DATA RETENTION AND DISPOSAL POLICY

Purpose-based retention, review, legal holds and secure deletion

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027 | IMPACT AP

1 | SCOPE AND ACCOUNTABLE LEAD

Manage personal information from creation to secure disposal across paper, email, Airtable, devices and service providers. Kirsty Lampkin coordinates retention with Kate and relevant independent case custodians. Retention must reflect record type, purpose, legal requirements, safeguarding risk and contractual obligations; one blanket period is not appropriate.

2 | CONTROLLED RETENTION SCHEDULE

Maintain a schedule naming each record category, lawful purpose, retention trigger, period or review rule, authority, storage, owner and disposal method. Verify requirements before adopting numeric periods. Record reasons where no fixed period applies. Do not treat these general categories as a completed setting-specific schedule without the supporting legal and contractual checks.

3 | LEARNER AND EDUCATION RECORDS

Set and verify retention for referrals, commissioning, attendance, learning, assessment and EHCP-related delivery records. Consider transfer requirements, complaint or claim periods and commissioner/awarding-body rules. Keep information necessary to evidence provision without retaining every duplicate indefinitely. Record handover, access and any agreed archive arrangements.

4 | SAFEGUARDING AND ALLEGATIONS

Apply specific current safeguarding retention rules and advice, including separate handling of allegations outcomes where relevant. Do not delete safeguarding records merely because a placement or employment ends. An independent lead retains control of cases involving Kate or a conflicted adult. Legal or statutory agency advice takes priority over routine deletion.

5 | HEALTHCARE AND INCIDENT RECORDS

Retain medical consents, administration, healthcare and accident information according to verified legal, safeguarding and insurance requirements. Consider the learner's age and any ongoing investigation or claim. Restrict access and remove unnecessary working copies when the authoritative record is secure. Preserve accurate medication and incident chronologies.

6 | STAFF AND RECRUITMENT RECORDS

Define separate rules for unsuccessful applications, appointment records, checks, payroll and employment matters. Follow DBS handling guidance and avoid unnecessary retention of full certificates. Protect criminal-record and health information with enhanced access controls. Explain relevant periods or decision criteria in staff/applicant privacy information.

DATA RETENTION AND DISPOSAL POLICY

Purpose-based retention, review, legal holds and secure deletion

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027 | IMPACT AP

7 | IMAGES, CCTV AND COMMUNICATIONS

Set purpose-based image and CCTV periods in their respective registers; do not adopt a default simply because a system has capacity. Review permission-based publicity when consent changes. Separate ordinary emails from messages that form part of an official case record. Ensure deletion processes include devices, exports and provider copies where appropriate.

8 | LEGAL HOLDS AND REQUESTS

Suspend routine deletion of relevant information when a complaint, subject-access request, litigation, safeguarding enquiry or other lawful hold requires preservation. Record the scope, reason, responsible person and review date. Preserve only what is relevant and release the hold through an authorised decision when the reason ends.

9 | SECURE DISPOSAL

Authorise disposal under the schedule and keep a proportionate destruction log. Shred or securely destroy confidential paper; use verified secure deletion or disposal for devices and electronic media. Check processors' deletion arrangements and backup cycles. Do not place readable records in ordinary waste or assume moving a file to a recycle bin completes secure deletion.

10 | AUDIT AND ACCOUNTABILITY

Review categories and overdue actions at least annually, with more frequent operational checks where needed. Sample access, exports, archived data and deletion evidence. Report loss or accidental deletion through the data-breach procedure. Record decisions and reasons so retention can be explained to families, staff, commissioners and regulators.

11 | POLICY CONTROL AND REVIEW

Policy owner: Kate Willis, Principal and Proprietor. Effective date: September 2026. Scheduled review: September 2027, or sooner after relevant changes, incidents or feedback. Record actual governance approval and implementation decisions and brief staff on their duties. These policy dates do not assert that approval, staff training or operational checks have already occurred. Use the Complaints or independent reporting route for concerns about implementation.

12 | SOURCES AND RELATED DOCUMENTS

UK GDPR storage-limitation principle; Data Protection Act 2018 as amended; ICO retention guidance and applicable safeguarding/contract requirements.

ico.org.uk; Impact Data Protection and CCTV policies.

Check current versions and apply according to Impact's legal and commissioning status.