy outdated, unused information at the earliest reasonable opportunity.

Suggested retention periods are set out in the Data Retention Schedule in Appendix 1 of this policy, and decisions relating to the retention and disposal/erasure of data should be taken with reference to the Schedule. Advice can be sought from our safeguarding partner, thirtyone:eight, if there is uncertainty about retention periods.

In all cases where the retention period recommended in the Schedule for specific types or items of personal information has expired, a review should be carried out prior to disposal, and consideration should be given as to the most appropriate method of secure erasure or disposal.

Ensuring that personal information is erased or anonymised when no longer required will reduce the risk of it becoming irrelevant, excessive, inaccurate or out of date, and the risk of it being processed in error.

7. Disposal/Erasure of Data

Documents containing confidential or personal information should be disposed of either by shredding or by using confidential waste bins or sacks. Documents other than those containing confidential or personal information may be disposed of by recycling or binning.

Information stored digitally should also be reviewed regularly and if no longer required should be closed and/or permanently deleted. This should not be done simply by archiving. It is understood that the word “deletion” can mean different things in relation to electronic data, and that it is not always possible to erase all traces of it. The key issue is to put the data beyond use. Therefore, it will normally be sufficient simply to delete the information, with no intention of it ever being used or accessed again by anyone. In addition to deleting personal information from a live system, it should also be deleted from any back-up of the information on that system. Deletion can also be effected by using one of the following methods of disposal:

- Using secure deletion software which can overwrite data;
- Using the function of “restore to factory settings” (where information is not stored in a removeable format);
- Sending the device to a specialist who will securely delete the data.

8. Data Subject Rights

Unless subject to an exemption under GDPR, data subjects have the following rights with respect to their personal data:

- The right to request a copy of the personal data which Seagate Church holds about them (This request must be made in writing to the Trustees. It is a criminal offence to

conceal or destroy personal data which is part of a subject access request. The request must be dealt with within one calendar month. A log of such requests will be kept for GDPR auditing purposes.)

- The right to request that any personal data found to be inaccurate, incomplete or out of date is corrected
- The right to request their personal data is erased where it is no longer necessary for Seagate Church to retain or use such data
- The right to withdraw their consent to the processing of their data at any time
- The right, where there is a dispute in relation to the accuracy or processing of their personal data, to request a restriction is placed on further processing
- The right to request that we provide data in a suitable format and transfer it to another organisation the individual has identified
- The right to object to the use or processing of their personal data

9. Data Security Breaches

A data breach is where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This can happen in many different ways, for example:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information by a member of staff, volunteer or third party
- Loss of data resulting from an equipment or systems failure
- Human error, such as accidental deletion, alteration or transfer of data
- Unforeseen circumstances, such as fire or flooding
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams

Should a data security breach occur, the chair of the Seagate Trustees must be notified immediately. If there is a high risk of the breach adversely affecting the rights and freedoms of individuals, then the UK Information Commissioner's Office (ICO) must be notified within 72 hours. All data breaches should be recorded, including the decision on whether to report to the ICO or not.

In situations where a personal data breach causes a high risk to a person, we will inform the data subjects without undue delay. This will enable them to take steps to protect themselves and/or exercise their rights.

Appendix 1: Data Retention Schedule

This Schedule is provided as a guide to common types of documents but is not exhaustive.

Record Type	Retention Period
HR/ Employees/ Volunteers	
Pre-employment application forms & interview notes of unsuccessful applicants (paid workers/volunteers)	6 months after completion of recruitment
Employee HR Records including recruitment documentation, right to work documentation, appraisals, disciplinary records, grievances, absence records	Duration of employment + 7 years (75 years if role involves contact with children or protected adults)
Volunteer Recruitment Forms	Duration of volunteering + 7 years
Parental Leave Records	18 years from date of birth of a child
Complaints (non-safeguarding)	7 years after resolution of complaint (unless further action is anticipated)
Training Certificates (Safeguarding, Food Hygiene, First Aid etc)	Duration of employment/volunteering + 7 years
Finance	
Financial records, including invoices, bills and expenses payable, income records, donations, bank statements and all supporting documentation	6 years from end of financial year in which transaction made
Payroll and pension payment records	6 years from end of the financial year the records relate to
Gift aid declarations & paperwork	6 years after the tax year to which it relates or until any current enquiries completed
Annual audit reports and financial statements	Indefinitely
Grant Applications	6 years after the tax year to which it relates or until any current enquiries completed
Health & Safety	
Accident Records	5 years from date of accident or end of any investigation (or if an accident involves a child/young person, then until that person reaches 21)
Records documenting external inspections	5 years after date of inspection
Hazardous material exposures	30 years
Injury and Illness Incident Reports (RIDDOR)	5 years
Health & Safety Risk Assessments	5 years from final date of use
Insurance	
Insurance documents	Indefinitely
Meetings	
ACR papers and minutes	Indefinitely
Trustee Meeting minutes	Indefinitely
Membership	
Church Membership List	Live document, indefinitely

Church members, adherents, friends contact details	Reviewed every 2 years, out of date information updated or deleted.
Property	
Title Deeds	Indefinitely or until property is disposed of
Building Alterations: Final plans, designs and drawings of building, planning consents, building certificates, warranties etc	Indefinitely or until 6 years after property is disposed of
Information relating to the management of properties, including sales, purchases, title deeds, construction documents	Indefinitely
Building Let Application Forms	6 years from end of the financial year the records relate to
Warranties	Duration of warranty + 6 years
Legal	
Application for charitable status	Indefinitely
OSCR filings	5 years from date of filing
Trust Deed & Legal Correspondence	Indefinitely
Documents relating to legal proceedings, potential or actual	Final settlement of matter or conclusion of any formal proceedings + 7 years
Safeguarding	
Annual General Information & Consent forms	7 years
Activity Consent Forms for Youth/Children	7 years
mainly music registration forms	Until child no longer attends activity
Records of attendance of children/youth and leaders/volunteers at activities where parents/guardians are not present	7 years after event unless a safeguarding incident or concern was raised.
Safeguarding Risk Assessments Safeguarding Log/ Complaints/ Allegations/ Concerns (Cause for Concern form used) Safeguarding Referrals to External Agencies Safeguarding Covenants of Responsibility/ Contracts *Low Level Cause for Concern	75 years after last contact with individual concerned. *Retention period will be proportionate to the identified concern and will be determined by Safeguarding Lead & Coordinator..
Record of PVG check	75 years after scheme member stops carrying out a regulated role for Seagate Church.
PVG Certificates (paper or email)	Until last day that a scheme member is carrying out a regulated role for Seagate Church.
Misc	
Policies & Procedures: superseded versions	Retained for the same period as the subjects to which they relate, to demonstrate what was notified to relevant employees/volunteers.
Registers of Marriage	Indefinitely

Personal data relating to events for which additional information is gathered e.g. church trip/ weekend away	Immediately after the event unless anything has occurred (e.g. accident) which requires longer retention of records
--	---