Aysgarth School

GDPR Data Storage and Retention policy

Responsibility of Andrew Francis
Reviewed 1st September 2019 and to be reviewed 1st September 2020

TABLE OF SUGGESTED RETENTION PERIODS

Type of Record/Document	**Suggested [1] Retention Period**
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	Permanent (or until closure of the school)
• Minutes of Governors' meetings	Permanent (or until closure of the school)
• Annual curriculum	Permanent (or until closure of the school)
INDIVIDUAL PUPIL RECORDS	***NB – this will generally be personal data***
• Admissions: application forms, assessments, records of decisions	Permanent (or until closure of the school) for those pupils admitted. For pupils that do not enroll, 7 years after the year of application
• Examination results (external or internal)	Permanent (or until closure of the school)
• Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	Permanent (or until closure of the school) subject where relevant to safeguarding considerations. Any material which may be relevant to potential claims should be kept for the lifetime of the pupil.
• Special educational needs records (*to be risk assessed individually*)	Permanent (or until closure of the school)

SAFEGUARDING	
• Policies and procedures • DBS disclosure certificates (if held)	Keep a permanent record of historic policies No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
• Accident / Incident reporting/RIDDOR	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. [2]
Child Protection files	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. Permanent (or until closure of the school) A red flag note is to be placed in a child's folder alerting one to the fact that there is data content held in a separate and secure Child Protection file that may be pertinent. A copy of all Child Protection notes must he handed on the the child's next School.

CORPORATE RECORDS (where applicable)	**eg *where schools have trading arms***
● Certificates of Incorporation	Permanent (or until dissolution of the company)
● Minutes, Notes and Resolutions of Boards or Management Meetings	Permanent (or until closure of the school)
● Shareholder resolutions	Permanent (or until closure of the school)
● Register of Members/Shareholders	Permanent (or until closure of the school)
● Annual reports	Permanent (or until closure of the school). Records held with Accountants and Companies House

ACCOUNTING RECORDS [3]	
● 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 – 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
● Tax returns	Minimum – 6 years
● VAT returns	Minimum – 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*) ● Deeds (or contracts under seal)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
● Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) ● Assignments of intellectual property to or from the school	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years. As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
● IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB this will almost certainly be personal data***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (not certificate)

• Contracts of employment	Permanent (or until closure of the school)
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file including; Health records relating to employees	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	Possibly permanent, depending on nature of scheme
● Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
● Immigration records	Minimum – 4 years
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	Minimum – 7 years
ENVIRONMENTAL & HEALTH RECORDS	
• Maintenance logs	10 years from date of last entry
• Accidents to children [4]	25 years from birth (unless safeguarding incident)
● Accident at work records (staff) [4]	Minimum – 4 years from date of accident, but review case-by-case where possible
● Staff use of hazardous substances [4]	Minimum – 7 years from end of date of use
● Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event or activity.

FOOTNOTES:

1. General basis of suggestion:

   Some of these periods will be mandatory legal requirements (eg 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.

2. 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 (eg every 6 years) in place.

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

4. 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.

Guidelines for Independent Schools on the Storage and Retention of Records and Documents (ISBA / Farrer & Co LLP)

[Please note this is guidance not legal advice, and schools' particular needs will vary: it is recommended that each school creates and follows its own policy, under advice as required]

Note 1: GDPR and document retention

The forthcoming General Data Protection Regulation (GDPR) from 25 May 2018 does not fundamentally change the principles for length of document retention – it is still a question of relevance and purpose, as well as data security.

It does, however, have stricter rules about use and storage of personal data generally with the practical effect of requiring more dynamic, efficient and secure storage systems – such that:

- All information held by schools needs to be justifiable, by reference to its purpose;
- The school must be transparent and accountable as to what it holds and understand why;
- Schools must be prepared to respond more quickly to subject access requests;
- Schools must be able to amend, delete or transfer data promptly upon any justified request;
- Personal data collected should be auditable as far as possible; and
- Personal data must be held securely and accessed only by those with reason to view it.

In practice these purposes must be explained to those affected – parents, pupils, ex-pupils, staff – although that is not to say a school's specific data retention periods need to be public. However, the basic principles do need to be communicated as part of its Data Protection Policy [link].

Note 2: IICSA, child protection and document retention

In the light of the Independent Inquiry into Child Sexual Abuse and various high-profile safeguarding cases, all independent schools will be aware of the emphasis currently being placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting. Many will be extending this rule to all personnel and pupil files on a 'safety first' basis.

This note has been drafted in full awareness of these considerations. It is strongly to be recommended in the current climate that schools do not embark on a policy of deleting historic staff and pupil files, or any material potentially relevant for future cases, even if it has been held for long periods already. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.

What should also be emphasised is that the present focus on safeguarding does not mean that existing laws in respect of data protection or confidentiality are now in suspension, nor

that schools may not still be liable for breaches of the Data Protection Act 1998 (such as retaining personal data longer or in greater volume than *is necessary for its purpose*, or a failure to keep the data accurately or safely).

Schools will already find legal support for lifetime retention of adequate and accurate records where they are of potential relevance to historic cases. However, schools should be aware that the longer they hold large amounts of personal data, the more onerous their exposure to subject access rights (individual requests for data) and data breach. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not), or details as to physical or mental health, should be kept securely and shared or accessible only on a need-to-know basis. Where a competent authority requests such information, there is likely to be an obligation to cooperate: but it may be appropriate to seek legal advice.

Some DSLs advise when schools pass on a child protection file to a new school, as required whenever a pupil is being transferred, that they should delete their own copy. We do not consider that necessary or appropriate in the current environment, or in light of possible future litigation, any more than it would apply to a pupil leaving the school at the normal academic age.

In due course we expect more settled guidance from the relevant authorities on striking this balance. In the meantime, the threat of historic abuse claims is to be weighed against that of relatively minor data protection contraventions. In such circumstances it would be very inadvisable to start disposing of historic insurance, pupil and personnel files except where no living person could bring a claim; and if practical resources mean that it is not feasible to conduct a thorough review, then schools should in the current climate err on the side of retention, rather than disposal, of staff and pupil files.

The purpose of this note

Schools will generally 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. However, whilst independent schools are not as directly regulated as state maintained schools, there are still legal considerations in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and (last but by no means least relevant)
- the Data Protection Act ("DPA"), to be replaced on 25th May 2018 (see below).

These will inform not only minimum and maximum retention periods, but also what to keep and who should be able to access it.

On 25th May 2018, the General Data Protection Regulation (GDPR) will take effect across the UK under a domestic Data Protection Bill.

Striking a balance

Even justifiable reasons to keep certain records, such as child protection records, for many years after pupils or staff leave the school will need to be weighed against personal rights. The longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative burden on schools, in terms of both secure storage and individual subject access rights.

Steps a school can take to support its retention policies are (a) communicating the reasons for the policy in privacy notices and staff or parent contracts; and (b) ensuring any records necessary to keep long-term are kept very secure, accessible only by trained staff on a need-to-know basis.

1. Meaning of "Record"

In these guidelines, "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 as defined in the DPA.

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.

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, 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.

Paper records

Paper records are most often damaged by 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 the DPA, paper records are only classed as personal data if held in a "relevant 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.

2. A note on "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). 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 (eg the Disclosure and Barring Service, the 'DBS'), were necessarily drawn up with data protection law in mind.

For example, the DPA 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 (eg 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.

3. 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); 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.

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

4. A note on litigation

One consideration in whether it is necessary or desirable to keep records is possible future litigation. Generally speaking, an institution will be better 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.

Ideally, therefore, records would not 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). For discrimination cases it is usually only 3 months. In the case of personal injury, and some other negligence claims, it is 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.

In some cases the prompt may be the end of a calendar year, so for the purpose of this guidance a contingency is generally built in (eg 7 years where the statutory limitation is 6 years).

Finally, limitation periods may be disapplied altogether by courts in the case of certain crimes or associated breaches of care (eg historic abuse), whether a charge is brought by the police or a school is sued under a private claim. It is not always possible to try a case where the evidence is inadequate, including due to a lack of corporate memory (eg records and witnesses). However, as recent cases and IICSA (the Independent Inquiry into Child Sexual Abuse) have shown, authorities will expect to see a full and proper record and inferences may be drawn otherwise.

Often these records will comprise personal or sensitive personal data (eg health or criminal allegations). In such instances, even justifiable reasons to keep records for many years will need to be weighed against personal rights. Recent 'historic' cases in the field of child protection make a cautious approach to record retention advisable and, from a DPA perspective, make it easier for a school to justify retention for long periods – even the lifetime of a pupil. The most important steps a school can take to support such a policy are (a) having adequate policies explaining the approach, including notices in both staff and parent contracts; and (b) ensuring any long-term records worth keeping are kept very secure, accessible only by trained staff on a need-to-know basis.

Insurance documents will not be personal data and relevant historic policies need to be kept for as long as a claim might arise.

5. The risks of longer retention

Notwithstanding the legal grounds and (in some cases) imperatives to do so, the longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative and storage burden on schools. This also increases the amount of material in respect of which schools must be accountable to data subjects (e.g.

information requests, "right to be forgotten" requests), and the consequences of data security breach become more serious.

Schools must take professional advice and decide for themselves where to draw the line in retaining data for these purposes: some may err on the side of caution and retain; others will apply a clear system for filleting pupil or personnel files, or indeed email folders, down to the information they think is likely to be relevant in the future. However, this is a decision that should always be made mindful of risk and knowledge of where historic incidents may have occurred or future complaints may arise.

It is also vitally 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.

6. A note on 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 will not be 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 should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information.

How to use the table of suggested retention periods

The table at the end of this guidance document has three main functions:

- it should help schools and staff identify the key types of document concerned.
- it should focus attention on any particular issues associated with those types of document.
- finally – and this needs to be emphasised – it acts as an outline guide only.

Note that, except where there is a specific statutory obligation to destroy records, it is misleading to present (or apply) any guidance as if it constitutes prescriptive time 'limits'. Figures given are not intended as a substitute to exercising thought and judgment, or take specific advice, depending on the circumstances.

Indeed, the essence of this guidance can be boiled down to 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.

Farrer & Co LLP

September 2017