Information and Records Retention Policy

Background

This policy covers the storage and retention of records and document.

The General Data Protection Regulation (GDPR) contains strict rules about use and storage of personal data such that:

- All information held by the school needs to be justifiable, by reference to its purpose;
- The school must be transparent and accountable as to what it holds and understand why;
- The school must be prepared to respond to subject access requests within statutory time limits;
- The school must be able to amend, delete or transfer data promptly upon any justified request;
- Personal data collected should be auditable as far as possible and
- Personal data must be held securely and accessed only by those with reason to view it.

IICSA, child protection and document retention

In the light of the Independent Inquiry into Child Sexual Abuse and various high-profile safeguarding cases, the School recognises the emphasis currently being placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting.

This policy has been drafted in full awareness of these considerations. The school's policy is not to embark on the wholesale deleting of historic staff and pupil files, or any material potentially relevant for future cases, even if it has been held for long periods already. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.

The present focus on safeguarding does not mean that existing laws in respect of data protection or confidentiality are now in suspension, nor that the School may not still be liable for breaches of The General Data Protection Regulation (EU) 2016/679 (GDPR) (such as retaining personal data longer or in greater volume than *is necessary for its purpose*, or a failure to keep the data accurately or safely).

The School will already find legal support for lifetime retention of adequate and accurate records where they are of potential relevance to historic cases. However, the School is aware that the longer large amounts of personal data are held, the more onerous our exposure to subject access rights (individual requests for data) and data breach. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not), or details as to physical or mental health, should be kept securely and shared or accessible only on a need-to-know basis. Where a competent authority requests such information, there is likely to be an obligation to cooperate but legal advice will be sought.

The school's policy when a child protection file is passed on to a new school, as required whenever a pupil is being transferred, is to retain its own copy of the file.

The School needs to weigh the threat of historic abuse claims against that of relatively minor data protection contraventions. In such circumstances, where practical resources mean that it is not feasible to conduct a thorough review, then the School will err on the side of retention, rather than disposal, of historic insurance, staff and pupil files except where no living person could bring a claim.

Legal and Practical Considerations

In determining our retention periods a balance has been struck between the benefits of keeping detailed and complete records with practical considerations of storage, space and accessibility. In addition legal requirements in respect of retention of records and documents have been borne in mind. These include:

- 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
- The General Data Protection Regulation (EU) 2016/679 (GDPR)

These inform not only minimum and maximum retention periods, but also what to keep and who should be able to access it.

Definitions

1. 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 the DPA.

An example of personal data would be the Single Central Record or a pupil file; however, a "record" of personal data could be simply the holding of an email on the school's systems.

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.

<u>Digital records</u>

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data must as a minimum be password-protected and held on a limited number of devices only, with passwords provided on a need-to-know basis and regularly changed. 'Cloud storage' may only be used in limited circumstance agreed by the Head, Finance Director and IT Manager. If personal information kept in this way is sensitive, or held in large quantities, digital encryption is required.

Emails (whether they are retained electronically or printed out as part of a paper file) are also "records".

A digital document's original metadata may indicate the date of its creation, its author or the history of its changes: this information must be preserved.

Paper records

Paper records must be kept in a safe and secure store, especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.

Under the DPA, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not.

However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the DPA.

2. Personal data

Some records will contain information about individuals e.g. staff, pupils, consultants, parents, contractors. Particular legal requirements will therefore apply.

That type of information is likely to amount to 'personal data' for the purposes of the GDPR and therefore be subject to data protection laws which may, in places, conflict with aspects of these 'document retention' guidelines. Neither the statutory time limits by which legal claims must be made, nor the precise stipulations of private contracts or governmental organisations (eg the Disclosure and Barring Service, the 'DBS'), were necessarily drawn up with data protection law in mind.

The GDPR requires that personal data is only retained for as long as necessary i.e. is necessary for the specific lawful purpose (or purposes) it was acquired. This will vary and may be shorter or longer than the suggested document retention period, according to context. This may therefore require tailored, specific advice on a case-by-case basis.

As a general rule, statutory legal duties, or the duty to report to safeguard vital interests, will 'trump' data protection concerns in the event of any contradiction. Certain personal data may legitimately need to be retained or disclosed subject to a private contractual duty (e.g. under a parent contract).

3. Archiving and the destruction or erasure of Records

All staff receive basic training in data management in issues such as security, recognising and handling sensitive personal data, safeguarding etc. Staff given specific responsibility for the management of records receive specific training and ensure, as a minimum, the following:

- 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 taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks, or

mobiles devices) 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;

- Questions of back-up or migration are 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) are supported by robust contractual arrangements providing for security and access;

- 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.

4. Litigation

Records may not be disposed of until the limitation period for bringing a claim has passed. For most contracts that will mean 6 years from any breach (or 12 years in case of, say, a witnessed deed), but the date to start counting from is the last day of the period under contract. Where there has been early termination, this will be the relevant date to apply (once the appeal process has been concluded): but for pupils, limitation periods will only apply from the age of 18 years.

The period of 6 years also applies to many claims outside contract (such as fraud, mistake or negligence). For discrimination cases it is usually only 3 months. In the case of personal injury, and some other negligence claims, it is 3 years. However, if the harm is only discovered later – e.g. 'latent' damage, or some unseen injury – then the timer only starts from the point of discovery: subject, in the case of latent property damage, to a 15-year backstop.

In some cases the prompt may be the end of a calendar year, so for the School policy a contingency is generally built in (e.g. 7 years where the statutory limitation is 6 years).

Finally, limitation periods may be disapplied altogether by courts in the case of certain crimes or associated breaches of care (e.g. historic abuse), whether a charge is brought by the police or a school is sued under a private claim. It is not always possible to try a case where the evidence is inadequate, including due to a lack of corporate memory (e.g. records and witnesses). However, as recent cases and IICSA (the Independent Inquiry into Child Sexual Abuse) have shown, authorities will expect to see a full and proper record and inferences may be drawn otherwise.

Insurance documents will not be personal data and relevant historic policies need to be kept for as long as a claim might arise.

5. Secure disposal of documents

Confidential, sensitive or personal information must be securely disposed of, in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

RETENTION PERIODS

Type of Record/Document	**Retention Period**
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	Permanent
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
• Assessment results (external or internal)	7 years from pupil leaving school
• Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth (subject where relevant to safeguarding considerations). Any material which may be relevant to potential claims should be kept for the lifetime of the pupil.
• Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

SAFEGUARDING	
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (if held)	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.
• Accident / Incident reporting	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).
• Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. 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).

CORPORATE RECORDS	
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Minutes, Notes and Resolutions of Boards or Management Meetings	Permanent
• Shareholder resolutions	Permanent
• Register of Members/Shareholders	Permanent (10 years for ex-members/shareholders)
• Annual reports	Permanent
ACCOUNTING RECORDS	
• Accounting records	Minimum – 7 years
• Tax returns	Minimum – 7 years
• VAT returns	N/A
• Budget and internal financial reports	Minimum – 5 years

CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	13 years from completion of contractual obligation or term of agreement
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, 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 licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	7 years from completion of contractual obligation concerned or term of agreement

EMPLOYEE / PERSONNEL RECORDS	
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (not certificate)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 12 years
• Pension or other benefit schedule records	Permanent
• Job application and interview/rejection records (unsuccessful applicants)	6 months
• Immigration records	4 years
• Health records relating to employees	7 years from end of contract of employment

<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.
• Employee and Public Liability Certificates	Permanent
• Correspondence related to claims/ renewals/ notification re: insurance	7 years
<u>ENVIRONMENTAL & HEALTH RECORDS</u>	
• Maintenance logs	10 years from date of last entry
• Accidents to children	25 years from birth (unless safeguarding incident)
• Accident at work records (staff)	4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances	7 years from end of date of use
• Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.

May 2018