



WALTHAMSTOW HALL SEVENOAKS

Records: Retention and Storage Policy **Including The Early Years Foundation Stage (EYFS)**

To be read in conjunction with all Safeguarding Policies

Walthamstow Hall will seek 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. Legal considerations, in respect of retention of records and documents must be borne in mind; these include:

- The Data Protection Act (2018) (DPA18).
- The General Data Protection Regulation (UKGDPR).
- Statutory duties and government guidance relating to schools.
- The law of confidentiality and privacy.
- Disclosure requirements in the course of litigation.
- Contractual obligations.

These will inform not only minimum and maximum retention periods, but also what to keep and how to keep it.

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 UKGDPR and DPA18, 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.

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

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, consider what data needs to be made available in this way. If personal information kept in this way is sensitive, or held in large quantities, digital encryption is advisable.

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.

Video / audio recordings

Particularly given the recent rise of remote provision of lessons, meetings, assessments and interviews, we are increasingly capturing many gigabytes of personal data (some of it impactful and personal).

The reasons for recording such virtual sessions may vary: from seeking to keep a record as a resource for those unable to attend at the time (notably for group or assembly sessions), via classes where a pupil was absent (e.g. owing to having to self-isolate), down to safeguarding reasons (e.g. for one on one lessons, VMT or counselling sessions, or application interviews).

Such recordings are also digital records and – depending to a degree on both their contents and how they are stored / tagged – may be deemed the personal data of anyone identifiable from the recording. How long they may be kept, therefore, should be judged in the same way any other type of record is: for what purpose is it kept, and how long is it necessary to keep it?

However, common sense dictates that not all such recordings will be necessary for long-term legal or safeguarding purposes. In practice, this would be expensive and unmanageable in storage terms, and could create unnecessary burdens (subject access rights, for example) and data security risks. SMG, DSL and IT teams should collectively agree what a feasible storage period is *based on what is a likely period in which a complaint or concern will generally be raised* following a virtual lesson or meeting (or when reviews or spot checks will be carried out, if sooner). This should be led by the safeguarding advice but – unless something arises that means it should be treated as a record of an incident – is unlikely to be more than 3 months.

Paper records

Paper records must not be kept in damp or poor storage conditions; but as well as applying common sense (i.e. dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper), security is also vital - especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.

Under UKGDPR, paper records are only classed as personal data if held in a qualifying "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. Remember: the DPA is only one consideration in retaining records, so it is preferable to keep paper documents ordered and accessible.

A note on "personal data"

Some records will contain information about individuals e.g. 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). Particular legal requirements will therefore come into play.

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 '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 (e.g. the Disclosure and Barring Service, the 'DBS'), were necessarily drawn up with data protection law in mind.

For example, UKGDPR requires that personal data is only retained for as long as necessary – that is, necessary for the specific lawful purpose (or purposes) it was acquired. This will of course vary and may be either shorter or longer than the suggested document retention period, according to context. This is a nuanced area which 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).

However, a higher standard would apply to the processing of "sensitive personal data". By way of example a contractual duty, or other legitimate interest of the School or third party, would not of itself justify the retention or sharing of sensitive personal data – but 'protection of vital interests' might. Sensitive personal data includes data relating to an individual in respect of their health, race, religion, sexual life, trade union membership, politics or any criminal proceedings, offences or allegations.

A record of concern, suspicion or allegation should be made at the time or as soon as possible after the event making use of CPOMS. (N.B. It is not advisable to make a written record whilst a child is disclosing abuse, as it may deter the child from speaking). Records should be factual, using the child's own words in cases where a disclosure is made. Professional opinion can be given, but needs to be supported by stating the facts and observations upon which the opinions are based. **(N.B. expressing an opinion as to whether the child is telling the truth is not helpful and can prejudice how a case proceeds).** Any handwritten records should be dated and signed with the name of the signatory clearly printed and filed in chronological order. It is useful to use the School 'Contact Note' pro-forma for recording information / concerns if CPOMS is not available. Any handwritten notes made immediately after the event, for example, a disclosure can act as evidence of them having been written at the time for any future court case. Therefore, these should not be destroyed if the details are recorded more formally at a later time, but instead kept securely attached to the child protection concern forms used. They can be scanned to CPOMS for retention. All recorded child protection concerns must be passed to the Designated Safeguarding Lead (DSL) as soon as possible. The DSL will need to make a professional judgement about what action needs to be taken in accordance with our child protection procedures.

The common law of confidentiality, data protection and human rights principles must be adhered to when obtaining, processing or sharing personal or sensitive information.

Confidential information is:

- Personal information of a private or sensitive nature.
- Information that is not already lawfully in the public domain or readily available from another public source.
- Information that has been shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

In summary, DPA18 requires that records should be accurate, relevant, kept up to date and securely kept for no longer than is necessary for the purpose. It is important to make it clear to pupils that any disclosure they make will be treated with sensitivity but may need to be shared with other professionals if it is considered necessary to protect the child or someone else from harm.

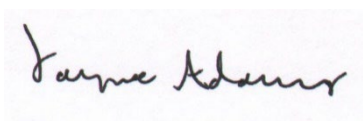
Archiving and the destruction or erasure of Records

All staff should receive basic training in data management - 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, as a minimum, the following:

- That 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.
- 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 CDs or 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 an up-to-date 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 not 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 robust contractual arrangements 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).
- 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.

This is particularly important in respect of the School's specific legal obligations under UKGDPR. However, they amount to common sense rules even where personal data is not directly involved.

Reviewed: March 2023
Next review date: March 2024



Signed:

Mrs J Adams
Chairman of the Governing Body

Date: 17 March 2023

Type of Record/Document	Retention Period
<u>Emails on Server</u>	
<ul style="list-style-type: none"> Pupil email account Staff emails 	Delete upon leaving School, or upon 1 year Routine deletion of historic emails after 2-3 years, and delete account within 1 year of leaving school
<u>SCHOOL-SPECIFIC RECORDS</u>	
<ul style="list-style-type: none"> Registration documents of School 	Permanent (or until closure of the School)
<ul style="list-style-type: none"> Attendance Register 	6 years from last date of entry, then archive.
<ul style="list-style-type: none"> Minutes of Governors' meetings 	6 years from date of meeting, then to the Archive.
<ul style="list-style-type: none"> Annual curriculum 	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
<u>INDIVIDUAL PUPIL RECORDS</u>	<i>NB - this will generally be personal data</i>
<ul style="list-style-type: none"> 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).
<ul style="list-style-type: none"> Examination results (external or internal) 	7 years from pupil leaving School
<ul style="list-style-type: none"> Pupil file including: <ul style="list-style-type: none"> Correspondence Parent contact details Pupil reports Pupil performance records Pupil medical records** 	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil).
<ul style="list-style-type: none"> Special educational needs records (<i>to be risk assessed individually</i>) 	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
<u>SAFEGUARDING</u>	
<ul style="list-style-type: none"> Policies and procedures 	Keep a permanent record of historic policies
<ul style="list-style-type: none"> DBS disclosure certificates (potentially sensitive personal data & must be secure) 	<u>No longer than 6 months</u> from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on SCR / personnel file, but not the certificate itself.
<ul style="list-style-type: none"> Incident reporting – all documents to be encrypted and password protected. 	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.
<ul style="list-style-type: none"> Child Protection files 	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. The School records low-level concerns, if there has been no multi-agency action, consider whether or not the child needs to be named in any record concerning an adult, or if a copy should be kept on the child protection file.
<ul style="list-style-type: none"> Audio/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.

<u>CORPORATE RECORDS</u> (where applicable)	e.g. the School's trading arms
<ul style="list-style-type: none"> Certificates of Incorporation 	Permanent (or until dissolution of the company)
<ul style="list-style-type: none"> Minutes, Notes and Resolutions of Boards or Management Meetings 	Minimum - 10 years
<ul style="list-style-type: none"> Shareholder Resolutions 	Minimum - 10 years
<ul style="list-style-type: none"> Register of Members/Shareholders 	Permanent (minimum 10 years for ex-members/shareholders)
<ul style="list-style-type: none"> Annual reports 	Minimum - 6 years
<u>ACCOUNTING RECORDS</u> <i>(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)</i>	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.
<ul style="list-style-type: none"> Tax returns 	Minimum - 6 years
<ul style="list-style-type: none"> VAT returns 	Minimum - 6 years
<ul style="list-style-type: none"> Budget and internal financial reports 	Minimum - 3 years

<u>CONTRACTS AND AGREEMENTS</u>	
<ul style="list-style-type: none"> Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>) 	Minimum - 7 years from completion of contractual obligations or term of agreement, whichever is the later
<ul style="list-style-type: none"> Deeds (or contracts under seal) 	Minimum - 13 years from completion of contractual obligation or term of agreement
<u>INTELLECTUAL PROPERTY RECORDS</u>	
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Assignments of intellectual property to or from the School 	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
<ul style="list-style-type: none"> 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

<u>EMPLOYEE / PERSONNEL RECORDS</u>		<i>NB this will almost certainly be personal data</i>
<ul style="list-style-type: none"> Single Central Record of employees 		Keep a permanent record that mandatory checks have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above)
<ul style="list-style-type: none"> Contracts of employment 		Minimum - 7 years from effective date of end of contract
<ul style="list-style-type: none"> Employee appraisals or reviews and staff personnel file 		Duration of employment plus minimum of 7 years Do not delete any information which may be relevant to historic safeguarding claims.
<ul style="list-style-type: none"> Payroll, salary, maternity pay records 		Minimum - 6 years
<ul style="list-style-type: none"> Pension or other benefit schedule records 		Possibly permanent, depending on nature of scheme
<ul style="list-style-type: none"> Job application and interview/rejection records (unsuccessful applicants) 		Minimum 3 months but no more than 1 year
<ul style="list-style-type: none"> Immigration records 		Minimum - 2 years from end of employment
<ul style="list-style-type: none"> Health records relating to employees 		Minimum of 7 years from end of contract of employment

<ul style="list-style-type: none"> Low-level concerns records about adults 	Regular review recommended in order to justify longer-term retention as part of safeguarding files.
<u>INSURANCE RECORDS</u>	
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Correspondence related to claims/ renewals/ notification re: insurance 	Minimum - 7 years
<u>ENVIRONMENTAL, HEALTH & DATA</u>	
<ul style="list-style-type: none"> Maintenance logs 	10 years from date of last entry
<ul style="list-style-type: none"> Accidents to children 	25 years from birth (longer for safeguarding)
<ul style="list-style-type: none"> Accident at work records (staff) 	Minimum - 4 years from date of accident, but review case-by-case where possible
<ul style="list-style-type: none"> Staff use of hazardous substance 	Minimum - 7 years from end of date of use
<ul style="list-style-type: none"> Covid-19 risk assessments, consents, notices etc. (subject to further review) 	Retain for now any legal paperwork but not individual test results
<ul style="list-style-type: none"> Risk assessments (carried out in respect of above) 	Minimum - 7 years from end of date of use 7 years from completion of relevant project, incident, event or activity.
<ul style="list-style-type: none"> Data protection records documenting processing activity, data breaches 	No limit: as long as up-to-date and relevant (as long as no personal data held)