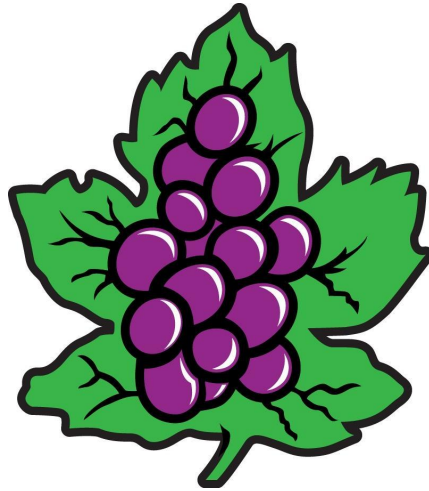


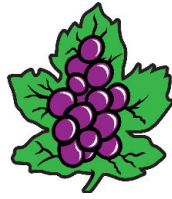


DATA RETENTION POLICY

Kerem School

Approved by: Compliance Committee **Date:** September 2021

Last reviewed on: August 2026 **Next review due by:** August 2027



KEREM SCHOOL

(This policy also applies to the Early Years Foundation Stage)

Data Retention Policy

Kerem School seeks to balance the benefits of keeping detailed and complete records - for the purposes of good practice, archives or general reference - with practical considerations of what is reasonable. This includes the consideration of storage, space and accessibility. We are mindful of the legal considerations in respect of retention of records and documents which include: - statutory duties and government guidance relating to schools; - the law of confidentiality and privacy; - disclosure requirements in the course of litigation; - contractual obligations; - the Data Protection Act (DPA). These will inform not only minimum and maximum retention periods, but also what to keep and how to keep it. This policy should be read alongside Kerem School's Data Protection Policy.

Meaning of Record

For the purposes of this Policy, a 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 will contain personal data of individuals as defined in the DPA, but not all. 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.

Digital records

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data, or any large quantity of data, will be wherever possible password-protected and held on a limited number of devices only, with passwords provided on a need-to-know basis and regularly changed. Emails (whether they are retained electronically or printed out as part of a paper file) are also records and may be particularly important: whether as disclosable documents in any litigation or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record.

Paper records

Paper records will wherever possible be stored in dry secure conditions. Staff procedures are in place to archive paper records to a central facility within the school at certain times of the year.

Archiving and the destruction or erasure of records

All staff must follow the basic training in data management that they received on induction and on issues such as security, recognising and handling sensitive personal data, safeguarding, etc. Staff given specific responsibility for the management of records must have specific training and ensure the following:

- Records - whether electronic or hard copy - are stored securely as above, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable. Paper records will be kept in locked cupboards or filing systems. Electronic records will be kept on devices that are password-protected.
- When important records, and large or sensitive personal databases, are taken home (whether paper or digital) they are kept securely. Paper records will be kept in locked cupboards or filing systems. Electronic records will be kept on devices that are password-protected.
- Questions of backup 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.
- 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).
- 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 reconstruction, of any records or information contained in them.

Retention Periods

General basis of suggestion:

Some of these periods will be mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011), but in the majority of cases, these decisions are up to the institution concerned. The suggestions will therefore be based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection. There might be occasions for long-term, lifetime or indefinite keeping of records relating to safeguarding incidents. NB. The Goddard Inquiry needs to be taken into consideration when considering data retention and disposal.

Type of Record/Document	Retention Period
SCHOOL-SPECIFIC RECORDS	
Registration documents of School	Permanent
Attendance Register	6 years from the last date of entry, then archive
Minutes of Governors' meetings	Minimum 6 years from the date of the meeting - then archived

Mark books and key assessments	3 years after pupils leave school
INDIVIDUAL PUPIL RECORDS - this will generally be personal data	
Admissions: application forms, assessments, records of decisions	25 years from the date of birth (or, if the pupil is not admitted, up to 7 years from that decision).
Examination results (external or internal)	7 years from the pupil leaving school
Pupil file including: · Pupil reports · Pupil performance records · Pupil medical records	ALL: 25 years from date of birth (subject to, where relevant, safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil)
Special educational needs records (<i>to be risk-assessed individually</i>)	Records should be passed to the next educational establishment. If not, these are kept up to 35 years from the date of birth (allowing for special extensions to the statutory limitation period)
SAFEGUARDING	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	<u>No longer than 6 months</u> from the recruitment decision, 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). Ideally, files are to be reviewed from time to time if resources allow and a suitably qualified person is available. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (e.g. every 6 years) in place. (Goddard Inquiry July 2018)

Child Protection files	If a referral has been made / social care has been involved or the child has been subject of a multi-agency plan – indefinitely. If low-level concerns, with no multi-agency action – these will be kept indefinitely.
ACCOUNTING RECORDS (<i>Retention period for tax purposes should <u>always</u> be made by reference to specific legal or accountancy advice</i>)	
<i>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)</i>	6 years from the end of the financial year in which the transaction took place
Gift Aid claims	6 years
Budget and internal financial reports	Minimum - 3 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 a contractual obligation or term of the agreement
IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS - this will be personal data	
Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but <u>not</u> DBS certificate itself: 6 months as above)
Contracts of employment	Duration of employment plus 7 years from the end of the contract
Employee appraisals or reviews and staff personnel file	Duration of employment plus 7 years from the end of the contract
Staff personnel files	As above, but <u>do not delete any information that may be relevant to historic safeguarding claims</u>
Payroll, salary, maternity pay records	7 years from the end of the tax year

Pension records	Possibly permanent, depending on the nature of the scheme
Job application and interview/rejection records (unsuccessful applicants)	3 months or up to 1 year if appropriate
Immigration records	Duration of employment plus 7 years from the end of the contract
Health records relating to employees	Duration of employment plus 7 years from the end of the contract
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.
Correspondence related to claims/ renewals/ notification re: insurance	7 years or longer if there is an ongoing claim
ENVIRONMENTAL & HEALTH RECORDS <i>(Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this: so keep a note of all procedures as they were at the time, and keep a record that they were followed. Also keep the relevant insurance documents.)</i>	
Compliance checklist	Minimum 5 years
Accidents to children	25 years from birth (unless there has been a safeguarding incident)
Accident at work records (staff)	Minimum - 4 years from the date of the accident, but review case-by-case where possible
Staff use of hazardous substances	7 years from the end of the date of use.
Risk assessments (carried out in respect of the above)	7 years from completion of relevant project, incident, event, or activity.
Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data is held)

CLOUD STORAGE AND DATA PROTECTION

As part of its ICT Infrastructure Kerem School uses Google, which utilises a cloud-based storage system. Likewise, the School backs up the data on its network using a cloud-based service provided by Google. Google guarantees school data is stored within the EU.