Data Retention Policy

Version	2.0
Date Policy Reviewed	August 2026
Policy Reviewed by	Head of Compliance
Date of Next Review	August 2027

1. Policy Statement

TP Tutors Ltd has a responsibility to maintain its records and record keeping systems. When doing this, the Company will take account of the most efficient and effective way of storing records and information; the confidential nature of the records and information stored; the security of the record systems used; privacy and disclosure; and accessibility of records and record keeping systems.

2. Status of this Policy

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the Company's current practice, the requirements of current legislation and best practice and guidance. It may be amended from time to time and any changes will be notified to employees. The Company may also vary any parts of this procedure, including any time limits, as appropriate in any case.

3. Data Protection

This policy sets out how long employment-related and student data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR). Data will be stored and processed to allow for the efficient operation of the Company. The Company's Data Protection Policy outlines its duties and obligations under the UK GDPR.

4. Retention Schedule

Information, whether held in hard copy or electronically, will be retained for at least the period specified in the attached retention schedule. When managing records, the Company will adhere to the standard retention times listed within that schedule. The retention schedule applies to all records regardless of the media in or on which they are stored, including paper, electronic, microfilm and photographic records. All

records will be regularly monitored to ensure they are retained, archived or securely destroyed in line with this policy and the retention schedule.

5. Destruction of Records

The schedule is a relatively lengthy document listing the many types of records used by the Company and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements. Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances. All paper records containing personal information or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The Company maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record at least the file reference or other unique identifier; file title or description; number of files; name of the authorising officer; date destroyed or deleted from the system; and the person or persons who undertook destruction.

6. Retention of Safeguarding Records

Any safeguarding records must be retained securely and confidentially, with access restricted to those who require it for safeguarding, legal, regulatory or business purposes. Safeguarding, welfare and child protection records, including records held within MyConcern, MyCommunity or any equivalent safeguarding case management system, must be retained securely and confidentially in line with the retention schedule. These records may include concerns, discussions, decisions, referrals, chronologies, outcomes and any supporting information used to safeguard or promote the welfare of a child or young person.

Where an allegation against an adult working in or on behalf of the Company is found to be malicious, it must not be retained on the individual's personnel file. For all other allegations, including substantiated, unsubstantiated, unfounded or false allegations, the Company must keep a clear summary of the allegation, details of how it was investigated and resolved, the outcome reached, and any action taken. These records must be retained in line with the retention schedule.

Records relating to harm-threshold allegations must be retained separately from low-level concern records, unless a low-level concern becomes part of a formal allegation, disciplinary process, safeguarding investigation or referral. Low-level concern records

should include the concern raised, the action taken, the rationale for decisions made and the outcome.

Risk assessments and medical or allergy-related records that are connected to safeguarding, welfare, lone working, provision planning or learner safety must be retained for the period set out in the retention schedule. Before destruction, these records must be reviewed to confirm whether any safeguarding, complaint, legal, insurance, regulatory or inquiry-related reason requires a longer retention period. Records relevant to statutory inquiries, regulatory investigations, safeguarding reviews, complaints, litigation or potential legal claims must not be destroyed while those matters are ongoing. Where there is uncertainty, the Data Protection Officer or appropriate senior manager should be consulted before any records are destroyed.

Any allegations made of sexual abuse should be preserved by the Company for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. In 2022 the Independent Inquiry into Child Sexual Abuse (IICSA) concluded and published their final report, leaving a recommendation that all records relating to child sexual abuse should be retained for a period of 75 years.

The ICO has not currently produced guidance or frameworks regarding retention as recommended by the inquiry. Until this has been produced, records will still be retained for a prolonged period as recommended initially by IICSA in order to fulfil potential legal duties that a school may have in relation to the inquiry or any further guidance.

7. Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Company. The appropriate staff member, when archiving documents, should record the file reference or other unique identifier; file title or description; number of files; and name of the authorising officer.

8. Transferring Information to Other Media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres, including cloud storage. The lifespan of the media and the ability to migrate data where necessary should always be considered.

9. Responsibility and Monitoring

The Data Protection Officer, in conjunction with the Company, is responsible for monitoring the use and effectiveness of this policy and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records. Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy, and are given adequate and regular training on it.

10. Emails

Email accounts are not case management tools in themselves. Generally, emails may need to fall under different retention periods. For example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a staff record. The retention period will depend on the content of the email and staff must file emails in the relevant areas to avoid data becoming lost.

11. Retention Schedule

File Description	Retention Period
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the Company has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained.
Job applications and interview records of successful candidates	6 years after employment ceases.
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases.
Right to work documentation including identification documents	6 years after employment ceases.
Immigration checks	Kept separately from personnel file and retained for 2 years after employment ceases. **Employer's guide to right to work checks: 21 June 2024**
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded, unless in exceptional circumstances, in which case for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification.

Emergency contact details	Destroyed on termination.
Personnel records	While employment continues and up to ten years after employment ceases.
Annual leave records	Six years after the end of the tax year they relate to, or possibly longer if leave can be carried over from year to year.
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards.
Working Time Regulations: opt-out forms and records of compliance with WTR	Two years from the date on which they were entered into, or two years after the relevant period.
Disciplinary records	6 years after employment ceases.
Training	6 years after employment ceases or for the length of time required by the professional body.
Staff training where it relates to safeguarding or other child-related training	Date of the training plus 40 years.
Safeguarding, Welfare and Learner Safety Records	
Safeguarding concerns, welfare concerns, child protection records, referral records and CPOMS/MyConcern/MyCommunity-style records	Retain until the child or young person reaches age 25, or for 10 years after the case is received or closed, whichever is longer. Review before destruction and retain longer where required due to ongoing safeguarding, complaint, legal, regulatory or inquiry-related reasons.
Low-level concern records relating to adults working in or on behalf of the Company	Retain for the duration of employment or engagement and review on termination. Records should normally be retained until employment or engagement ceases, unless they have become part of a safeguarding allegation, disciplinary matter, referral, repeated pattern of concern or other process requiring longer retention.
Pupil, educational, lone working and medical risk assessments, including records created within the Tuition Management system or any successor system	Retain while the provision is active and for 10 years after the provision ends, or longer where the risk assessment is linked to safeguarding, complaints, incidents, insurance, legal claims or regulatory requirements. Where risk assessment records form part of a safeguarding record, apply the safeguarding retention period.
Medical information provided by parents/carers, allergy management plans, emergency healthcare plans and medical incident records	Retain while the provision is active and for 10 years after the provision ends. Where records relate to a safeguarding concern, serious incident, allergy incident, complaint, insurance matter or legal claim, review before destruction and retain for the longer applicable period.

12. Version Control

Version	Date	Author	Summary of Changes	Approved By	Next Review Date
2.0	August 2026	Head of Compliance	Updated to reflect safeguarding changes, including MyConcern/MyCommunity, and revised safeguarding-related retention periods.	Judicium	August 2027