KING WILLIAM'S COLLEGE

THE BUCHAN SCHOOL

King William's College, The Buchan School & The Buchan Nursery

Guidelines on Storage and Retention

of Records and Documents

Issue Date: 05/2021

Last Review Date: 06/2023

Next Review 06/2025

Moira Mackie
Chief Operating Officer

'The School' is defined as King William's College, The Buchan School and The Buchan Nursery (and includes the Barrovian Foundation, Bishop Barrow's Foundation and Bishop Barrow's Charity, as being related entities). The registered address of the School is King William's College, Castletown, Isle of Man (Registration Number: 000063M Charity Number: 1196)

Legal note 1: The legal framework around data and document retention in the UK

The Data Protection Act 2018 (**DPA**) and UK General Data Protection Regulation (**UK GDPR**), the retained UK version of GDPR following Brexit, are not prescriptive about the length organisations are able to retain documents or data – although sometimes specific document retention periods are set out in other sources of law or guidance (see the table at the bottom of this note).

The rule under data protection law is based on principle: that *personal* data (that is, data by which a living individual or 'data subject' may be identified) must not held for longer than is necessary for the particular lawful purpose for which it was collected[1]. Nor should 'data controllers' – such as schools – keep *more* personal data than is necessary for that purpose. In this way, UK GDPR requires schools to set policies reflecting these key data protection principles: but most actual retention periods are matters of judgment.

For some types of data long term retention is justified, although this draws in further questions around data security, erasure or access requests, and cost. The key considerations are as follows:

- All information held by schools needs to be justifiable by reference to a lawful purpose;
- Schools should have transparently explained what they collect and why to all its data subjects, including by reference to "*the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period*";[2]
- Schools must be accountable to individuals as to what they hold and, although there are limits to individuals' right of access, as a general principle data subjects can ask to see their data;
- As well as the right of subject access, schools must be able to amend, delete or transfer data promptly upon any valid request, or otherwise prepared to explain why they will not do so;
- Schools must also be accountable to the regulator (the Information Commissioner's Office, or **ICO**). This means schools understanding and being able to explain the reasons why they hold data – which also means keeping records of their processing activities (**ROPA**s)[3];
- It should be possible to audit how the personal data you hold was collected, and when; and
- Sensitive data (notably special category data, including around health and pastoral matters, or criminal allegations) must be held securely and accessed only by those with reason to view it. For certain purposes

[1] Article 5(1)(e) UK GDPR and section 39(1) of DPA 2018

[2] There is no requirement that a school's full data retention schedule (like the one attached to this guidance) needs to be included in its privacy notice or made publicly available. The ISBA's template privacy notice can be found here.

[3] The ICO has produced guidance around the documentation process required by Article 30 UK GDPR here and here, and has provided templates here. ROPAs do not contain personal data of any identifiable individuals, and as such can be kept indefinitely as legal records, but should be updated as required from time to time.

schools will need an "appropriate policy document"[4] explaining why the data is needed and what your intentions are in respect of erasure and retention.

Different rules and considerations will apply to genuine archiving of documents for their enduring value, as explained in ISBA's note with the School Archives and Records Association (SARA) found here.

Legal note 2: IICSA update (November 2022) and implications for document retention

From its launch in 2015, the Independent Inquiry into Child Sexual Abuse (**IICSA**) frequently spoke out about document retention[5]. All independent schools were duly put on notice of the need for long-term (lifetime or even indefinite) keeping of full records related to incident reporting and, whether or not core participants in the inquiry, were advised not to embark on a policy of deleting any material potentially relevant for future cases, even where data had been held for long periods already.

On 20 October 2022, IICSA published its final report (which can be found here, with IICSA's summary available here). As hoped, the final report did deal with the issue of document and data retention[6], drawing on both established legal principles and key lessons learned from actual cases, although for the most part it deferred the responsibility for producing guidance to the ICO itself. There is currently no timeline set for when the ICO will be producing this guidance.

The final report from IICSA did make one clear recommendation – that any data relating to child sexual abuse (**CSA**) allegations should be kept for 75 years, but subject to regular review.

IICSA's report acknowledges (at paragraph 70) that this may create burdens, even for purely electronic document storage. But the recommendation is a response to various issues IICSA encountered, such as (i) the varied approach by organisations to their data retention policies (as generally permitted by data protection law); (ii) cases where records having been destroyed had subsequently hindered investigation into allegations; and (iii) the difficulties faced by victims and survivors in being able to access their data, or the time that may need to lapse before they are ready to do so (see paras. 72 to 75 and 100 to 104).

IICSA's 75-year recommendation is not yet binding in law, nor reflected in ICO guidance. All IICSA's recommendations are made to government rather than directly to organisations. However, data protection law – being principles-based – does allow data controller organisations to make its own decisions as to how to process and retain data, based on all available lawful considerations and its reasonable aims.

As such, whilst not yet a legal requirement, it is open to schools to decide that 75 years is an appropriate period to adopt now for all child protection records[7]. It makes sense from a legal claim perspective, given that historic limitation periods can be set aside for CSA cases, and should be perfectly compatible with the current recommended policies of indefinite or lifetime retention of such records, that schools may already have in place. However, quite apart from the technical challenges in meeting the requirement (digitally or on paper), IICSA's recommendation does leave some critical questions unanswered, namely:

(i) What is meant by "regular review" – how detailed, how strict, and how often;

(ii) What, specifically, constitutes a CSA record – and what does not (IICSA refers at paragraph 69 of the report to "*specific records relating to child sexual abuse*" which could be interpreted narrowly. It also refers to "*inherent value to survivors*"); and

(iii) what retention period should be chosen for 'other' non-CSA records of safeguarding value (including low-level concerns).

The safest position for schools is to take a conservative (broad) approach to what is a CSA record until we have the detailed ICO guidance that has now been recommended, despite the associated burdens.

---

[4] Where required by Sch.1 the Data Protection Act 2018 (and as defined therein): the ICO has a template here.
[5] See e.g. here from 2015 and the November 2021 update here

[6] See paragraphs 66 to 71 of the report and Recommendation 17 (extracted in full below)

[7] This is in contrast to the current advice as to other recommendations in IICSA's report – which is in most cases to observe, consider and prepare for changes rather than enact them at this time.

In terms of where to draw the line as to what may constitute a child protection / safeguarding record:

(a) Whilst IICSA's focus is on CSA records, most if not all of the relevant considerations will apply to other forms of abuse in relation to children, including physical or emotional abuse and neglect. It would be both practical and appropriate therefore to apply the same retention period.

(b) This longer retention period can, and indeed should, safely be applied to potentially relevant documents wherever substantive abuse or neglect is reasonably suspected. Schools may decide to apply this longer retention period to all child protection files, depending on their capacity to conduct regular reviews upon a pupil leaving (see further below).

(c) Schools may also want to consider what could be relevant to future legal claims – whether or not the document itself directly concerns CSA, it could be relevant to how the school handled an issue or query. If so, similarly long retention periods can be justified.

(d) Historic insurance documents and relevant school policies in place at a particular time, which are not in any event likely to contain personal data, should be retained indefinitely.

However, for other documents the position may be less clear cut. For example:

(i) Pupil and personnel files will be subject to the usual rule of approximately 6-7 years' retention following departure from the school (or after school leaving age as applicable). Whilst these files may contain sensitive material, if policies on record keeping have been well followed then schools should be confident that they are not relying on such files as a repository of safeguarding information, that should be stored elsewhere (under need-to-know access).

(ii) Similarly, nothing relevant to CSA or safeguarding should be sitting long-term on email servers (see further below). This should all have been extracted and filed.

(iii) Medical records held by clinical staff may have value, but should generally be held separately and subject to retention principles applicable to practitioners under relevant clinical codes.

(iv) Records of low-level concerns are not going to constitute CSA records unless, individually or cumulatively, they have reached the threshold of a concern or allegation that meets the harm threshold (and therefore falls within clear guidance[8] on reporting, recording and managing). KCSIE is clear that low-level concerns records (**LLCs**) should be kept at least until the relevant staff member has left the school, but should ideally be reviewed for relevance at that point or otherwise in line with when the relevant personnel file is also marked for deletion. [9]

It is worth noting the IICSA recommendation (in relation to CSA records) that files should be subject to "regular review" – which is in line with best practice from a data protection perspective. Of course, it also imposes a further administrative burden requiring trained practitioner judgment (e.g. by a DSL).

There is case law[10] to suggest courts may be sympathetic to the real-world pressures on practitioners and organisations with safeguarding responsibilities. As a general rule, concerns about data protection issues should never put child safety at risk: if there is a risk that too draconian or burdensome a requirement to review documents for erasure might prove a disproportionate drain on key safeguarding personnel's time, or result in a 'short cut' approach that could risk routine erasure of important documents, then these may be fair considerations in terms of what is an achievable policy. These reasons should be recorded by way of justification, e.g. in the form of a data protection impact assessment (**DPIA**).

Schools should also be aware that the longer they hold large amounts of personal data, the more onerous their exposure to subject access or erasure requests and the risk of data security breaches. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not) – or details as to

[8] As seen in HM Government (2018) Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children (WTSC); and Department for Education (2022) Keeping Children Safe in Education: Statutory guidance for schools and colleges (**KCSIE**) (both accessed on 31 August 2022).

[9] Further detail on retention of LLCs is found in the Farrer & Co Low Level Concerns Guidance.

[10] *R (C) v Northumberland County Council & ICO* [2015] EWHC 2134 (Admin)

physical or mental health – should be kept securely, shared with or accessible to proper persons on a need-to-know basis.

There is also specific provision in the below table concerning low-level concerns and video recordings (e.g. for remote provision), to the extent these may be retained or reviewed in a safeguarding context.

What should also be emphasised, however, is that the need to prioritise safeguarding does not mean that existing laws in respect of data protection or confidentiality are in suspension, nor that schools may not still be liable for breaches of data protection legislation (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).

Final report text (October 2022): IICSA recommendation 17

> **Recommendation 17: Access to records**
>
> The Inquiry recommends that the UK government directs the Information Commissioner's Office to introduce a code of practice on retention of and access to records known to relate to child sexual abuse.
>
> The retention period for records known to relate to allegations or cases of child sexual abuse should be 75 years with appropriate review periods.
>
> The code should set out that institutions should have:
>
> - retention policies that reflect the importance of such records to victims and survivors, and that they may take decades to seek to access such records;
> - clear and accessible procedures for victims and survivors of child sexual abuse to access such records;
> - policies, procedures and training for staff responding to requests to ensure that they recognise the long-term impact of child sexual abuse and engage with the applicant with empathy.

Legal note 3: child protection files and KCSIE

When schools pass on a **child protection file** to a new school, as Keeping Children Safe In Education (**KCSIE**) requires (at paragraph 122) when a pupil under 18 is transferred, some DSLs and local authorities advise that schools should delete their own copy. That is not the view of ISBA's legal advisers.

Whilst this may be appropriate for maintained schools (where a single copy will be kept within the local authority system), for independent schools in the current environment – in light of IICSA's statement and possible future claims against the school – it is a clear risk to delete any records of incidents that occurred while the pupil was at the school, or any information that was relevant to what action the school took. That applies just as it would for a pupil leaving the school at the normal academic age.

Schools should also consider in the relevant circumstances exactly what needs to be shared and/or retained from the file. It should be noted that the requirement under KCSIE does not stipulate that the school must hand over the full child protection file, as it stood at the point of departure, without review or edit. Some critical judgment may need to be exercised in terms of what is actually necessary to pass on to the new school or college to ensure continuity of care and support for the pupil, and safety for others – in fair consultation with the child and/or their parents *if appropriate* (though of course this may be highly sensitive). In any event, redactions may be necessary to preserve third-party data of staff or other pupils and their families, if they may be identifiable by what is on the child protection file.

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. The following legal considerations apply to independent schools 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 e.g. KCSIE;
- disclosure and evidence requirements for potential future litigation;
- contractual and insurance obligations;
- the laws of confidentiality and privacy; and (last but by no means least relevant)
- GDPR and the DPA, which enshrines it in UK law.

These will inform not only minimum and maximum retention periods (the rationale for which should be notified to data subjects via privacy notices and, for more sensitive personal data, recorded in appropriate policy documents), but also what to keep and who should be able to access it.

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 GDPR.

An obvious example of a record containing personal data would be a database (such as a mailing list or the staff Single Central Record), or a pupil or personnel file specific to an individual. However, a "record" of personal data could arise simply by holding an email on the school's systems: your policies should ensure staff do not use email accounts or inboxes as proxy filing systems for key documents.

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 for retention purposes than its contents, and the reason for keeping it (although format is of course an important consideration in terms of how best to preserve documents securely).

Digital records

Many schools who have historically relied on paper records will have been going through a process of digitisation of existing records, perhaps over a number of years. This is generally to be encouraged.

However, 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 (ideally with two-factor authentication), with internal access on a need-to-know basis. Consideration should be given, either on an individual or (ideally) a policy basis, to when password protection should be applied to sensitive attachments to emails, or if secure links are preferable (see further below). Where 'cloud storage' or intranet access is used, consider what data needs to be made available to which users.

If personal information of any volume or sensitivity is permitted to be kept on personal devices, **digital encryption** is essential. That will usually be the difference between a lost laptop being a simple matter of the cost of the device, or a serous reportable data breach.

Email accounts and internal messaging systems

Emails and other internal messages – whether they are retained electronically or printed out as part of a paper file – are also "records" likely to contain personal data (of the sender, recipient, or a third party) in their body, footer, in the sent/received fields, or in attachments. As such they will potentially fall within the scope of a subject access request made against the school.

They may also contain particularly important information: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) in a subject access request. Again, however, school policy and training should mitigate against using email accounts as proxy filing systems.

It is our view that short term email retention policies of no more than 2 or 3 years – whether imposed on staff centrally, or as a requirement for each staff member to follow – will encourage the correct habits in terms of not relying on email accounts to retain important information, resources, contracts, legal advice, attendance notes, safeguarding concerns or incident reports that ought to be properly held elsewhere (i.e. in the appropriate file, accessed only by the appropriate persons).

Such policy and training must also stress to staff the great importance of care and professionalism in how such records are created by casual email (or other forms of instant messaging such as Team or Slack, which are also records for these purposes). This will become particularly apparent when a subject access request is made by a colleague, pupil or parent and the data recorded may need to be provided.

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 – or its deletion. Metadata may be necessary to examine under a legal claim or a data audit.

Records on personal devices including SMS / WhatsApp

Whether text / WhatsApp messages, and any other files or notes held by a staff member or governor on their personal device (including tablet or smartphone) counts as a school "record" will depend on the circumstances – and to a large extent the school's policies on the official use of such platforms.

As a general rule, an employee has an expectation of privacy in their own messaging for personal use, and is not subject to UK GDPR for solely domestic or 'household' uses of data.

However, where personal devices are used by employees or governors / trustees / board members for official school use – for example to discuss a pupil issue, parental complaint or disciplinary matter – it may be deemed an official record of the school. This means it may be disclosable in litigation or under a subject access request, if the school has reasonable grounds to believe relevant evidence or personal data might be found on the device, including by SMS, WhatsApp or personal email. In that sense, any staff or governor WhatsApp group must be used with the same professional formality as email.

What the school policy or handbook says about use of personal devices or personal / 'social media' messaging systems for official school purposes will be an important factor in assessing whether they are to be deemed searchable records. If staff members or governors are using their devices contrary to official policy, there are grounds to argue these should not be deemed school records under school control, and need not be searched.

Schools may seek to impose common-sense rules around how to use personal devices and manage data on them in a work context, what is acceptable "personal" use of school systems, and what is legitimate work use of social media. This has clear benefits in terms of certainty and digital governance, but there is a risk of thereby accepting a degree of legal responsibility for their use. See this note from ISBA.

Video / audio recordings

Particularly given the recent rise of remote provision of lessons, meetings, assessments and interviews, schools 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 child was absent (e.g. owing to having to self-isolate), down to safeguarding reasons (e.g. for one on lessons, VMT or counselling sessions, or application interviews). This throws up many issues, some of which are dealt with in this (Covid-specific) ISBA note, but one of them is retention.

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?

Some confusion has been caused by schools having notified users or parents that recordings are being kept for safeguarding purposes, and (as stated in some cases) for those purposes only. This can create issues if the recording is then needed for some other disciplinary, complaint or training purpose; it can also cause confusion as to how long a recording needs to be kept, with many schools operating a blanket policy of preserving all safeguarding-related records indefinitely.

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. Your school senior leadership team, 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. A similar approach may already be in place for short-term CCTV recording storage and review: see the ISBA CCTV policy and guidance note.

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 GDPR, 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 so searchable much as a digital database might be. By way of example, personnel files searchable by marked dividers will likely fall under within GDPR. A daily notebook, or diary, or chronological file of correspondence may not, unless it is readily clear to whom the file or notebook substantially relates: for example, a complaint or case file.

However, schools should not be tempted to retain or store personal data in disorganised or inaccessible hard copies, except as part of an appropriate archiving policy (which may be subject to an exemption from data protection rules around access and erasure in any event: see below). Schools are likely to remain responsible, as a principle of data security, for personal information contained on handwritten notes, print-outs taken from electronic files, or disclosures from their systems made orally. Remember: data protection law is only one consideration in retaining records, and it is far preferable for governance and legal reasons to keep paper documents ordered and accessible.

2. A note on "personal data": what it is, and when it is lawful to retain

Aside from purely charitable, corporate, estate or financial records (including asset lists, IP, accounts, contracts etc.), most records will contain information about living[11] individuals: e.g. pupils, parents, alumni, governors, staff (past, present and prospective), and consultants / contractors / VMTs. You will also likely hold professional contacts, including at other schools or local authorities, and supporter / donor lists. That type of information is likely to amount to "personal data" for these purposes, and therefore be subject to data protection laws which necessarily interact with these 'document retention' guidelines.

Generally, the sources of law that determine how long you retain personal data will not be GDPR or the DPA, but derive from elsewhere: e.g. statutory time limits by which legal claims must be made; the stipulations of your contracts; or the requirements of governmental organisations (e.g. the Disclosure and Barring Service, Charity Commission, IICSA etc.). As a general rule, in the event of any doubt or apparent contradiction with data protection law, statutory legal duties (including those under KCSIE / safeguarding) should be followed. However, data protection law is the overarching legal framework here and – properly understood and applied – does accommodate all these statutory duties on schools.

[11] Data protection rights and obligations do not apply to deceased individuals, even though they may be identifiable. Therefore lifetime retention periods, in terms of GDPR applicable, may equate to permanent retention.

What data protection law requires is simply that personal data is only retained for as long as necessary – and only as much as is necessary – for the specific lawful purpose (or purposes) it was acquired, or at least for clearly compatible purposes[12]. This will of course vary and, in accordance with the policies and processes adopted by your school, may be either shorter or longer than the suggested document retention period, according to context. This enters an area of context and judgment which may therefore require tailored, specific policy-making by your school on a case-by-case basis.

3. What is a lawful purpose to hold and retain personal data?

Most "ordinary" personal data may be processed in connection with a private contractual duty (e.g. under an employment or parent contract) or where necessary for a "legitimate interest" as defined in GDPR (which ought to be set out in your school's privacy notice). It may then be retained for a reasonable and necessary period of time afterwards, generally linked to legal claims.

However, a higher standard would apply to the processing of "*special category* [= sensitive] personal data", including notably health, trade union membership, ethnicity, religious beliefs, political views and sexual life. Similar rules apply to any records of criminal proceedings, offences or allegations. A mere contractual need to process, or a legitimate interest of the school or third party, would not in itself justify the retention of such personal data – but if it were necessary in connection with the defence of future legal claims, or to help prevent or detect crime or unlawful behaviour, or as part of the school's safeguarding duties, then a lawful GDPR or DPA basis to retain will arise.

4. Archiving, data management, 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 (alongside training in safeguarding and first aid, etc.) – at least every two years, in accordance with ICO guidance. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, 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;

- important records, and large or sensitive personal databases, are not left sitting in email accounts, 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). Where this is absolutely necessary, it should be subject to a risk assessment and in line with an up-to-date IT use policy;

- 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;

- arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage), and in whatever territory – are supported by robust, GDPR-compliant contractual arrangements providing for secure control, access and retrieval;

- 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

- 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 GDPR. However, they amount to common sense rules even where personal data is not directly involved.

Please be aware of the difference between *archiving* and *retention for a "live" purpose*, and refer to the SARA/ISBA note here. Record keeping for potential (rather than known) legal claims is a "live" purpose.

[12] This may include archiving in the public interest and statistical record-keeping, with suitable safeguards.

4. A note on litigation and limitation periods for claims

One consideration in whether it is necessary (or prudent) 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. Guidance from the ICO has suggested that records relevant to duties of care (for example, allergy information) may be processed on grounds of being necessary for defence of future legal claims. This is supportive to some degree of a "just in case" policy, but reasonable judgment should be exercised – especially where the data retained is impactful, surprising, or if an individual has reasonably objected.

Ideally, key records would not be disposed of until the limitation period for bringing a claim has passed. In respect of these periods, and how they are reflected in the template schedule, please note:

- In some cases, the "clock" may begin with a specific event, or when the claimant became aware of it; or it may be the end of a calendar year; but a school's review of any documents marked for deletion may be conducted annually at the end of a school year. Therefore, for the purpose of this guidance a contingency is generally built in: i.e. 7 years where the statutory limitation is 6.

- For most contracts the limitation will be 6 years from any breach (but 12 years in case of a witnessed deed), so the date to start counting from is the last day of the period under contract.

- The period of 6 years also applies to many claims outside contract (such as fraud, mistake or many common types of negligence / duty of care claim, from when the cause arose).

- In the case of personal injury, and some other types of negligence claims, it is only 3 years. However, if the harm is only discovered later – e.g. '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. See further below regarding historic abuse claims.

- Where termination of employment of a staff member is concerned, contractual claims may be brought up to 6 years later. For discrimination cases (which can of course apply to applications, and indeed pupils) it is usually only 3 months: however, where a contractual relationship was formed, the longer contractual period for claims will provide the necessary limitation backstop.

- Where there has been early exclusion of a pupil from the school, a parent may bring a claim under the parent contract for 6yrs from the point of termination. Be aware that application processes (for pupils) have a contractual element, although it is probably excessive to keep unsuccessful applications for the full 6/7 years unless the school is aware of a likely claim.[13]

- For pupils, limitation periods will only apply from when they reach the age of 18, and they may bring a negligence claim separately to their parents (hence the rule of 25 years from birth).

Insurance documents will not be personal data and relevant historic policies need to be kept for as long as a claim might arise. Finally, limitation periods may be disapplied altogether by courts in the case of certain crimes or associated breaches of care (e.g. 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 (e.g. 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 (e.g. 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 GDPR 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

[13] There may be administrative reasons for keeping records of applications beyond conclusion of the entry process: for example, if the pupil might try entry again the following cycle (i.e. within 1 year) or at a later entry stage. Such a policy should be notified at the point of application together with the chance to object.

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.

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 records handlers bear in mind, when creating documents and records of any sort (particularly email, but also video meeting recordings and internal staff messaging systems), 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 GDPR. The watchwords of record-keeping are therefore accuracy, clarity, professionalism and objectivity.

6. A note on secure disposal of documents and devices

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. For **hard copy** documents, skips and 'regular' waste disposal will not be considered secure. Paper records or images should be shredded using a cross-cutting shredder; devices for digital storage and recordings should be dismantled or broken into pieces. 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.

For **digital devices**, a number of individual steps are advisable prior to disposal: wiping the hard drive and/or activating drive encryption; uninstalling and/or deauthorising applications or accounts that could enable a user to access secure school systems (including wiping browsing history and cookies); and/or physically destroying the drive with a drill or hammer. Policies will be different according to whether devices are being recycled between staff or disposed of, but where schools allow a policy of using "own devices" then it must be clear that the same disposal polices apply to them, and that school IT support will be available if assistance is needed in safely destroying, wiping or readying devices for others.

How to use the table of suggested retention periods

The table below is, broadly, guidance rather than a template and 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; and
- finally – and this needs to be emphasised – it acts as an outline guide only. Except where stated, these are rarely terms imposed by specific law. Common sense can, and must, be applied.

Many schools will consider it appropriate to have a fuller and more comprehensive table. That is to be encouraged, but only where it is achievable, realistic and suitable for the school. It must be clear who has overall or departmental responsibility for each element or category of document. There is no point having a highly detailed retention schedule if it is confusing, impractical, or not followed in practice.

It is not suggested that schools need to include this level of detail in external privacy notices, or make the retention schedule publicly available. However, some indication of the basis for retention applied by the school should be set out in privacy notices, and when responding to access or erasure requests.

TABLE OF SUGGESTED RETENTION PERIODS

Except where there is a specific statutory obligation to destroy records, it is misleading to treat these suggestions as prescriptive time 'limits'. Figures given are not intended as a substitute to exercise of thought and judgment; specific advice, depending on the circumstances, may be appropriate. Other resources and/or template schedules are available to schools for determining retention periods, and it should not be considered that one is correct or authoritative where the other is not. Do however be mindful that some resources of this type are aimed at maintained schools, with different considerations.

The figures suggested in this table are, in most cases, guides as to what are periods of reasonable necessity that could be defensible if challenged. Some of these periods will be mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011, as applicable), 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.

Case-by-case decision making for documents may be ideal in theory, but practical considerations mean that regular pruning of records may not be an acceptable use of school resources. It is accepted that sometimes a more systemic or broad-brush approach is necessary, which is where the table comes in.

Please note: this is not an archiving policy, which is the subject of separate SARA/ISBA guidance. Schools should consider one of two actions at the end of a document's "life": secure deletion, or archiving.

Type of Record/Document	**Suggested Retention Period**
EMAILS ON SERVER	[*see note on email retention and storage*]
• Pupil email account	Delete upon leaving school, or within one year.
• Staff emails [*schools may wish to set their own policies, either centrally or with staff*]	Routine deletion of historic emails after 2-3 years, and delete account within 1 year of leaving school.
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	***NB these records will contain personal data***
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or up to 7 years from the pupil leaving). If unsuccessful: up to 1 year[1].
• Student immigration records	Duration of student sponsorship plus min. 1 year
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil file including: - Pupil reports and performance records - Pupil medical records (*not accidents*)	ALL: 25 years from date of birth (*subject where relevant to any material that may be relevant to potential historic claims: see below*). Date of birth plus up to 35 years (*risk assessed*)
• Special educational needs records	

SAFEGUARDING	[*see note on IICSA guidelines*]
• Policies, procedures and insurance	Keep a permanent record of historic policies
• DBS disclosure certificates (if held)	No longer than 6 months 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.
• 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 to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]
• Child Protection files and specific records of child sexual abuse	If a referral has been made / social care have been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years. [2]
• Video recordings of meetings	Where any one-on-one meetings of classes, counselling, or application interviews are recorded (e.g. 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.
CORPORATE RECORDS (where applicable)	**e.g. *where schools have trading arms***
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
• Shareholder resolutions	Minimum – 10 years
• Register of Members/Shareholders	Permanent (minimum 10 years for ex members/shareholders)
• Annual reports	Minimum – 6 years
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 Internationally: can be up to 20 years depending on local legal/accountancy requirements
• 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*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	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)	Permanent (in the case of any right which can be permanently extended, e.g. trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licenses and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB these records will contain personal data***
• Single Central Record of employees	Keep a permanent record that mandatory checks have been undertaken (but do not keep DBS certificate information itself: 6 months as above)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	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	Potentially permanent (i.e. lifetimes of those involved), depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year (as CVs will rapidly be out of date)
• Staff immigration records (Right to work, etc.)	Minimum – 2 years from end of employment
• Tier 2 migrant worker sponsor records	Minimum – 1 year from end of employment

• Health records relating to employees	7 years from end of employment
• Records of low-level concerns about adults	At least until end of employment (as recommended by KCSIE), then subject to review for relevance: e.g. 7 years from end of employment if they have ongoing relevance for employment claims, longer if necessary for safeguarding purposes / claims.
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 (*but this will depend on what the policy covers and whether e.g. historic claims may still be made*)
ENVIRONMENTAL, HEALTH & DATA	
• Maintenance logs	10 years from date of last entry
• Accidents to children [4]	25 years from birth (longer for safeguarding)
• 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
• Covid-19 risk assessments, consents etc. (*for now: this to be subject to further review*)	Retain for now legal paperwork (consents, notices, risk assessments) but not individual test results
• Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event or activity.
• Art.30 UK GDPR records of processing activity (**ROPAs**), data breach records, data protection impact assessments	No limit (as long as no personal data held), but must be kept up-to-date, accurate and relevant.

FOOTNOTES:

1. 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.

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 (e.g. 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.

CONCLUSION

The above guidelines are drawn from the ISBA reference library and (including the table) is not legal advice.

It should be noted that reference to legislation in this guidance is to UK legislation, pending further Isle of Man guidance in due course.

Our particular needs will vary therefore in all cases staff must seek guidance from the Chief Operating Officer if unsure about any aspect of these guidelines and before taking an action with regards the retention of records.

Moira Mackie
Chief Operating Officer
11 June 2023