



Data retention policy

This Policy

The purpose of this policy is to set out the policy for data retention at Giggleswick School ("the School").

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, but not all, will contain personal data of individuals. 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.

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.

Paper records should be stored in appropriate, secure conditions (dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper). 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.

Records management

All records – whether electronic or hard copy – must be 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.

Important records, and large or sensitive personal databases, must not be 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 controls put in place which include security of the portable device, password protection and appropriate lock screen settings.

Arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – must be supported by robust contractual arrangements providing for security and access.

Reviews should be conducted on a regular basis, in line with the guidance in this policy, 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).

Data destruction

All destruction or permanent erasure of records, if undertaken by a third party, must be carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.

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 should be shredded using a cross-cutting shredder; devices for digital storage 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 should ideally be supervised but, in any event, under adequate contractual obligations to the School to process and dispose of the information.

Table of retention periods

Type of Record/Document	Retention Period
<p>SCHOOL-SPECIFIC RECORDS</p> <ul style="list-style-type: none"> • Registration documents of School • Attendance Register • Minutes of Governors' meetings • Annual curriculum 	<p>Permanent (or until closure of the School)</p> <p>6 years from last date of entry, then archive.</p> <p>6 years from date of meeting</p> <p>From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)</p>
<p>INDIVIDUAL PUPIL RECORDS</p> <ul style="list-style-type: none"> • Admissions: application forms, assessments, records of decisions • Examination results (external or internal) • Pupil file including: <ul style="list-style-type: none"> ○ Pupil reports ○ Pupil performance records ○ Pupil medical records • Special educational needs records (<i>to be risk assessed individually</i>) 	<p><i>NB – this will generally be personal data</i></p> <p>25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).</p> <p>7 years from pupil leaving school</p> <p>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 pupil.</p> <p>Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period).</p>
<p>SAFEGUARDING</p> <ul style="list-style-type: none"> • Policies and procedures • DBS disclosure certificates (if held) • Accident / Incident reporting • Child Protection files 	<p>Keep a permanent record of historic policies</p> <p><u>No longer than 6 months</u> from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.</p> <p>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.</p> <p>If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).</p>

Type of Record/Document	Retention Period
<p><u>CORPORATE RECORDS</u></p> <ul style="list-style-type: none"> • Certificates of Incorporation • Minutes, Notes and Resolutions of Boards or Management Meetings • Shareholder resolutions • Register of Members/Shareholders • Annual reports 	<p>Permanent (or until dissolution of the company)</p> <p>Minimum – 10 years</p> <p>Minimum – 10 years</p> <p>Permanent (minimum 10 years for ex members/shareholders)</p> <p>Minimum – 6 years</p>
<p><u>ACCOUNTING RECORDS</u></p> <ul style="list-style-type: none"> • Accounting records • Tax returns • VAT returns • Budget and internal financial reports 	<p>Minimum – 3 years for private UK companies (except where still necessary for tax returns)</p> <p>Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place</p> <p>Internationally: can be up to 20 years depending on local legal/accountancy requirements</p> <p>Minimum – 6 years</p> <p>Minimum – 6 years</p> <p>Minimum – 3 years</p>
<p><u>CONTRACTS AND AGREEMENTS</u></p> <ul style="list-style-type: none"> • Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>) • Deeds (or contracts under seal) 	<p>Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later</p> <p>Minimum – 13 years from completion of contractual obligation or term of agreement</p>
<p><u>INTELLECTUAL PROPERTY RECORDS</u></p> <ul style="list-style-type: none"> • Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) • Assignments of intellectual property to or from the school 	<p>Permanent (in the case of any right which can be permanently extended, e.g. trademarks); otherwise expiry of right plus minimum of 7 years.</p> <p>As above in relation to contracts (7 years) or, where applicable, deeds (13 years).</p>

Type of Record/Document	Retention Period
<ul style="list-style-type: none"> IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents) 	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
<p><u>EMPLOYEE / PERSONNEL RECORDS</u></p> <ul style="list-style-type: none"> Single Central Record of employees Contracts of employment Employee appraisals or reviews Staff personnel file Payroll, salary, maternity pay records Pension or other benefit schedule records Job application and interview/rejection records (unsuccessful applicants) Immigration records Health records relating to employees 	<p><i>NB this will contain personal data</i></p> <p>Keep a permanent record that mandatory checks have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above)</p> <p>7 years from effective date of end of contract</p> <p>Duration of employment plus minimum of 7 years</p> <p><u>As above, but do not delete any information which may be relevant to historic safeguarding claims.</u></p> <p>Minimum – 6 years</p> <p>Possibly permanent, depending on nature of scheme</p> <p>Minimum 3 months but no more than 1 year</p> <p>Minimum – 4 years</p> <p>7 years from end of contract of employment.</p>
<p><u>INSURANCE RECORDS</u></p> <ul style="list-style-type: none"> Insurance policies Correspondence related to claims/ renewals/ notification re: insurance 	<p>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.</p> <p>Minimum – 7 years</p>
<p><u>ENVIRONMENTAL, HEALTH & DATA</u></p> <ul style="list-style-type: none"> Maintenance logs Accidents to children ⁴ 	<p>10 years from date of last entry</p> <p>25 years from birth (longer for safeguarding)</p>

Type of Record/Document	Retention Period
<ul style="list-style-type: none"> • Accident at work records (staff) • Staff use of hazardous substances 	<p>Minimum – 4 years from date of accident, but review case-by-case where possible</p> <p>Minimum – 7 years from end of date of use</p>
<ul style="list-style-type: none"> • Risk assessments (carried out in respect of above) 	<p>7 years from completion of relevant project, incident, event or activity.</p>
<ul style="list-style-type: none"> • Data protection records documenting processing activity, data breaches 	<p>No limit: as long as up-to-date and relevant (as long as no personal data held)</p>

Reviewed by: MZ Hodge, Bursar and Data Protection Coordinator
 Review period: Annual
 Updated: August 2020
 Next review date: August 2021