



ST MARGARET'S

SCHOOL

Data Retention Policy

ST MARGARET'S

SCHOOL

Data Retention Policy Review:

Review Date	February 2026
Reviewed By	Martin Scoble – Director of Finance & Operations
Approval Date	May 2026
Approved By	Full Board
Next Review Date	May 2030

Contents

Introduction.....	2
Striking a Balance	2
Meaning of "Record"	2
‘Personal Data’ - What it is, and When it is Lawful to Retain	4
Lawful Purpose to Hold and Retain Personal Data?.....	4
Archiving, Data Management, and the Destruction or Erasure of Records.....	4
The Risks of Longer Retention	5
Secure Disposal of Documents and Devices.....	5
Table of Retention Periods.....	6

Introduction

St Margaret's School will seek to balance the benefits of keeping detailed and complete records, for the purposes of good practice, archives or general reference, with practical considerations of storage, space and accessibility. The following legal considerations apply in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including e.g. KCSIE;
- disclosure and evidence requirements for potential future litigation;
- contractual and insurance obligations;
- the laws of confidentiality and privacy; and (last but by no means least relevant)
- UK GDPR and the DPA 2018

These will inform not only minimum and maximum retention periods (the rationale for which should be notified to data subjects via privacy notices and, for more sensitive personal data, recorded in appropriate policy documents), but also what to keep and who should be able to access it.

Striking a Balance

Even justifiable reasons to keep certain records, such as child protection records, for many years after pupils or staff leave the school will need to be weighed against personal rights. The longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative burden on the school, in terms of both secure storage and individual subject access rights.

Steps St Margaret's take to support its retention policies are (a) communicating the reasons for the policy in privacy notices and staff or parent contracts; and (b) ensuring any records necessary to keep long-term are kept very secure, accessible only by trained staff on a need-to-know basis.

Meaning of "Record"

In this policy, "record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material, but not all, will contain personal data of individuals as defined in UK GDPR.

An obvious example of a record containing personal data would be a database (such as a mailing list or the staff Single Central Record), or a pupil or personnel file specific to an individual. However, a "record" of personal data could arise simply by holding an email on the school's systems: your policies should ensure staff do not use email accounts or inboxes as proxy filing systems for key documents.

Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important for retention purposes than its contents, and the reason for keeping it (although format is of course an important consideration in terms of how best to preserve documents securely).

Digital records

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data or any large quantity of data should as a minimum be password-protected (ideally with two-factor authentication), with internal access on a need-to-know basis. Consideration should be given, either on an individual or (ideally) a policy basis, to when password protection should be applied to sensitive attachments to emails, or if secure links are preferable. Where 'cloud storage' or intranet access is used, consider what data needs to be made available to which users.

If personal information of any volume or sensitivity is permitted to be kept on personal devices, digital encryption is essential. That will usually be the difference between a lost laptop being a simple matter of the cost of the device, or a serious reportable data breach.

Email accounts and internal messaging systems

Emails and other internal messages – whether they are retained electronically or printed out as part of a paper file – are also "records" likely to contain personal data (of the sender, recipient, or a third party) in their body, footer, in the sent/received fields, or in attachments. As such they will potentially fall within the scope of a subject access request made against the school.

They may also contain particularly important information: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) in a subject access request. Again, however, school policy and training should mitigate against using email accounts as proxy filing systems.

St Margaret's has a short term email retention policy of no more than 3 years. Emails should not be used to retain important information, resources, contracts, legal advice, attendance notes, safeguarding concerns or incident reports that ought to be properly held elsewhere (i.e. in the appropriate file, accessed only by the appropriate persons).

Such policy and training must also stress to staff the great importance of care and professionalism in how such records are created by casual email (or other forms of instant messaging such as Teams or Slack, which are also records for these purposes). This will become particularly apparent when a subject access request is made by a colleague, pupil or parent and the data recorded may need to be provided.

It is also worth remembering that a digital document's original metadata may indicate the date of its creation, its author or the history of its changes – or its deletion. Metadata may be necessary to examine under a legal claim or a data audit.

Records on personal devices including SMS / WhatsApp

Whether text / WhatsApp messages, and any other files or notes held by a staff member or governor on their personal device (including tablet or smartphone) counts as a school "record" will depend on the circumstances – and to a large extent the school's policies on the official use of such platforms.

As a general rule, an employee has an expectation of privacy in their own messaging for personal use, and is not subject to UK GDPR for solely domestic or 'household' uses of data.

However, where personal devices are used by employees or governors / trustees / board members for official school use – for example to discuss a pupil issue, parental complaint or disciplinary matter – it may be deemed an official record of the school. This means it may be disclosable in litigation or under a subject access request, if the school has reasonable grounds to believe relevant evidence or personal data might be found on the device, including by SMS, WhatsApp or personal email. In that sense, any staff or governor WhatsApp group must be used with the same professional formality as email.

Video / audio recordings

Given the rise of remote provision of learning, meetings, assessments and interviews, schools are increasingly capturing many gigabytes of personal data (some of it impactful and personal).

The reasons for recording such virtual sessions may vary: from seeking to keep a record as a resource for those unable to attend at the time (notably for group or assembly sessions), via classes where a child was absent, down to safeguarding reasons (e.g. for one on lessons, VMT or counselling sessions, or application interviews).

Such recordings are also digital records and – depending to a degree on both their contents and how they are stored / tagged – may be deemed the personal data of anyone identifiable from the recording. How long they may be kept, therefore, should be judged in the same way any other type of record is: for what purpose is it kept, and how long is it necessary to keep it?

Not all such recordings will be necessary for long-term legal or safeguarding purposes. In practice, this would be expensive and unmanageable in storage terms, and could create unnecessary burdens (subject access rights, for example) and data security risks. SMT, DSL and IT teams should collectively agree what a feasible storage period is *based on what is a likely period in which a complaint or concern will generally be raised* following a virtual lesson or meeting (or when reviews or spot checks will be carried out, if sooner). This should be led by the safeguarding advice but – unless something arises that means it should be treated as a record of an incident – is unlikely to be more than 3 months. A similar approach may already be in place for short-term CCTV recording storage and review.

Paper records

Paper records are most often damaged by damp or poor storage conditions; but as well as applying common sense (i.e. dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper), security is also vital – especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.

Under UK GDPR, paper records are only classed as personal data if held in a qualifying "filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible – and so searchable much as a digital database might be. By way of example, personnel files searchable by marked dividers will likely fall within UK GDPR. A daily notebook, or diary, or chronological file of correspondence may not, unless it is readily clear to whom the file or notebook substantially relates: for example, a complaint or case file.

However, schools should not be tempted to retain or store personal data in disorganised or inaccessible hard copies, except as part of an appropriate archiving policy (which may be subject to an exemption from data protection rules around access and erasure in any event: see below). Schools are likely to remain responsible, as a principle of data security, for personal information contained on handwritten notes, print-outs taken from electronic files, or disclosures from their systems made orally. Remember: data protection law is only one consideration in retaining records, and it is far preferable for governance and legal reasons to keep paper documents ordered and accessible.

‘Personal Data’ - What it is, and When it is Lawful to Retain

Aside from purely charitable, corporate, estate or financial records (including asset lists, IP, accounts, contracts etc.), most records will contain information about living¹ individuals: e.g. pupils, parents, alumni, governors, staff (past, present and prospective), and consultants / contractors / VMTs. The school will also hold professional contacts. That type of information is likely to amount to "personal data" for these purposes, and therefore be subject to data protection laws which necessarily interact with these 'document retention' guidelines.

Generally, the sources of law that determine how long you retain personal data will not be UK GDPR or the DPA 2018, but derive from elsewhere: eg statutory time limits by which legal claims must be made; the stipulations of your contracts; or the requirements of governmental organisations (e.g. the Disclosure and Barring Service, Charity Commission, IICSA etc.). As a general rule, in the event of any doubt or apparent contradiction with data protection law, statutory legal duties (including those under KCSIE / safeguarding) should be followed. However, data protection law is the overarching legal framework here and – properly understood and applied – does accommodate all these statutory duties on schools.

What data protection law requires is simply that personal data is only retained for as long as necessary – and only as much as is necessary – for the specific lawful purpose (or purposes) it was acquired, or at least for clearly compatible purposes².

Lawful Purpose to Hold and Retain Personal Data?

Most “ordinary” personal data may be processed in connection with a private contractual duty (e.g. under an employment or parent contract) or where necessary for a “legitimate interest” as defined in UK GDPR (which ought to be set out in your school’s privacy notice). It may then be retained for a reasonable and necessary period of time afterwards, generally linked to legal claims.

However, a higher standard would apply to the processing of "special category [= sensitive] personal data", including notably health, trade union membership, ethnicity, religious beliefs, political views and sexual life. Similar rules apply to any records of criminal proceedings, offences or allegations. A mere contractual need to process, or a legitimate interest of the school or third party, would not in itself justify the retention of such personal data – but if it were necessary in connection with the defence of future legal claims, or to help prevent or detect crime or unlawful behaviour, or as part of the school’s safeguarding duties, then a lawful UK GDPR or DPA 2018 basis to retain will arise.

Archiving, Data Management, and the Destruction or Erasure of Records

All staff should receive basic training in data management – issues such as security, recognising and handling sensitive personal data (alongside training in safeguarding and first aid, etc.) – at least every two years, in accordance with ICO guidance. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, that:

- records – whether electronic or hard copy – are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

- important records, and large or sensitive personal databases, are not left sitting in email accounts, taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets). Where this is absolutely necessary, it should be subject to a risk assessment and in line with an up-to-date IT use policy;
- questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action;
- arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage), and in whatever territory – are supported by robust, UK GDPR-compliant contractual arrangements providing for secure control, access and retrieval;
- reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and
- all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.

This is particularly important in respect of the school's specific legal obligations under UK GDPR. However, they amount to common sense rules even where personal data is not directly involved.

The Risks of Longer Retention

Notwithstanding the legal grounds and (in some cases) imperatives to do so, the longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative and storage burden on schools. This also increases the amount of material in respect of which schools must be accountable to data subjects (e.g. information requests, "right to be forgotten" requests), and the consequences of data security breach become more serious.

St Margaret's may take professional advice and decide where to draw the line in retaining data for these purposes. This is a decision that should always be made mindful of risk and knowledge of where historic incidents may have occurred or future complaints may arise.

It is also vitally important that all records handlers bear in mind, when creating documents and records of any sort (particularly email, but also video meeting recordings and internal staff messaging systems), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a subject access request under UK GDPR. The watchwords of record-keeping are therefore accuracy, clarity, professionalism and objectivity.

Secure Disposal of Documents and Devices

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. For **hard copy** documents, skips and 'regular' waste disposal will not be considered secure. Paper records or images should be shredded using a cross-cutting shredder; devices for digital storage and recordings should be dismantled or broken into pieces. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information.

For **digital devices**, a number of individual steps are advisable prior to disposal: wiping the hard drive and/or activating drive encryption; uninstalling and/or deauthorising applications or accounts that could enable a user to access secure school systems (including wiping browsing history and cookies); and/or physically destroying the drive with a drill or hammer.

Table of Retention Periods

Type of Record/Document	Retention Period
<u>EMAILS ON SERVER</u>	<i>[see note on email retention and storage]</i>
Pupil email account	Delete upon leaving school, or within one year.
Staff emails [schools may wish to set their own policies, either centrally or with staff]	Routine deletion of historic emails after 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). <i>(Schools may then wish to archive in order to retain a definitive record of who attended the school when)</i>
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	Duration of student sponsorship plus min. 1 year
Examination results (external or internal)	7 years from pupil leaving school.
Pupil file including: - pupil reports and performance records - pupil medical records (not accidents) - pupil disciplinary records (not issues of safeguarding) - attendance data	ALL: 25 years from date of birth (subject where relevant to any material that may be relevant to potential historic claims: see below).
Special educational needs records	Date of birth plus up to 35 years (risk assessed)
<u>SAFEGUARDING</u>	<i>[see note on IICSA guidelines]</i>
Policies, procedures and insurance	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	<u>No longer than 6 months</u> 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 Child Protection files and specific records of child sexual abuse Video recordings of meetings	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. 3 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. 3 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.
<u>CORPORATE RECORDS</u> (where applicable) Certificates of Incorporation Minutes, Notes and Resolutions of Boards or Management Meetings Shareholder resolutions Register of Members/Shareholders Annual reports	<i>eg where schools have trading arms</i> Permanent (or until dissolution of the company) Minimum – 10 years Minimum – 10 years Permanent (minimum 10 years for ex members / shareholders) 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>) <u>[NB specific ambit to be advised by an accountancy expert]</u> Tax returns VAT returns Budget and internal financial reports	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 Minimum – 6 years Minimum – 6 years Minimum – 3 years
<u>CONTRACTS AND AGREEMENTS</u> Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>) Deeds (or contracts under seal)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later 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) Assignments of intellectual property to or from the school IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years. As above in relation to contracts (7 years) or, where applicable, deeds (13 years). Minimum – 7 years from completion of contractual obligation concerned or term of agreement
<u>EMPLOYEE / PERSONNEL RECORDS</u> Single Central Record of employees Contracts of employment Employee appraisals or reviews Staff personnel file Payroll, salary, maternity pay records Pension or other benefit schedule records Job application and interview/rejection records (unsuccessful applicants) Staff immigration records (Right to work, etc.) Tier 2 migrant worker sponsor records Health records relating to employees Records of low-level concerns about adults	<i>NB these records will contain personal data</i> Keep a permanent record that mandatory checks have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above) 7 years from effective date of end of contract Duration of employment plus minimum of 7 years As above, <u>but do not delete any information which may be relevant to historic safeguarding claims</u> Minimum – 6 years Potentially permanent (ie lifetimes of those involved), depending on nature of scheme 12 months (<i>NB – ACAS has extended the early conciliation period to 12 weeks from 1 December 2025 and there are also proposals to extend the time limit for bringing a tribunal claim from 3 to 6 months</i>). [<i>In respect of DBS certificates and records of criminal information disclosed by the candidate (if applicable), see DBS section in 'Safeguarding' above.</i>] Minimum – 2 years from end of employment Minimum – 1 year from end of employment 7 years from end of employment 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.
<u>INSURANCE RECORDS</u> 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>)
<u>ENVIRONMENTAL, HEALTH & DATA</u>	
Maintenance logs	10 years from date of last entry
Accidents to children	25 years from birth (longer for safeguarding)
Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances	Minimum – 7 years from end of date of use
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
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>).



www.stmargarets-school.org.uk

Merry Hill Road, Bushey
Hertfordshire, WD23 1DT
United Kingdom

+44 (0)20 8416 4400
schooloffice@stmargarets-school.org.uk