READING BLUE COAT

GDPR - Data Retention Policy

This policy sets out the minimum periods of retention of the personal data that we process. The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors:

- 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
- Their accessibility.

However, there are legal considerations 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 for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and
- the General Data Protection Regulations and associated legislation.

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

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. The School may vary this policy or any parts of this procedure, including any time limits, as appropriate in any case.

Data Protection

This policy sets out how long student, employment and corporate and governance related data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's *Data Protection Policy* outlines its duties and obligations under the GDPR.

Child protection and document retention

In the light of the Independent Inquiry into Child Sexual Abuse and various high-profile safeguarding cases, all independent schools are aware of the emphasis currently being placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting. Regardless of suggested retention timescales set out below, the School may at its discretion extend this rule to any and/or all personnel and student files on a 'safety first' basis.

These guidelines have been drafted in full awareness of these considerations. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding

Meaning of "Record"

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

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.

Both paper and digital records will be stored securely and all appropriate measures taken to ensure the security of the data at all times.

Secure disposal of documents

When data is to be destroyed, this may be carried out by an appropriately licenced third party, with whom an appropriate Data Processing Agreement is in place.

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. Skips and 'regular' waste disposal will not be considered secure.

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

Where third party disposal experts are used they will be subject to adequate contractual obligations to the school to process and dispose of the information confidentially and securely.

Transferring information to other media and archiving

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

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives, primarily being digitised where possible or held securely in paper format.

The Head's Secretary is responsible for archiving and converting paper documents relating to students to digital media. The Assistant Bursar is responsible for data relating to other matters.

Timescales for retention

Except where there is a specific statutory obligation to destroy records, it is misleading to treat these suggestions as prescriptive 'time limits'. Figures given are not intended as a substitute to exercising thought and judgment, or taking specific advice, depending on the circumstances.

The figures suggested in this table are, in most cases, guides as to what are periods of reasonable necessity that could be defensible if challenged. Case by case decision making for documents would in theory be ideal, but in reality practical considerations mean that regular 'pruning' of records may not be an acceptable use of school resources. It is therefore accepted that sometimes a more systemic or broad-brush approach is necessary.

Responsibility and monitoring

The Data Protection Coordinator, in conjunction with the School is responsible for monitoring the policy's use and effectiveness and dealing with any queries on its interpretation. The Data Protection Coordinator will consider the suitability and adequacy of this policy and report improvements directly to the Senior Leadership Team and the Governors.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

TABLE OF SUGGESTED RETENTION PERIODS

Type of Record/Document	**Suggested Retention Period**
EMAILS ON SERVER 1. Student email account 2. Staff emails	1. Delete upon leaving school, or within one year 2. Routine deletion of historic emails after 2–3 years and delete account within 1 year of leaving the School.
SCHOOL-SPECIFIC RECORDS 1. Registration documents of School 2. Attendance Register 3. Minutes of Governors' meetings 4. Annual curriculum	1. Permanent (or until closure of the school) 2. 6 years from last date of entry, then archive. 3. 6 years from date of meeting 4. From end of year: 3 years (or 1 year for other class records: e.g. marks/timetables/ assignments)
INDIVIDUAL STUDENT RECORDS 1. Admissions: application forms, assessments, records of decisions 2. Student immigration records 3. Examination results (external or internal) 4. Student file including: a. Student reports b. Student performance records c. Student medical records 5. Special educational needs records (to be risk assessed individually)	***NB – this will generally be personal data*** 1. 25 years from date of birth (or, if student not admitted, up to 7 years from that decision). 2. Duration of student sponsorship plus minimum 1 year 3. 7 years from student leaving school 4. 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 student. 5. Date of birth plus up to 35 years (risk assessed)

SAFEGUARDING 1. Policies and procedures 2. DBS disclosure certificates (if held) 3. Accident / Incident reporting 4. Child Protection files 5. Video recordings of meetings	1. Keep a permanent record of historic policies 2. No longer than 6 months from decision on recruitment, unless police specifically consulted – but a record of the checks being made must be kept on the SCR/Personnel file, but not the certificate itself. 3. 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. 4. If a referral has been made / social care have been involved or child has been subject of a multi-agency plan, or there is a risk of future claims – indefinitely. 5. Where, for example, one on one meetings of classes, counselling or application interviews are recorded for safeguarding purposes, a shorter term retention policy is acceptable based on the DSL's view of how quickly a concern will be likely to be raised (eg3-6 months or immediately upon DSL review).
CORPORATE RECORDS (where applicable) 1. Certificates of Incorporation 2. Minutes, Notes and Resolutions of Boards or Management Meetings 3. Shareholder resolutions 4. Register of Members/Shareholders 5. Annual Report	1. Permanent (or until dissolution of the company) 2. Minimum- 10 years 3. Minimum – 10 years 4. Permanent (minimum 10 years from ex-members/shareholders) 5. Minimum – 6 years
ACCOUNTING RECORDS 1. Accounting records (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) 2. Tax returns 3. VAT returns 4. Budget and internal financial reports	1. 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. 2. Minimum – 6 years 3. Minimum – 6 years 4. Minimum – 3 years

CONTRACTS AND AGREEMENTS 1. Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments) 2. Deeds (or contracts under seal)	1. Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later 2. Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS 1. Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) 2. Assignments of intellectual property to or from the school 3. IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	1. Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years. 2. As above in relation to contracts (7 years) or, where applicable, deeds (13 years). 3. Minimum – 7 years from completion of contractual obligation concerned or term of agreement.
EMPLOYEE / PERSONNEL RECORDS 1. Single Central Record of employees 2. Contracts of employment 3. Employee appraisals or review 4. Staff personnel file 5. Payroll, salary, maternity pay records 6. Pension or other benefit schedule records 7. Job application and interview/rejection records (unsuccessful applicants) 8. Staff Immigration Records 9. Work Sponsor Records 10. Health Records relating to employees 11. Low level concerns records about adults (where applicable ad under a school policy	***NB these records will contain personal data*** 1. Keep a permanent record of all mandatory checks that have been undertaken (but do not keep DBS certificate itself: 6 months as above) 2. 7 years from effective date of end of contract. 3. Duration of employment plus minimum of 7 years 4. As above, but do not delete any information which may be relevant to historic safeguarding claims. 5. Minimum – 6 years 6. Possibly permanent, depending on nature of scheme 7. Minimum 3 months but no more than 1 year 8. Minimum 2 years from end of employment 9. Minimum 1 year from end of employment 10. 7 years from end of employment 11. Regular review recommended in order to justify longer term retention as part of safeguarding files.
INSURANCE RECORDS 1. Insurance policies (will vary – private, public, professional indemnity 2. Correspondence related to claims/ renewals/ notification re: insurance	1. 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. 2. Minimum – 7 years (depending on what the policy covers and whether eg historical claims could be made)

ENVIRONMENTAL & HEALTH RECORDS 1. Maintenance logs 2. Accidents to children 3. Accident at work records (staff) Minimum – 4 years from date of accident, but review 4. Staff use of hazardous substances 5. COVID 19 risk assessments, consent etc (for now: to be subject to further review) 6. Risk assessments carried out in respect of above) 7. Article 30 GDPR records of processing activity, data breach records, impact assessments	1. 10 years from date of last entry. 2. 25 year from birth (longer for safeguarding incident) 3. Minimum – 4 years from date of accident, but review case by case where possible 4. Minimum – 7 years from end of date of use 5. Retain for now legal paperwork (consents, notices, risk assessments) but not individual test results 6. 7 years from completion of relevant project, incident, event or activity. 7. No limit (as long as no personal data held) but must be kept up to date, accurate and relevant.

Author(s):	Tom Tabrah (Bursar)
Date:	February 2022
Review Frequency:	Bi-Annually
Next Review Date:	February 2024
Approval:	Pete Thomas (Head)
Date of Agreement:	February 2022