Tandridge Learning Trust

Excellent Teaching
Inspiring Leadership
Innovative Training

Data Retention Policy

Drafted By	Governance Lead
Review By	Governance Lead
Status & Review Cycle	Annual (or when there are changes in legislation)
Next Review Date	Spring 2027

1. Introduction

This policy contains recommended retention periods for the different record series created and maintained by Tandridge Learning Trust. The schedule refers to all information whether it is held in hard copy or electronic format including cloud and web based or on third party platforms.

Some of the retention periods are governed by statute. Others are guidelines, following best practice, employed by schools throughout the United Kingdom. Every effort has been made to ensure that these retention periods are compliant with the requirements of the UK General Data Protection Regulation 2018 (UK GDPR), the Data Protection Act 2018 (DPA), the Human Rights Act 1998, the Freedom of Information Act 2000 (FOI) and the Code of Practice on Records Management (under Section 46 of the FOI).

Managing records series using these retention guidelines will be deemed to be 'normal processing' under the terms of the legislation noted above. If those record series are to be kept for longer or shorter periods than the time scales held in this document, the reasons for any deviation will be recorded.

2. Purpose

This policy, for managing records at Tandridge Learning Trust has been drawn up in conformity with legislation, regulations affecting schools and best practice as promoted by the Information and Records Management Society (IRMS).

As well as containing Record Retention tables, this document sets out more general information and guidelines for recording, managing, storing and the disposal of data, whether they are held on paper or electronically (including online), in order to assist staff, and the Trust, to comply with the General Data Protection Regulation (EU) 2016/679 (GDPR) including as adopted by the United Kingdom as a result of its exit from the European Union ("UK GDPR"), Data Protection Act 2018 and the FOI. It will be read and used in conjunction with all of our related policies.

It is expected that;

- All information held by the Trust needs to be justifiable, by reference, to its purpose.
- The Trust will be transparent and accountable as to what data they hold.
- The Trust will understand and explain the reasons why they hold data.
- The Trust will be able to respond to Subject Access Requests.
- The Trust will be able to amend, delete or transfer data promptly upon any justified request.
- The Trust will be able to audit how personal data was collected and when and why.
- The Trust will hold sensitive data securely, accessed only by those with reason to view it and possess a policy as to why it is needed.
- The Trust will have retention policies that reflect the importance of records relating to child sexual abuse to victims and survivors, and that they may take decades to seek access to such records.

3. Disposal of Data

Article 5 (e) of the UK GDPR states that personal data will be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes… in order to safeguard the rights and freedoms of the data subject ('storage limitation')'.

Not all data needs to be destroyed. The Trust will determine whether records are to be selected for permanent preservation, or for destruction or to be transferred into a different format.

When information is no longer required, it will be destroyed. For confidential, sensitive or personal information, to be considered securely disposed of, it will be in a condition where it cannot either be read or reconstructed.

Skips, 'regular' waste disposal and ribbon shredders are not secure.

Paper records will be cross-shredded, incinerated, or pulped.

CDs/DVDs/discs will be cut into pieces. Hard copy images, AV recordings and hard disks will be dismantled and destroyed. Where third party disposal companies are employed, a certificate of destruction will be obtained. Staff working for external provider will have been trained in the handling and destruction of confidential data.

If the Trust receives a request for records that have not yet been destroyed, even if they should have been destroyed, that record will still be made available to the requestor.

The FOI requires the trust to maintain a list of all records that have been destroyed and who authorised their destruction. This record will be retained for 15 years. The appropriate members of staff (Data Lead) will record:

- File reference and/or unique identifier
- File title or brief description of contents
- Number of files
- Name of the authorising officer

4. Transfer of Records to Archives

a) Storage archives, for Trust business purposes

Little-used records can clutter up the work environment. Some trusts relieve pressure by moving records to a storage space until the retention period runs out. A trust lacking room to keep its records safe from harm (such as fire, flood, unauthorised access) may transfer them to a commercial storage service with credentials such as certification to the ISO 27001 information security standard. The Trust remains legally responsible for the records.

b) Historic archives, for Trust heritage

Usually, disposal means securely destroying the documents after the retention period. But if there is an enduring historical value in the records, disposal need not mean destruction. Instead, the Trust may offer to transfer them to the care of a dedicated archival repository, such as the relevant local authority record office. Establishing a relationship with an archival repository is the standard method for preserving institutional heritage, as it allows the community to view historic information in a comfortable and supervised setting. Archivists are trained not just to care for the physical documents (using acid-free packaging, humidity-controlled storage, etc) but to manage requests for access in accordance with data protection legislation. They may also loan documents back to the Trust for special occasions such as anniversary events.

To identify records of historic value, look out for "offer to local record office" in the guidance below. Other records may have obvious historic interest even if they are not mentioned (e.g. a World War II roll of honour). The trust should approach the record office with a list of files and agree on how and when to transfer them. It may help to set aside items for permanent preservation routinely, such as by filing a single signed copy of the minutes and key agenda papers after each meeting of the governing body, ready to offer to the repository every few years.

Attempting to set up an onsite alternative to a local record office would be a complex undertaking. A trust wishing to do so should consult its Data Protection Officer and approach the record office for advice on management and storage conditions. Remember that archives can include electronic data such as digital photographs, which can only be digitally preserved with the right technical interventions (see the Digital Preservation Handbook).

5. Transfer of Records to other Media

Where lengthy retention periods have been allocated to records, organisations will consider converting paper records to other media (e.g. digital or virtual, 'cloud' based). The lifespan of the media, and the ability to migrate data, will be documented in a Digital Continuity Policy. A scanning risk assessment is recommended to ensure the procedure is adequate. Further information about digital continuity can be found on the National Archives website who also provide guidance on assessing and managing digital continuity risks and a digital continuity checklist. Organisations that believe that they need to retain digital records over a long period on devices, software systems or in formats that may become inaccessible due to developments in technology will seek further advice from the Data Protection Officer and their IT support staff.

Once any paper records have been digitally converted, the paper copies of these records will then be securely and confidentially disposed of (see section 4. Disposal of Data). The Trust will ensure that a record of destruction is held for these paper records (see Appendix A- example of how to create a destruction record). The only records that should always be retained as physical records are any original documents such as birth certificates, passports, marriage certificates etc (it is unlikely that schools will hold these types of documents). Documents of historical significance such as logbooks may also be retained as hard copies.

6. Transfer of Records to other Settings & 'Last Known School'

When a child leaves the Trust, all pupil records, including safeguarding/child protection records will be transferred in a secure manner, to the child's new school. If the records contain sensitive information (e.g. Child Protection records), proof of receipt will be obtained and logged by the Trust's Data Lead. Keeping Children Safe in Education 2024 (KCSiE) states that "where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, and within 5 days for an in-year transfer or within the first 5 days of the start of a new term to allow the new school or college to have support in place for when the child arrives. The designated safeguarding lead should ensure secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file." All copies of data held by the Trust that the child has departed will then be deleted or retained in line with the retention schedule below, including all paper records and data stored electronically. Generally, a record will be kept for tracking and auditing purposes only. Trusts will be aware that where electronic systems are used, sending a pupil file to the next setting does not mean that their own copy of the file is deleted, so action should be taken to delete or archive copies retained where they are no longer required by the school that the pupil has left.

There are four main categories of pupil records that need to be transferred to other settings:

- **Management Information System (MIS) data**

Data held on the MIS is extracted by the Trust using the Common Transfer File mechanism as specified in The Education (Pupil Information) (England) Regulations 2005 and subsequent amendments. The Department for Education specifies what data is to be included in the CTF in technical specification documentation. This will mean that the majority of information held on the MIS is transferred using the CTF method. However, it is important to note that **not all personal data is transferred, only the data sets specified in the CTF schema.** If the MIS has been used to store additional information (documents such as copies of end of year reports or letters) Trusts will take proactive action to ensure these are sent separately and securely. Traditionally, this sort of documentation was held in a pupil 'buff' file, but as organisations have turned to digital ways of working, these are frequently stored by attaching them to the digital MIS record.

- **Safeguarding/Child Protection records**

Trusts frequently use vendor educational technology (edtech) products to hold and transfer these records. Many of these products include the functionality to electronically transfer a copy of (and obtain receipt for) pupil records directly to the next school, where the same product is also used by the receiving school. Where this is not possible, these products should have the functionality to download a pupil record for it to then be transferred electronically or printed out and delivered to the new school. Paper records will be dealt with carefully to ensure that these are safely received by the new school.

Some safeguarding edtech products enable Trusts to use the same system to record behavioural and other information in the same log. Trusts will ensure that safeguarding/child protection records are clearly identified as such so that the receiving school can quickly identify this information. The Trust will consider if information such as behaviour notes needs to be transferred to the next setting, or whether it

will be deleted if no longer required or relevant (e.g. a child's toileting routine may be very relevant when younger, or merits/demerits received but does not need to be part of a permanent safeguarding record).

- **Special Educational Needs records**

It is becoming more common for Trusts to use vendor edtech products to manage these records. Whether stored in such edtech products, on Trust IT systems/cloud storage or on paper, the SEND co-ordinator will ensure that a complete record is compiled and passed securely to the next school.

- **Pupil 'buff' files**

For many trusts, in recent years, the traditional pupil buff files have dwindled in relevance and importance as organisations have increasingly moved to digital storage. Trusts are left with either sending or receiving folders which are very light and seemingly irrelevant. However, there will be documentation, whether on paper or electronic (on the server, in emails, in the MIS) that will be sent to the next setting that the pupil will attend. The Education (Pupil Information) (England) Regulations 2005 state that this "Educational Record" will be transferred to the next setting within 15 school days of confirmation that a pupil is registered at another school. There may be a significant amount of material that is not contained in the CTF, safeguarding or SEND records that will be transferred to the next setting. Trusts may have inadvertently not adapted their records transfer practices as management of these records have moved from a paper 'buff' file to digital format and so this will be noted where relevant on the retention schedule below.

Trusts may wish to retain some minimal 'skeleton' data about pupils' admission, departure and next destination (where known) in order to respond to any requests for information about these pupils and for the historical archive. They may also wish to retain records relating to safeguarding/child protection or SEND records, even though there is no legislative requirement to do so (i.e. to have their own copy of evidence in case of any later legal action). If trusts intend to create and maintain skeleton records or retain copies of records, this will be noted on the retention policy. In some instances, trusts may have a legitimate interest in retaining a copy of more detailed pupil records for a longer time period. If the Trust does retain pupil records, then they will be prepared to justify this retention and will need to consider if a Data Protection Impact Assessment should be completed for any extended retention of records once a pupil has left the trust. See section 17.5 below.

Responsibility for maintaining the pupil record passes to the 'last known school'.

The school is the final or last known school if:

- secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- at any point the pupil left for elective home education, they are missing from education, or have left the UK, or have died.

Tertiary colleges are not included in this definition, therefore the Trust will retain the record. However, the college will receive a copy of the child protection file, as per the requirements of KCSiE above.

The Pupil Record will be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed.

SEN and other support service records can be retained for a longer period of 31 years to enable defence in a "failure to provide a sufficient education" case.

If a trust wishes to retain data for analysis or statistical purposes, it will be done in an anonymised fashion.

8. Management Information System (MIS)

The majority of pupil records and some staff records are held on the Trust MIS. Managing data retention on the MIS can be complex because different data sets held on the MIS have different retention requirements. Trust staff have limited time and resources to manage these differing retention periods and will work with their MIS provider to request support on how to efficiently delete data sets from a record without deleting the entire record (or deleting all data sets except those that are required as part of the 'skeleton' record for long term retention). Where this is not possible, trusts may make a policy decision to retain the entirety of a record for the longest applicable retention period for a data set within the MIS (usually current plus six years). The Trust will set out how records will be retained in the MIS in the relevant section of the Retention Table (Appendix A) in with DfE guidance:

Data protection in schools - Record keeping and management - Guidance - GOV.UK

9. Records relating to Child Sexual Abuse

Records relating to child sexual abuse will be retained for 75 years, in line with the recommendations arising from the outcome of the Independent Inquiry into Child Sexual Abuse (IICSA). The Inquiry stated that these records should be retained for such a long period in recognition of the importance of these records to victims, but that they should be regularly reviewed during that extended retention period. Organisations will particularly need to consider digital continuity where:

- they hold digital records for staff or governors/trustees or
- they are the 'last known school' responsible for this long retention period for any relevant pupil records.

Where there is evidence, or allegations of child sexual abuse, then it will almost certainly be appropriate to retain the entire pupil, staff or other record as a whole, not just the parts of the record that pertain to the abuse. Staff whose duties include reviewing or digitising records will be trained to understand the importance of any evidence or allegations of child sexual abuse that they may happen to uncover, whether that was what they were looking for and the importance of them bringing these to the attention of Trust leadership and/or preserving these records.

The Inquiry report also recommends that the UK government directs the Information Commissioner's Office (ICO) to introduce a Code of Practice on retention of and access to records known to relate to child sexual abuse. This Policy will be updated in line with any Code of Practice from the ICO. The report states that such a 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.

10. Retention of Records relating to Staff

As stated above regarding the long-term retention of minimal pupil records, Trust may wish to retain very basic 'skeleton' records about staff beyond the normal retention of the whole personnel/HR file. This information may include the staff name, role, contract start and end dates. This may be useful for trusts who may need to respond to requests for information from/regarding staff, in the event of it being needed for litigation or other legal purpose and as part of their historical archive.

11. Academisation

When a maintained school becomes an academy, it is legally a new organisation. However, it can still have an operational need for the records of the original school, including files relating to former pupils and employees. The Commercial Transfer Agreement that created the academy may include a section assigning responsibility for these old records, so the rights of the academy and the local authority are formally established. For instance, the agreement might direct the academy to keep the school records on trust until the retention period runs out, and to offer historically valuable documents to the local record office (see 5. Transfer of Records to Archives).

For further information regarding academy record keeping and retention information from the DfE, please see the following link:

Record keeping and retention information for academies - GOV.UK

12. Responsibility and Monitoring

The Headteachers and/or Data Lead, hold primary and day to day responsibility, for implementing this policy. The Data Protection Officer, in conjunction with the Trust, is responsible for monitoring its use and effectiveness and resolving any queries with regards the interpretation of the policy.

All permissions to access data are granted by the Headteacher and recorded in the member of staff's personnel file.

All teaching and office staff are given training and guidance on accessing and managing on Trust records, to ensure compliance with the time scales laid out under the retention schedule. All members of staff, with access to records, are expected to;

- Manage their current record keeping systems using the Retention Policy.
- Only dispose of records in accordance with the requirements outlined in this policy, if authorised to do so.
- Ensure that any proposed divergence from the records retention schedule and disposal policies is authorised and documented by the Head Teacher.

This policy does not form part of any employee's contract of employment and is not intended to have a contractual effect. However, it does reflect the Trusts current practice, the requirements of current legislation and best practice and guidance. It may be amended by the Trust but any changes will be notified to employees within one month of the date on which the change is intended to take effect. The Trust may also vary any parts of the procedure, including time limits, as appropriate.

Appendix A – Retention of Records Schedule

Document Type	Retention Period	Action at end of retention period
Primary school pupil records	Until the pupil leaves	Transfer to secondary school or other primary school when pupil leaves
Secondary school pupil records	Until pupils 25th birthday	Dispose of securely or if pupil joins another school, transfer records to that school
Child Protection files	Until child 25th birthday. If relates to sexual abuse then until child's 75th birthday	Dispose of securely or if child joins another school transfer to that school separately from main file
Allegations of child protection against a member of staff, including unfound allegations	Until staff members normal retirement age, or ten years from the date of allegation, whichever is later	Dispose of securely
Finance contracts	6 years from the last payment on the contract	Dispose of securely
Debtors records	6 years from end of the financial year	Dispose of securely
VAT records	6 years from finance year end	Dispose of securely
Admissions	6 years from the admission date	Dispose of securely
Attendance registers	6 years from date of entry	Dispose of securely
Curricular record	At least 1 year	Dispose of securely
Directors disqualification	15 years from the date of disqualification	Dispose of securely
Records of educational visits	10 years from date of visit. If there was an incident then retain permission slips for all pupils and incident report in the pupil record	Dispose of securely
School vehicles	6 years from the disposal of the vehicle	Dispose of securely
Statutory register of compliance	Memorandums of understanding – life of academy plus 6 years Annual report – 10 years from date of report Board meeting records–10 years after meeting	Dispose of securely

Accessibility plans	Life of plan plus 6 years	Dispose of securely
Accident records	3 years from date of accident	Dispose of securely
Monitoring exposure to substances hazardous to health, including asbestos	5 years	Dispose of securely
Health surveillance records	40 years	Dispose of securely
Other health records of staff	While the worker is employed in your school	Dispose of securely
Fire assessments	Life of the risk assessment plus 6 years	Dispose of securely
Maintenance records	6 years from finance year end	Dispose of securely
Title deeds	12 years from end of deed	Dispose of securely
Copies of DBS certificates	6 months from date of recruitment	Dispose of securely
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends	Dispose of securely
Pay records	3 years from the end of the tax year they relate to	Dispose of securely
Personnel files	6 years from termination of employment	Dispose of securely
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed	Dispose of securely