

Retention of Records Policy

(Reviewer: Darren Carpenter, August 2023)

1. Background

- The College needs to create and maintain accurate records in order for it to function. This policy for managing records has been drawn up in conformity with legislation and regulations affecting schools in general and with the UK General Data Protection Regulation (GDPR).
- In retaining records the College will pay due regard to legal considerations in respect of the retention of records and documents, including:
 - statutory duties and government guidance relating to schools, including for safeguarding;
 - disclosure requirements for potential future litigation;
 - contractual obligations;
 - the law of confidentiality and privacy; and (last but by no means least relevant)
 - GDPR.
- 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 information about individuals – e.g., staff, pupils, consultants, parents, contractors, or other individuals, whether they are a part of the school or some other third party (for example, another school). Such information is likely to amount to 'personal data' for the purposes of GDPR and may be subject to data protection laws which may, in places, conflict with aspects of these 'document retention' guidelines. In such cases, statutory legal duties such as those outlined above – or the duty to report to safeguard vital interests – will be considered alongside data protection concerns in the event of any contradiction. In addition, certain personal data may legitimately need to be retained or disclosed subject to a private contractual duty (e.g., under a parent contract).
- 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 than its contents and the purpose for keeping it.

2. Archiving and the destruction or erasure of Records

- All staff will receive basic training in data management – issues such as security, recognising and handling sensitive personal data, safeguarding etc.
- Staff given specific responsibility for the management of records will have specific training and ensure, as a minimum, the following:
 - That records – whether electronic or hard copy – are stored securely, 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;
 - Those important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or stored locally on portable devices, mobiles and handheld electronic tablets, unless absolutely necessary, in which case it should be subject to a risk assessment and in line with an up-to-date IT use policy;
 - That 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;

- That arrangements with external storage providers – whether physical or electronic (in any form, but most particularly ‘cloud-based’ storage) – are supported by robust contractual arrangements providing for security and access;
- That reviews are conducted on a regular basis 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
- That 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.

3. Retention periods

- Records will be retained as follows:

Records will generally be securely erased as soon as practicable after the end of the minimum retention period.

Type of Record/Document	Retention Period
<p><u>SCHOOL-SPECIFIC RECORDS</u></p> <ul style="list-style-type: none"> Registration documents of School Attendance Register Minutes of Governors' meetings Annual curriculum 	<p>Permanent (or until closure of the school)</p> <p>6 years from last date of entry, then archive.</p> <p>6 years from date of meeting</p> <p>From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)</p>
<p><u>INDIVIDUAL PUPIL RECORDS</u></p> <ul style="list-style-type: none"> Admissions: application forms, assessments, records of decisions Examination results (external or internal) Pupil file including: <ul style="list-style-type: none"> ○ Pupil reports ○ Pupil performance records ○ Pupil medical records Special educational needs records (<i>to be risk assessed individually</i>) 	<p><i>NB – this will generally be personal data</i></p> <p>25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).</p> <p>7 years from pupil leaving school</p> <p>ALL: 25 years from date of birth (<i>subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil</i>).</p> <p>Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)</p>

Type of Record/Document	Retention Period
<p><u>SAFEGUARDING</u></p> <p>Policies and procedures DBS disclosure certificates (if held)</p> <p>Accident / Incident reporting</p> <p>Child Protection files</p>	<p><i>NB – <u>All records to be kept permanently pending outcome of IICSA.</u></i></p> <p>Keep a permanent record of historic policies</p> <p>No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.</p> <p>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.</p> <p>If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely.</p> <p>If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).</p>
<p><u>EMPLOYEE / PERSONNEL RECORDS</u></p> <p>Single Central Record of employees</p> <p>Contracts of employment Employee appraisals or reviews Staff personnel file</p> <p>Payroll, salary, maternity pay records Pension or other benefit schedule records</p> <p>Job application and interview/rejection records (unsuccessful applicants)</p> <p>Immigration records Health records relating to employees</p>	<p><i>NB this will contain personal data</i></p> <p>Keep a permanent record of all mandatory checks that have been undertaken (but <u>not</u> DBS certificate itself: 6 months as above)</p> <p>7 years from effective date of end of contract</p> <p>Duration of employment plus minimum of 7 years</p> <p>As above, but <u>do not delete any information which may be relevant to historic safeguarding claims</u></p> <p>Minimum – 6 years</p> <p>7 years from effective date of end of contract</p> <p>Minimum 3 months but no more than 1 year unless request received to keep records on file</p> <p>Minimum – 4 years</p> <p>7 years from end of contract of employment</p>

Type of Record/Document	Retention Period
<p><u>CORPORATE RECORDS</u></p> <p>Certificates of Incorporation Minutes, Notes and Resolutions of Boards or Management Meetings Shareholder resolutions Register of Members/Shareholders Annual reports</p>	<p>Permanent (or until dissolution of the company) Minimum – 10 years Minimum – 10 years Permanent (minimum 10 years for ex-members/shareholders) Minimum – 6 years</p>
<p><u>ACCOUNTING RECORDS</u></p> <p>Accounting records Tax returns VAT returns Budget and internal financial reports</p>	<p>Minimum – 6 years from the end of the financial year in which the transaction took place <i>Internationally: can be up to 20 years depending on local legal/accountancy requirements</i> Minimum – 6 years Minimum – 6 years Minimum – 3 years</p>
<p><u>INSURANCE RECORDS</u></p> <p>Employers Liability Certificates Insurance policies (will vary – private, public, professional indemnity) Correspondence related to claims/renewals/notification re: insurance</p>	<p>Minimum – 40 years 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. Minimum – 7 years</p>
<p><u>CONTRACTS AND AGREEMENTS</u></p> <p>Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments) Deeds (or contracts under seal)</p>	<p>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</p>
<p><u>INTELLECTUAL PROPERTY RECORDS</u></p> <p>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 eg maintenance; storage; development; coexistence agreements; consents)</p>	<p>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</p>

Type of Record/Document	Retention Period
<p><u>ENVIRONMENTAL, HEALTH & DATA</u></p> <p>Maintenance logs Accidents to children Accident at work records (staff)</p> <p>Staff use of hazardous substances Risk assessments (carried out in respect of above) Data protection records documenting processing activity, data breaches</p>	<p>10 years from date of last entry 25 years from birth (longer for safeguarding) Minimum – 4 years from date of accident, but review case-by-case where possible Minimum – 7 years from end of date of use 7 years from completion of relevant project, incident, event or activity No limit: as long as up-to-date and relevant (as long as no personal data held)</p>
<p><u>EMAILS</u></p>	<p>Unless archived by the user or the College's Network Manager, emails will be stored for a period of up to 2 years from the date and time they are sent from or received to the College's email system.</p>

Owner: DRC	Date for review: September 2026
------------	---------------------------------