

Data Retention Policy

Approved by:	Tom Evans
Date:	June 2025
Review date:	June 2026
Relevant Schools:	Academy21, King's InterHigh

1. Policy and Objectives

We are the Inspired Education Group (the “**Group**”). The Group collects, stores and processes a large amount of data and information, including personal information about individuals (principally, our staff, and the students and parents at the schools within the Group).

All our data and information in all formats and mediums must be suitably protected, safeguarded, stored properly and securely and disposed of appropriately when no longer necessary having regard to Group’s reasonable needs and the sensitivity and confidentiality of the relevant records.

This Data Retention Policy provides a simple framework for determining whether a document or record should be retained or destroyed. It seeks to balance the needs of the Group (and the schools and other entities within the Group) for retaining data and our legal obligations to destroy personal data (which may be by way of anonymization) and, in some cases, other types of information when it is no longer required.

This Data Retention Policy applies in addition to the Group’s other relevant policies, including the Group’s:

- IT policies, including the Acceptable Use Policy;
- Data Protection Policy;
- Privacy Notice (pupils and parents); and
- Privacy Notice (staff).

This Data Retention Policy may be updated from time to time to ensure continued compliance with applicable law and to reflect best practice. The Group’s Global DPO is responsible for monitoring and reviewing this policy.

2. Scope

This Data Retention Policy applies to all data and information (including personal data) recorded in any format and any medium, wherever stored either by the Group or externally on our behalf on-site or off-site, whether in filing cabinets, cupboards, computers, servers and in the cloud (the “**Records**”). It also applies at all schools within the Group.

Categories and formats of Records include:

- Pupil and Parent Records, including pupil admissions, attendance, attainment, safeguarding and parent payment Records;
- Staff and HR type Records, including passport copies, CVs of personnel and of potential candidates, performance reviews;
- Administrative records including: personnel, estates, financial and accounting;
- Information concerning complaint handling;
- Voicemails, data on business phones, SIM cards etc.;
- Electronic, digital documents;
- Audio-visual recordings, e.g. from lesson recordings
- Paper documents, handwritten files, emails;
- Data processed on any devices, including mobile phones, laptops, iPads etc.; and
- Computer media e.g. server records, drives, backup tapes.

All Group employees, contractors, casual staff, and consultants are responsible for how they handle Records and must comply with this policy.

3. Storage of Records

Key principles:

- **Secure and appropriate storage:** Stored as securely as possible to avoid potential misuse or loss and in a place and format most convenient for its purpose and taking into account the nature of the information;
- **Archiving and Destruction:** Records will be disposed, destroyed, anonymized or archived in a secure manner when no longer required (see section **Error! Reference source not found.** below). Please refer to the Group's Information Security Policy for the process. As a general rule, 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.
- **Personal Data and Confidential Information:** In cases of hard copy paper Records, where these Records contain confidential information, personal data or information which is relevant to any dispute or litigation, it should be stored in lockable cabinets. In cases of electronic Records, these should be stored in electronic folders, appropriately filed and stored on an approved software system and server – this ensures that the Record will automatically be backed-up securely off-site. These Records should be subject to restricted access to a limited number of persons with appropriate authority on a need-to-know basis. Keys and passwords must also be stored securely and accessible only to authorised person

4. Table of retention periods

The relevant data retention periods are set out below. The suggested retention periods are intended to apply across the Group, however it is recognised that case-by-case decision making will be required for certain Records because, for example, local law requirements may set different retention periods. Any proposed changes in retention periods from those set out in the table below must be approved by the Global DPO and CIO.

The Group applies the GDPR standard globally, accordingly the Group will retain personal data for no longer than is necessary for the purposes for which it is processed. Where Records containing personal data are listed in the table below, we have balanced this storage limitation principle against our legitimate requirements to retain the personal data.

Type of Record/Document	Retention Period	<u>Reason / comments</u>
EMAILS ON SERVER <i>NB these records will contain personal data</i>		
Pupil email account	Delete upon leaving the School, or within one year.	If any emails sent or received by pupils have been flagged or monitored as concerning, they should be stored on the relevant pupil file or child protection file. Otherwise, pupil email accounts should be deleted one year after the pupil's departure. This should be sufficient to permit students to request access for legitimate reasons in the months following departure.
Staff emails	Routine deletion of historic emails after 2-3 years, and delete account within 1 year of leaving the School.	Sensitive or important material should not remain stored on email servers. It should be routinely and properly filed by staff, and good email hygiene involves regularly 'flushing' (i.e. clearing out) email accounts. Otherwise, it poses a data security risk, increases storage costs, and creates subject access liabilities.
Individual's (e.g. alumni and parents) names and email addresses who receive newsletters and other school / Group communications for marketing purposes	Held in line with the individual's communication preferences.	Reflecting any applicable consents and/or communication preferences.

Type of Record/Document	Retention Period	Reason / comments
SCHOOL-SPECIFIC RECORDS		
Registration documents of Group / School within the Group	Permanent (or until closure of the Group / School within the Group)	These are important documents that will need to remain accessible whilst the Group / School is active.
Attendance Records	6 years from last date of entry, then archive	Limitation period.
Minutes of leadership meetings	6 years from date of meeting	Limitation period.
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)	This reflects best practice recommendations in the sector.
INDIVIDUAL PUPIL RECORDS <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 later). If unsuccessful or turned down the offer: up to 1 year.	Becomes part of pupil file. See below. In case of claims and enables the Group / schools to check against previous intake cycle.
Student immigration records	Duration of student sponsorship plus a minimum of 1 year	In line with government guidance.
Academic data / Examination results (external or internal)	7 years from pupil leaving the School. Longer retention period may apply for archiving, research and statistical purposes, provided such information taken out of day-to-day processing and is subject to suitable data minimisation procedures (e.g. pseudonymisation if anonymization not possible and/or subject to access restrictions)	Limitation period: contract.

Type of Record/Document	Retention Period	Reason / comments
Pupil file including: <ul style="list-style-type: none"> Pupil reports and performance records Pupil medical records (<i>not accidents</i>) 	ALL: 25 years from date of birth (this is subject where relevant to any material that may be relevant to potential historic claims: see below).	Limitation period for duty of care / contract plus 1 year (to allow for school year cycles): 7 years. Minors cannot bring claims in their own right, but the limitation period restarts when they turn 18. As a result, the retention period is 25 years from the date of birth.
Special educational needs records	Date of birth plus up to 35 years (this should be risk assessed on a case-by-case basis)	Allowing for extended limitation on claims.
SAFEGUARDING		
Policies, procedures and insurance	Keep a permanent record of historic policies	Historic policies can be used as a useful comparison.
DBS / criminal records checks 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 Single Central Record / personnel file, but not the certificate itself.	In line with government guidance.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim. Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.	Civil claim limitation periods can be set aside in cases of abuse, justifying a longer retention period.
Child Protection files and specific records of child sexual abuse	If a referral has been made / social care has been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years.	Civil claim limitation periods can be set aside in cases of abuse, justifying a longer retention period. In line with best practice guidance.
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	Unlikely to be necessary to retain video meeting recordings beyond a short period, as they can be intrusive and consume significant storage. Transcripts of important meetings should be made promptly. Exceptions may be made for recordings of incidents (as with CCTV).

Type of Record/Document	Retention Period	Reason / comments
	immediately upon DSL review.	
CORPORATE RECORDS (where applicable)		
Certificates of Incorporation	Permanent (or until dissolution of the company)	These are important documents that will need to be accessible whilst the Group / School is active.
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years	In line with relevant company law.
Shareholder resolutions	Minimum – 10 years	In line with relevant company law.
Register of Members/Shareholders	Permanent (minimum 10 years for ex members/shareholders)	In line with relevant company law.
Annual reports	Minimum – 6 years	Reflects best practice, in line with general accounting and tax rules.
ACCOUNTING RECORDS		
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>) [NB specific ambit to be advised by an accountancy expert]	Internationally: can be up to 20 years depending on local legal/accountancy requirements, a shorter period can be applied in line with any specific local tax law requirements	In line with tax law requirements.
Tax returns	Minimum – 6 years	In line with tax law requirements.
VAT returns	Minimum – 6 years	In line with tax law requirements.
Budget and internal financial reports	Minimum – 3 years	In line with relevant company law.

Type of Record/Document	Retention Period	Reason / comments
CONTRACTS AND AGREEMENTS		
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	Limitation period
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement	Limitation period
INTELLECTUAL PROPERTY RECORDS		
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, e.g. trade marks); otherwise expiry of right plus minimum of 7 years.	Limitation period
Assignments of intellectual property to or from the Group / School	Permanent (or until the lifetime of the intellectual property right)	Limitation period
IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement	Limitation period
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 UK requirement: do not keep DBS certificate information itself: 6 months as above)	Permanent record for accountability. See comments relating to DBS records above.
Contracts of employment	7 years from effective date of end of contract	Limitation period
Employee appraisals or reviews	Duration of employment plus minimum of 7 years	Limitation period
Staff personnel file	As above, but <u>do not delete any information which may be relevant to historic safeguarding</u>	Limitation period. See comment relating to safeguarding Records.

Type of Record/Document	Retention Period	Reason / comments
	<u>claims</u>	
Payroll, salary, maternity pay records	Minimum – 6 years	Limitation period.
Pension or other benefit schedule records	Potentially permanent (i.e. lifetimes of those involved), depending on nature of scheme	To ensure accountability and the proper administration of such schemes.
Job application and interview/rejection records (<u>unsuccessful applicants</u>)	Minimum 3 months but no more than 1 year	CVs and job applications can quickly become outdated, so this information should be deleted no later than one year after receipt.
Staff immigration records (Right to work, etc.)	Minimum – 2 years from end of employment	Follows government guidance.
Tier 2 migrant worker sponsor records	Minimum – 1 year from end of employment	Follows government guidance.
Health records relating to employees	7 years from end of employment	Limitation period.
Records of low-level concerns about adults	At least until end of employment, 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.	Limitation period.
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.	Limitation period.
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>)	Limitation period.

Type of Record/Document	Retention Period	Reason / comments
ENVIRONMENTAL, HEALTH & DATA <i>NB these records may contain personal data</i>		
Maintenance logs	10 years from date of last entry	Reflects best practice.
Accidents to children	25 years from birth (longer for safeguarding)	<p>limitation period - 3 year limitation period for most personal injury claims plus 1 year, and 6 years for contract claims.</p> <p>Minors cannot bring claims in their own right, but the limitation period restarts when they turn 18. As a result, the retention period is 25 years from the date of birth.</p>
Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible	Limitation period – 3 year limitation period for most personal injury claims plus 1 year.
Staff use of hazardous substances	Minimum – 7 years from end of date of use	Limitation period.
Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.	Limitation period.
Records of data processing activity, data breach records, and data protection impact assessments	No limit (as long as no personal data held), but must be kept up-to-date, accurate and relevant.	These are useful accountability documents, so should be retained (and maintained) indefinitely.