

Table of Contents

Introduction	1
Roles And Responsibilities	2
Data Retention guideline	2
Emails	3
Safe destruction of data	3
Archiving	3
Transferring Data to Other Media	4
Transferring Data to Another School	4
Appendix A: Data Retention.....	5

Introduction

Data will be stored and processed to allow for the efficient operation of the School. The School has a legal responsibility to maintain its records and record keeping systems. When doing this, the following factors will be taken into account:

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Accessibility of records and record keeping systems.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

This policy applies to all St Faith's staff and Governors, as well as to third parties working with St Faith's. It sets out how data will normally be processed and held by the School, and when that data will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR).

This policy is to be considered alongside other relevant policies and documents as set below, which are accessible to parents on the school's [website](#) or can be provided upon request, at no charge.

- Information Security Policy;
- Information Technology Acceptable Use Policy;
- Data Protection Policy;
- Data Breach Policy
- Personal Device Policy for Staff And Visitors

All School policy documents are held on the server and may be accessed via SharePoint at this [link](#).

Roles And Responsibilities

The School's board of **Governors** has the responsibility to ensure that the school has data protection policies and procedures in place to safeguard systems, staff and pupils and comply with data protection legislation.

The **Bursar** has overall strategic responsibility to implement this policy and related procedures. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

The **Compliance Officer** is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation, and provide advice on policy and practice relating to data handling and records management.

The **Data Protection Officer** will consider the suitability and adequacy of this policy and report improvements directly to management.

The **Senior Management Team** and Heads of Department are responsible for:

- disseminating and promoting this policy to relevant staff within their areas;
- Ensuring that staff within their areas are informed about, comprehend this policy, and receive sufficient and ongoing training to perform the required procedures;
- advising on strategic developments that are likely to impact on data classification.

All St Faith's staff are responsible for:

- adhering to this policy;
- having an awareness of the four data retention policy and schedule;
- handling, classifying and protecting the School's data appropriately;
- bringing this policy to the attention of any associates and third parties they are working with.

Associates working with St Faith's, including agency staff, data processors, third parties and collaborators are responsible for:

- adhering to this policy;
- handling, classifying and protecting the data they work with appropriately and in accordance with the School's Data Protection policies and processes.

The IT Helpdesk: can be contacted with any queries relating to the appropriate security and technical controls required to store and protect data.

Data Retention guideline

Under data protection law, **personal data should only be kept as long as needed for the legal purpose it was collected for**, and 'data controllers', like schools, should **avoid storing more personal data than necessary**.

The retention periods are based on business needs and legal requirements. The Data Retention schedule refers to all records regardless of the media (e.g., paper, electronic, microfilm, photographic etc) in/on which they are stored.

All records will be regularly monitored by designated members of staff, who will conduct periodic reviews and

keep a data destruction log. When managing records, the School will adhere to the standard retention times listed within that schedule.

Emails

Generally, emails may need to fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a pupil record). It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

Safe destruction of data

Where records have been identified for destruction, they should be disposed of in an appropriate way.

All data must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

- All paper records containing personal data or sensitive information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate wastepaper merchant.
- All electronic data will be deleted.
- CDs / DVDs should be cut into pieces
- Audio /Video Tapes should be dismantled and shredded
- Hard Disks should be dismantled and sanded

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list the following:

- File reference (or other unique identifier);
- File title/description;
- Number of files and date range;
- Name of the authorising officer;
- Date destroyed or deleted from system; and
- Person(s) who undertook destruction, or, if outsourced, request from the third party provider a certificate of safe destruction. .

Archiving

Where data have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archive is maintained online with the school's offsite archive provider, OASIS. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

Transferring Data to Other Media

Where lengthy retention periods have been allocated to data, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

Transferring Data to Another School

We retain the pupil's educational data whilst the child remains at the School. Once a pupil leaves the School, their file should be sent to their next school. We may delay destruction for a further period where there are special factors such as potential litigation.

Appendix A: Data Retention

Type of Record/Document	<u>Suggested</u> Retention Period
<u>EMAILS ON SERVER</u>	See note on emails above
Pupil email account	Delete upon leaving school, or within one year.
Staff emails [<i>schools may wish to set their own policies, either centrally or with staff</i>]	Routine deletion of historic emails after 2-3 years, and delete account within 1 year of leaving school.
<u>SCHOOL-SPECIFIC RECORDS</u>	
Registration documents of School	Permanent (or until closure of the school)
Admission Register ('the school roll')	At least 6 years from date of entry (monthly backup required).
Attendance Register	At least 6 years from date of entry (monthly backup required)
Minutes of Governors' meetings	6 years from date of meeting
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
Complaints Register / Log	7 years from pupil leaving school

<u>INDIVIDUAL PUPIL RECORDS</u>	<i>NB these records will contain personal data</i>
Admissions: application forms, assessments, records of decisions	25 years from date of birth (or up to 7 years from the pupil leaving). If unsuccessful: up to 1 year.
Student immigration records Examination results (external or internal) Pupil file including: Pupil reports and performance records Pupil medical records (<i>not accidents</i>) Pupil disciplinary records (<i>not issues of safeguarding</i>) Attendance data Special educational needs records	Duration of student sponsorship plus min. 1 year 7 years from pupil leaving school. ALL: 25 years from date of birth (<i>subject where relevant to any material that may be relevant to potential historic claims: see below</i>). Where there is a historic claim - Date of birth plus up to 35 years (<i>risk assessed</i>)
<u>SAFEGUARDING</u>	
Policies, procedures and insurance	Keep a permanent record of historic policies

DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on SCR / personnel file, but not the certificate itself.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim.
Child Protection files and specific records of child sexual abuse	If a referral has been made / social care have been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years.
Video recordings of meetings	Where any one-on-one meetings of classes, counselling, or application interviews are recorded (e.g. for safeguarding purposes), a shorter-term retention policy is acceptable based on the DSL's view of how quickly a concern will likely be raised: e.g. 3-6 months or immediately upon DSL review.
CORPORATE RECORDS (where applicable)	
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
Shareholder resolutions	Minimum – 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex members/shareholders)

Annual reports	Minimum – 6 years
<u>ACCOUNTING RECORDS</u>	
Accounting records (<i>normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state</i>)	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
<u>CONTRACTS AND AGREEMENTS</u>	
Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
<u>INTELLECTUAL PROPERTY RECORDS</u>	
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.

Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP / IT agreements (including software licenses and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	<i>NB these records will contain personal data</i>
Single Central Record of employees	Keep a permanent record that mandatory checks have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above)
Contracts of employment	7 years from effective date of end of contract Duration of employment plus minimum of 7 years
Employee appraisals or reviews	As above, but <u>do not delete any information which may be relevant to historic safeguarding claims</u>
Staff personnel file	
Payroll, salary, maternity pay records	Minimum – 6 years
Pension or other benefit schedule records	Potentially permanent (ie lifetimes of those involved), depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	12 months - <i>In respect of DBS certificates and records of criminal information disclosed by the candidate (if applicable), see DBS section in 'Safeguarding' above.</i>
Staff immigration records (Right to work, etc.)	Minimum – 2 years from end of employment
Tier 2 migrant worker sponsor records	Minimum – 1 year from end of employment
Health records relating to employees	7 years from end of employment

Records of low-level concerns about adults	At least until end of employment (as recommended by KCSIE), then subject to review for relevance: e.g. 7 years from end of employment if they have ongoing relevance for employment claims, longer if necessary for safeguarding purposes / claims.
INSURANCE RECORDS	
Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years (<i>but this will depend on what the policy covers and whether e.g. historic claims may still be made</i>)
ENVIRONMENTAL, HEALTH & DATA	
Maintenance logs (PPM, RPM and Projects)	10 years from date of last entry
Accidents to children	25 years from birth (longer for safeguarding). Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. Therefore keep a note of all procedures as they were at the time, plus a record that they were followed, and relevant insurance documents.
Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. Therefore keep a note of all procedures as they were at the time, plus a record that they were followed, and relevant insurance documents.

Staff use of hazardous substances	Minimum – 7 years from end of date of use. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. Therefore keep a note of all procedures as they were at the time, plus a record that they were followed, and relevant insurance documents.
Staff exposure to Asbestos	40 years - plus retention of any asbestos related risk assessments, accident records and working practices at the time.
Covid-19 risk assessments, policies and other key documents	7 years from date of creation
Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. Therefore keep a note of all procedures as they were at the time, plus a record that they were followed, and relevant insurance documents.
Art.30 UK GDPR records of processing activity (ROPAs) and "Appropriate Policy Document" (if different) where relying on certain special category data processing grounds	No limit (as long as no personal data held), but must be kept up-to-date, accurate and relevant.
Data protection impact assessments (DPIAs)	As above
Data breach log / register	Keep up to date and retain details of breaches for the last 6 years (where risk of claims) and at least 3 years in the ordinary course. (<i>Consider if necessary to hold any personal data as part of the breach log</i>).

Date reviewed: Aug 26
Next review: Aug 27

Page 12 of 12

Responsibility: Bursar