THE HAVEN

Operated by the Autistic Girls Network charity — 1196655 (England and Wales), SC054837 (Scotland)

Data Retention Policy and Data Breach Procedure

The Haven — The Haven

Document	Data Retention Policy and Data Breach Procedure
Version	05.26
Status	live
Last reviewed	21 May 2026
Next review	21 May 2027
Owner	Data Protection Officer
Approved by	Proprietor + Governing Body

Part A: Data Retention Policy

1. Purpose

This policy sets out how long The Haven retain personal data, and the principles by which retention periods are decided. It supports compliance with the UK GDPR principle of storage limitation, the Data Protection Act 2018, and statutory record-keeping obligations relevant to education, safeguarding, and charity governance.

2. Scope

This policy applies to all personal data held by The Haven, in any format, including electronic and paper records. It applies to all staff, volunteers, governors and contractors. It is read alongside our Data Protection Policy and the four Privacy Notices.

3. Principles

- Personal data is kept no longer than necessary for the purpose for which it was collected.
- Retention periods are documented, reviewed annually, and justified.
- Safeguarding records are retained in line with statutory expectations, which generally exceed the period for ordinary education records.
- Where statutory minimum periods apply, those override this policy's defaults.
- At end of retention, data is securely deleted, or anonymised where there is a legitimate ongoing purpose for which identification is no longer required.

4. Retention schedule

The following retention periods apply. Where statutory guidance changes, the schedule is updated.

5. Method of deletion

At end of retention, records are securely deleted using methods proportionate to the sensitivity of the data. Electronic records are deleted from primary systems and from backups in line with our backup cycle. Paper records, where any exist, are shredded. Records of deletion are maintained where deletion concerns safeguarding-relevant data.

6. Roles and responsibilities

- Data Protection Lead: Maintains this schedule and oversees its application.
- Head / DSL: Oversees safeguarding-record retention specifically.
- System owners: Apply retention rules to the systems they manage.
- All staff: Follow retention rules in day-to-day work.

Part B: Data Breach Procedure

7. Purpose

This procedure sets out how The Haven respond to a personal data breach, in line with Articles 33 and 34 of the UK GDPR. The aim is to detect, contain, assess, report and learn from breaches in a timely and proportionate way.

8. Definition

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- An email containing personal data sent to the wrong recipient.
- Loss or theft of a device containing personal data.
- Unauthorised access to a learner record.
- Ransomware or other cyber incident affecting personal data.
- Disclosure of personal data without lawful basis.

9. Reporting a suspected breach

Any member of staff, volunteer, governor or contractor who becomes aware of a suspected or actual data breach must report it immediately to the Data Protection Lead, regardless of how minor it appears. Reporting routes:

- Email the Data Protection Lead directly.
- In urgent or out-of-hours cases, contact the Head.
- Where the breach involves safeguarding data, also notify the DSL immediately. Delay in reporting is itself a serious concern.

10. Containment and immediate response

On receipt of a report, the Data Protection Lead takes immediate steps to contain the breach. These may include:

- Recalling or deleting a misdirected email.

- Suspending compromised accounts or access.
- Isolating affected systems.
- Securing or wiping a lost device remotely.
- Identifying which data subjects are affected.

11. Assessment

Within 24 hours, the Data Protection Lead assesses:

- The nature, scope and categories of personal data affected.
- The number of data subjects affected.
- The likely consequences for those data subjects.
- The risk to rights and freedoms of those data subjects.

12. Notification to the Information Commissioner's Office (ICO)

Where the breach is likely to result in a risk to the rights and freedoms of data subjects, the ICO is notified within 72 hours of awareness. The Data Protection Lead makes this notification, in line with ICO guidance. Notification covers the nature of the breach, the categories and approximate number of subjects, the likely consequences, and the measures taken or proposed.

If a notification is not made within 72 hours, the reason for delay is documented.

13. Notification to data subjects

Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, those subjects are informed without undue delay. Notification is clear, plain-English, and includes:

- A description of the nature of the breach.
- The likely consequences.
- Measures taken or proposed by The Haven.
- Contact details for further information.
- Action recommended for the data subject, where relevant.

14. Record-keeping

All breaches — including those that do not require notification — are logged in the Data Breach Register. The register records the facts, effects and remedial action. The register is reviewed annually by the Data Protection Lead and presented to governors as part of the annual data protection review.

15. Lessons learned

After every notifiable breach, and at least annually for the breach register as a whole, the Data Protection Lead conducts a lessons-learned review. Outcomes feed into policy review, staff training, and changes to systems or processes.

16. Roles and responsibilities

- Data Protection Lead: Owns this procedure; first point of contact for reports; makes ICO and data subject notifications.

- Head: Oversees response; supports decision-making in serious cases.
- DSL: Engaged where breach involves safeguarding records.
- Governors: Receive an annual review of breaches and the breach register.
- All staff: Report immediately; cooperate with response.

17. Related documents

- Data Protection Policy
- Privacy Notices (Staff / Visitors / Students and Parents / CLA)
- Cyber Security Policy
- BYOD Policy
- Online Safety Policy
- Safeguarding and Child Protection Policy

18. Review

This policy is reviewed annually by the Data Protection Lead and approved by the Board of Governors.

Document version	1.0
Date issued	May 2026
Next review	May 2027
Document owner	Data Protection Lead
Approved by	Board of Governors

Category	Examples	Retention period
Learner education records	Reports, assessment data, mentor notes, attendance records	Current age + 25 years (or until age 25), in line with DfE / Ofsted guidance
Safeguarding records	Child protection files, chronologies, DSL records	Held in line with Keeping Children Safe in Education and IICSA guidance — until age 25 minimum; longer where indicated by ongoing concern or LADO involvement
Admissions records (unsuccessful)	Referrals not progressed to placement	12 months
Family communication records	Emails, meeting notes	Duration of placement + 6 years
Lesson recordings	Live session recordings	Reviewed against need; default deletion at end of academic year unless safeguarding/QA review requires longer retention

Category	Examples	Retention period
Examination records	Coursework, candidate records, results	In line with awarding body requirements (typically 6 years)
Staff records	Recruitment, contracts, supervision, training	Duration of employment + 6 years
DBS check records	Date of check and certificate number only	Duration of employment; certificate not retained
Safer recruitment records	Application forms, interview notes, references	6 months for unsuccessful candidates; duration of employment + 6 years for successful candidates
Financial records	Invoices, payments, payroll	7 years (HMRC requirement)
Governor records	Minutes, decisions, registers	Permanently (charity governance)
Complaints records	Complaint correspondence and outcomes	6 years from resolution
IT system logs	Platform activity logs, audit logs	12 months default; longer where required for safeguarding or security investigation
Marketing consents	Newsletter opt-in records	Until withdrawal of consent + 2 years for evidence

---