Sponsor	**DFO**
Issue Date	**July 2020**
Next Review Date	**June 2021**
Committee	**Estates**

WOLDINGHAM SCHOOL

DATA RETENTION & STORAGE POLICY

1. Aims

Woldingham 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 storage, space and accessibility. There are legal considerations in respect of retention of records and documents which must be borne in mind by all staff. All aspects of Data Protection are covered by Woldingham Schools Data Protection Policy.

2. Data Storage.

Information and records relating to pupils, parents and staff will be stored securely and will only be accessible to authorised school staff. Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. See Appendix 1 for school guidelines.

It is Woldingham Schools responsibility, through the Director of IT, to ensure all personal and school data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party. This and other data and system security matters are covered in Woldingham Schools Information Security policies.

3. Meaning of "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 will contain personal data of individuals as defined in the Data Protection Act.

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 - should 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. Where 'cloud storage' is used, the IT department will confirm what data needs to be made available in this way.

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.

It is also worth remembering that a digital document's original metadata may indicate the date of its creation, its author or the history of its changes: so it is important that this information is preserved.

Paper records. Paper records are to be stored in dry and secure conditions. Paper records are to be 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 e.g. an alphabetical personnel file split into marked dividers. Personal information contained on print-outs taken from electronic files also falls under the DPA.

4. Personal Data. Some records will contain information about individuals eg. staff, pupils, consultants, parents, contractors - or indeed other individuals, whether they are a part of the school or some other third party (for example, another school). That type of information is likely to amount to "personal data" for the purposes of the DPA and therefore be subject to data protection laws which *may*, in places, conflict with aspects of these guidelines.

As a general rule, statutory legal duties 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 (eg under a parent contract).

5. Archiving and the Destruction or Erasure of Records. All staff are to receive basic training/awareness in data management - issues such as security, recognising and handling sensitive personal data, safeguarding, etc, on induction and periodic staff INSET training thereafter. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, the following:

- That records - whether electronic or hard copy - are stored <u>securely</u> 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;
- That 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 data sticks or mobiles and handheld electronic tablets) unless absolutely necessary, *in which case* it should be subject to a risk assessment and in line with the IT use policy;
- That questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and <u>not</u> individual *ad hoc* action;
- That arrangements with external storage providers - whether physical or electronic (in any form, but most particularly "cloud-based" storage) - are supported by <u>robust contractual arrangements</u> providing for security and access;
- That 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
- That 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.

6. Litigation. The school will be well placed to deal with claims if it has a strong corporate memory - including adequate records to support its position, or a decision that was made.

Records are not to 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). In the case of personal injury it is only 3 years. However, if the harm is only discovered later - eg '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.

The most important steps Woldingham School takes to support our policy is:

- having adequate notices and consents in both staff and parent contracts;
- ensuring any long-term records worth keeping are kept very secure, accessible only by trained staff on a need-to-know basis. Insurance documents need to be kept in respect of historic policies for as long as a claim might arise.

7. Recording Information. It is important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed - whether as a result of litigation or investigation, or because of a subject access request under the DPA. **The watchwords of record-keeping are therefore accuracy, clarity, professionalism and objectivity**.

8. Secure Disposal of Documents. 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 are not 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.

Where third party disposal experts are used they are to be supervised by the Director of IT, under adequate contractual obligations to the school to process and dispose of the information securely.

Appendices:

1. Woldingham School Document Retention Periods.
2. Woldingham School Exam Centre Requirements.

Appendix 1
TABLE OF WOLDINGHAM SCHOOL RETENTION PERIODS

This table:

- Guides staff to identify the key types of document concerned.
- Focuses attention on particular issues associated with those types of document.

If in any doubt staff are to speak with the DFO.

The essence of this policy is the necessity of exercising thought and judgment - albeit that practical considerations mean that case-by-case 'pruning' of records may be impossible. It is accepted that sometimes a more systemic or broad-brush approach is necessary, which is where the table comes in.

Type of Record/Document	**Retention Period**	**Lead:**
SCHOOL-SPECIFIC RECORDS • Registration documents of School	Permanent (or until closure of the school)	Registrar
• Attendance Register	6 years from last date of entry, then archive.	Registrar
• Minutes of Governors' meetings	6 years from date of meeting	DFO
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)	Dep Head - Academic
INDIVIDUAL PUPIL RECORDS	***NB - this will generally be personal data***	
• 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).	Registrar / Head's PA
• Examination results (external or internal)	7 years from pupil leaving school	Dep Head - Academic / Exams Officer

• Pupil file including:
  • Pupil reports
  • Pupil performance records
  • Pupil medical records
	ALL: 25 years from date of birth*
	
	* *unless there is good reason to consider this may be applicable evidence in a medical negligence or abuse claim:* see 'Safeguarding' below.
		Registrar / Head's PA

• 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)	HoD / SEN
SAFEGUARDING		
• Policies and procedures	Keep a permanent record of historic policies	Deputy Head Operations

• DBS disclosure certificates (potentially sensitive personal data & must be secure)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted - but keep a record of the fact that checks were undertaken, if not the information itself).	Head's/DFO's PA Pers Manager
• Incident reporting	Keep on record for 35 years, ideally reviewed regularly (eg every 6 years) if a suitably qualified person is available and resources allow. **	DFO
Limitation periods can be disapplied in criminal or civil abuse cases. However, rights under the DPA and insurers' requirements remain relevant.	**Courts may be sympathetic if not, but the ICO (Information Commissioner's Office) will expect to see a responsible assessment policy in place.	
CORPORATE RECORDS (where applicable) • Certificates of Incorporation	Permanent (or until dissolution of the company)	DFO / Financial Controller
• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum - 10 years	DFO / Financial Controller
• Shareholder resolutions	Minimum - 10 years	DFO / Financial Controller
• Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)	DFO / Financial Controller
• Annual reports	Minimum - 6 years	DFO / Financial Controller
ACCOUNTING RECORDS • 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)* [NB specific ambit to be advised by an accountancy expert]	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	Financial Controller
• Tax returns	Minimum - 6 years	Financial Controller
• VAT returns	Minimum - 6 years	Financial Controller
• Budget and internal financial reports	Minimum - 3 years	Financial Controller

CONTRACTS AND 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	DFO / Director of IT / Financial Controller
• Deeds (or contracts under seal)	Minimum - 13 years from completion of contractual obligation or term of agreement	DFO / Financial Controller
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.	DFO
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).	DFO
• IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	Minimum - 7 years from completion of contractual obligation concerned or term of agreement	Director of IT
EMPLOYEE / PERSONNEL RECORDS • Contracts of employment	***NB this will almost certainly be personal data*** Minimum - 7 years from effective date of end of contract	DFO / Head of HR
• Employee appraisals or reviews and staff personnel file	Duration of employment plus minimum of 7 years	DFO / Head of HR
• Payroll, salary, maternity pay records	Minimum - 6 years	Financial Controller
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme	Financial Controller
• Job application and interview/rejection records (unsuccessful applicants)	Minimum - 3 years (but see note of DBS disclosure certificates above)	Head of HR
• Immigration records	Minimum - 4 years	Head of HR
• Health records relating to employees	Minimum of 7 years from end of contract of employment	Head of HR
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.	DFO

• Correspondence related to claims/ renewals/ notification re: insurance	Minimum - 7 years	DFO
ENVIRONMENTAL & HEALTH RECORDS • Maintenance logs • Accidents to children3	10 years from date of last entry 25 years from birth (unless safeguarding incident)	DFO / Estate Manager
• Accident at work records (staff)3	Minimum - 4 years from date of accident, but review case-by-case where possible	DFO
• Staff use of hazardous substances3 • Risk assessments (carried out in respect of above)3	Minimum - 7 years from end of date of use 7 years from completion of relevant project, incident, event or activity.	DFO

FOOTNOTES:

General basis of suggestion:

The suggestions will 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.

1. Retention period for tax purposes should always be made by reference to specific legal or accountancy advice.
2. 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.

Appendix 2
Woldingham School Exam Centre Requirements.

As an Approved Exam Centre Woldingham School follows the General Regulations from the Joint Council for Qualifications (JCQ). This requires all candidates to sign a Data Protection Notice to acknowledge the use of the following personal data by Woldingham School and the exchange of personal data with various exam boards relating to exam entries.

a. Personal data relating to the name(s), date of birth, gender, unique candidate identifier (UCI) and unique learner number (ULN) of an individual candidate will always be collected by an awarding body for the purposes of examining and awarding qualifications. In some cases additional information, which may include sensitive personal data relating to health, will also be collected to support requests for access arrangements and reasonable adjustments and/or special consideration. Such personal data will be supplemented by the results of examinations and assessments undertaken by the respective candidate.

b. A candidate's personal data will only be collected from registered examination centres in the context of examination entries and/or certification claims.

c. Such data collected will not be used by an awarding body other than for the administration of the examinations process, conducting assessments and the certification of results claims.

d. Personal data within candidates' work will be collected and processed by an awarding body for the purposes of marking, issuing of examination results and providing candidates with access to post-results services. Examination results will be retained for a minimum of forty years.

e. In order for an awarding body to achieve this, some personal information may be transferred to third parties such as examiners, who may in some instances, reside outside the European Economic Area.

f. Awarding bodies may be required to provide a candidate's personal data to educational agencies such as DfE, WG, DENI, The Skills Funding Agency, Ofqual, HESA, UCAS, Local Authorities, EFA and Learning Records Service (LRS). Additionally, candidates' personal data may be provided to a central record of qualifications approved by the awarding bodies for statistical and policy development purposes.6. Some of the information candidates supply will be used by the Skills Funding Agency to fulfil its statutory functions, issue/verify a candidate's Unique Learner Number (ULN) and update/check a candidate's Personal Learning Record.

g. The Skills Funding Agency may share a candidate's ULN and Personal Learning Record with other education related organisations, such as a careers service, a candidate's school or college, Government Departments and public bodies responsible for education. Further details of how information is processed and shared can be found at: http://www.learningrecordsservice.org.uk/

h. Awarding bodies are obliged to confirm what personal data is held, what it is held for, to whom the data are to/may be disclosed, and disclose the information that

they hold about data subjects, (e.g. the candidates) within 40 days of receiving a formal request for disclosure, subject to the application of any relevant exemptions under the Data Protection Act 1998.