Retention of Records and Data Storage Protocol

1. This Protocol

1.1. The Ladies' College, comprising Melrose (including the Pre-Preparatory department), the Senior School and the Sixth Form (together the "**College**") recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the College. This document provides the framework through which this effective management can be achieved and audited.

1.2. This Protocol applies to all records created, received or maintained by colleagues (i.e. staff, comprising employees and contractors (as the case may be)) throughout the College in the course of carrying out its functions. In this Protocol, "**students**" means pupils of Melrose and students of the Senior School and the Sixth Form; and "**parents**" means parents, guardians and carers. "**Records**" are defined as those documents or items of data which contain evidence or information relating to the College, its students or colleagues and which facilitate the business and activities carried out by the College. These records are, in each case, thereafter retained (for a set period) to provide evidence of the transactions, business or activities of the College, its students or colleagues. These records may be created, received, maintained or stored in hard copy or electronically.

1.3. The suggested retention period for each type of information or item of data is set out in Appendix 1.

2. Responsibilities

2.1. The Bursar as Data Protection Officer has overall responsibility for this Protocol.

2.2. Individual members of staff must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with this Protocol. All data, whether in current filing systems or archived, must be kept secure at all times and in line with applicable policies.

3. Child Protection and Document Retention – Caveat

3.1. In light of the Independent Inquiry into Child Sexual Abuse and various high-profile safeguarding cases, ISBA (the Independent Schools' Bursars Association) have advised that independent schools do NOT embark on a policy of deleting historic staff and student files, or any material potentially relevant for future cases, even if it has been held for long periods already.

3.2. This advice does not preclude us archiving data; and it makes it more important that our archiving is well organised so that we can respond to Subject Access Requests on a timely basis, **but deletion of data is on hold until we receive further guidance from ISBA**.

4. Safe Disposal of Records

4.1. Where records have been identified for destruction, they should be securely disposed of in an appropriate way. All paper records or images containing personal, confidential or sensitive information, including special category data and sensitive commercial information, should be shredded before disposal using a cross cut shredder, or by contracting with an approved contractor to dispose of the information (under appropriate and adequate contractual obligations to the College). No such documents should be put in the wastepaper bins, regular paper recycling bins or a skip. There should be no risk of re-use, disclosure or reconstruction of such records or the information contained in them. Devices for digital storage and recordings should be dismantled or broken into pieces. Particular consideration should be given to ensuring the secure disposal for digital or hard copy records containing sensitive or special category data or large quantity data.

4.2. We are required to maintain a list of records which have been destroyed together with who authorised their destruction.

4.3. Departments are responsible for maintaining an electronic Archive Log which documents (i) what is stored where, so that, in the case of a Subject Access Request, data can be quickly located, or (ii) that there is evidence to support that it has been destroyed in accordance with this Protocol – a proforma Archive Log is included as Appendix 2.

5. Location and Access to Storage

5.1. All records (whether electronic or hard copy) should be stored securely and those that are archived should be stored securely with restricted access. Departments must know where their documents are stored (and record this on the Archive Log).

Appendix 1: Suggested Time Limits for Record Retention[1]

The table below gives suggested time limits for record retention based on both the States of Guernsey Education Services and ISBA guidance. Beyond these time limits records should be disposed of securely (as per point 4 above) unless they are determined to be required for longer (for example for a legal reason) or are to be retained within the College's formal archives.

[1] The retention periods are either based on legal requirements or are as otherwise determined by the College. There should be regular reviews of records to ensure it is appropriate to continue to hold the relevant records; this should also take into account the practical considerations for retention (such as considering any potential legal claim limitation period against whether it is reasonable (from a data protection perspective) to continue to hold certain data).

Type of Data	Normal Retention Period
EMAILS ON SERVER	
Pupil email account	Automatic deletion 90 days after leaving school.
Staff email account	Automatic deletion 90 days after leaving school or, if contents are required for business continuity purposes, routine archiving of account (accessible only to IT staff and other colleagues as needed) after leaving. Account deleted once no longer required.

STUDENTS (NB these records will contain personal data)	
Documents relating to admission: application forms, assessments, records of decisions	DOB of the student + 25 years (or up to 7 years from the student leaving). If unsuccessful application: up to 1 year after decision.
Student Records, including medical (not accidents), academic achievements & conduct and Records of Achievement	DOB of the student + 25 years (*except that name, date of birth and parents' address retained permanently).*
Examination results – Public	Permanent.
Special Educational Needs files, reviews and Individual Education Plans (*risk assess individually*)	DOB of the student + up to 35 years. *Do NOT delete any information relevant to historic safeguarding considerations/ any materials which may be relevant to potential claims without legal advice, even following culmination of a cas*e. *NOTE: States of Guernsey advise that some authorities choose to keep files for a longer period of time to defend themselves in any future case.*

SAFEGUARDING	
Policies, procedures and insurance	Keep a permanent record of historic policies.
DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless police specifically consulted, or with consent. A record of the checks being made must be kept on Single Central Record of employees / HR file, but not the certificate itself.
Accidents or incident reporting	DOB of the student + 25 years or for as long as a living victim may bring a claim (if longer). Ideally, files to be

	reviewed from time to time if resources allow and a suitably qualified person is available.[2] *Do NOT delete any information relevant to historic safeguarding considerations/ any materials which may be relevant to potential claims without legal advice, even following culmination of a case.*
Child Protection files (including those held electronically)	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): indefinitely.
Video recordings of meetings	Where e.g., 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 likely be raised: e.g., 3-6 months or immediately upon DSL review.
Trips & Visits: contact, health information & parental permission (including information held electronically) • No major incident • Major incident on trip (**Major incident** defined as either being major in scale affecting many students or where the conduct and supervision of the school is under question)	• If no major incident, on return of trip. • If a major incident, DOB of the student involved + 25 years or for as long as any living victim may bring a claim (if longer). Regular review recommended to justify longer term retention using a responsible assessment policy. The permissions slips for **all** students on the trip need to be retained to show that the procedure had been followed for all students.

COLLEAGUES/ PERSONNEL RECORDS (NB these records will contain personal data)	
Single Central Record of Employees	Retain permanent record that mandatory checks have been undertaken (but *do NOT keep DBS certificate for more than 6 months unless (as above) with consent or police specifically consulted*).
Contract of employment	7 years from effective date of end of employment.
Appraisals and last reference	Duration of employment and minimum 7 years after end of employment.

[2] [The English High Court has found that a retention period of 35 years was within the bracket of legitimate approaches for retaining safeguarding records. The UK ICO (Information Commissioner's Office) still expects to see a regular review policy in place (e.g. every 6 years), although the High Court also held that could be a disproportionate use of resource for many organisations' safeguarding teams.]

Personnel Files	As above, but *do NOT delete any information which may be relevant to historic safeguarding claims*.
Payroll, salary, maternity pay records	Minimum – 6 years.
Pension or other benefit schedule records	Potentially permanent (i.e. lifetimes of those involved), depending on nature of scheme.
Disciplinary Proceedings: • Verbal warning • Written warning • Decision to terminate	• Verbal warning – Note of informal meeting held permanently on personnel file. • First written warning remains active for six months; a record of the warning is retained permanently on the colleague's personnel file. • Final written warning remains active for 12 months; a record of the warning is retained permanently on the colleague's personnel file. • Record in retained on the colleague's personnel file. *Do NOT delete any warning where any disciplinary proceedings relate to a child protection matter.*
Capability Proceedings: • Informal discussions • Performance improvement notice • Final performance improvement notice • Decision to terminate	• Note of informal meeting held permanently on personnel file • Normally remains on record for 6 months from the date it is put in place, unless extended. • Normally remains on record for 6 months from the date it is put in place, unless extended. • Record in retained on the colleague's personnel file.
Job application & interview/rejection records (unsuccessful applicants)	6 months – unless we have consent to keep their details on file.
Information relating to those on the Supply List / supervised / unsupervised volunteers	If application not completed or unsuccessful – 6 months. If application successful, 7 years (as for permanent colleagues) from effective date of end of employment/end of most recent activity.
Staff immigration records (Right to work, etc.)	Minimum – 2 years from end of employment.
Health records relating to employees	7 years from end of employment.
Low-level concerns records about adults (*where applicable and under a school policy)*	File note for duration of employment. Regular review recommended to justify longer term retention as part of child protection policy.

SCHOOL SPECIFIC RECORDS	
Attendance register	Held online and archived annually but available.
Annual curriculum	From end of year: minimum of 3 years for overall time table

HEALTH & SAFETY[3]	
Accident Reports – Children	DOB of the student + 25 years or for as long as a living victim may bring a claim (if longer). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. *Do NOT delete if relates to a child protection matter.*
Accident Reports – Adults	Date of Incident + 7 years or for as long as a living victim may bring a claim (if longer). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
Maintenance logs	Minimum of 10 years from date of last entry or longer to cover lease period.
Control of Substances Hazardous to Health (COSHH) records	Minimum 7 years from end of use
Asbestos Management: records where employees and persons are likely to have come into contact with asbestos	Last action + minimum 40 years to cover lease period.
Risk assessments for above	7 years from completion of the relevant project, incident, event or activity.
Covid-19 risk assessments, consents etc. (for now; this to be subject to further review)	Retain for now legal paperwork (consents, notices, risk assessments) but not individual test results.

[3] Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. Therefore, keep a note of all procedures as they were at the time and keep a record that they were followed. Keep the relevant insurance documents.

CORPORATE[4]	
Registration documents of the College	Permanent.
Minutes of Board and Committee meetings	Indefinite.
SLT and other internal minutes	Minimum 7 years for SLT minutes and others making significant decisions (*do NOT delete any minutes that relate to a child protection matter).*

ACCOUNTING RECORDS	
Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained and which give a true and fair view of the company's financial state) • Transactional – e.g.: approved invoices subsequently entered onto accounting system • Accounting records, bank statements • Annual Reports	• Minimum 3 years. • Minimum 7 years. • Permanent.
Budget and internal financial reports	Minimum – 3 years.

CONTRACTS & AGREEMENTS	
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later. (English law governed contracts which are deeds or signed under seal – minimum 13 years from completion of contractual obligations or term of agreement.)

INSURANCE POLICIES	
Insurance policies	Duration of policy (or as required by the policy) plus a period for any run-off 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/notifications	Minimum 7 years (but this will depend on what the policy covers and whether e.g. historic claims may still be made).

[4] Retention period for tax/legal purposes should be made by reference to legal and accountancy advice.

CCTV	
On-system data	90 days (Auto-deleted).
Internally exported data	1 year, with annual review to retain or destroy.
Access logs	7 years.

INTELLECTUAL PROPERTY RECORDS	
Formal documents of title (trademark or registered design certificates; patent or utility model certificates)	Permanent (for rights which can be permanently extended). Otherwise, expiry of right plus minimum of 7 years. Do NOT delete as long as up-to-date and relevant (as long as no personal data held).
Assignments of intellectual property to or from the school	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.
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	As above in relation to contracts (7 years) or, where applicable, English law deeds (13 years). Minimum – 7 years from completion of contractual obligation concerned or term of agreement.

DATA PROTECTION	
Data protection records documenting processing activity, data breaches	No limit (as long as no personal data held). Permanent. Do NOT delete as long as up-to-date and relevant.

Appendix 2 Proforma Archive Log

The table below sets out the information that needs to be recorded on an Archive Log for each Department:

Archive Box No.	Date Range From: To:	Contents /Description	Archive Location	Owner	Destruction Date	Approval for Destruction	Date Destroyed	Method & By Whom – Internal /External?

- An Archive Log (as shown above) should be **kept for each department or area (not individually)** and summarise all items stored in the Archives.

- **Archive Boxes must be sequentially numbered** so that all boxes can be accounted for.

- T**he Archive Box should be clearly labelled with the relevant details above** (Archive Box No. through to Destruction Date).

- Approval for Destruction should be given by the Principal or the head of the relevant department or area, taking into consideration if there is any legal action or child protection issues outstanding.

- Archived data that is being destroyed in accordance with this Protocol, but not logged when archived initially, should also be noted down so that a record is maintained of how it has been dealt with.