

THE HAVEN

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

The Haven Data Protection, Confidentiality & Privacy Policy (v3.1)

Document	The Haven Data Protection, Confidentiality & Privacy Policy (v3.1)
Version	10.25
Status	live
Last reviewed	01 October 2025
Next review	01 October 2026
Owner	Data Protection Officer
Approved by	Proprietor

Date: October 2025

Review Date: October 2026

Coordinator: Data Protection Officer (DPO)

Nominated Governor: the Co-Chair of Governors

Version:10.25

1. Statement of Intent

The Haven is committed to respecting the privacy, dignity, and safety of all learners, staff, and families. We recognise our duty to handle information responsibly, transparently, and in accordance with UK data protection legislation and safeguarding law.

We aim to:

- Protect the rights of individuals under the UK GDPR and Data Protection Act 2018.
- Embed privacy, confidentiality, and security as standard practice.
- Share information appropriately to uphold safeguarding, wellbeing, and legal compliance.
- Maintain robust systems for responding to incidents and ensuring continuity across digital platforms.

2. Legal Framework

This policy aligns with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012

- The Education (Pupil Information) (England) Regulations 2005 (amended 2018)
- The Privacy and Electronic Communications Regulations 2003
- DfE Guidance: *Keeping Children Safe in Education (2026)
> *
- ICO Guidance: *Guide to the UK GDPR (2022)
> *

It operates in conjunction with The Haven's:

- Cyber Security Policy v01.26 (2025)
- Incident Response Plan (2025)
- Child Protection and Safeguarding Policy v01.26
- Staff Conduct Policy v10.25
- Records Management Policy
- Navigating the Digital Age of Consent_ A Guide for Parents at The Haven v10.25 Guide

3. Scope and Principles

The Haven processes personal data to support learning, meet statutory duties, manage operations, and maintain safeguarding. We adhere to the six principles of data protection:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

4. Confidentiality and Privacy

- Confidentiality is never absolute where safeguarding concerns exist.
- Information is shared on a *need-to-know basis* and in line with statutory guidance (*Information Sharing: Advice for Practitioners*, DfE 2018).
- Learners are informed, in age-appropriate ways, that safeguarding overrides confidentiality.
- Personal images, video, or voice recordings are never shared publicly without explicit parental consent. Lesson recordings are only available to class members. If recordings need to be shared for safeguarding reasons, the identity of learners not related to the incident will be obscured.
- Only secure platforms are used (TutorCruncher, Google Meet, Google Classroom, Google Workspace).

Termly joint DSL/DPO reviews monitor confidentiality breaches.

5. Roles and Responsibilities

- All staff must:
 - Use strong passwords, MFA, and secure storage.
 - Report data incidents immediately to the DPO/DSL.
 - Follow guidance on sharing and recording information securely.
- *The DPO leads on GDPR compliance and ICO liaison; the DSL ensures safeguarding practice aligns with data-protection principles.
> *
- Governors oversee compliance and ensure adequate resourcing.

6. Lawful Processing and Consent

Processing occurs under lawful bases such as consent, legal obligation, public task, or legitimate interest.

Sensitive data is handled only under explicit consent or legal authority.

Consent must be freely given, specific, informed, and unambiguous — and can be withdrawn at any time.

Where safeguarding applies, consent may be overridden to prevent harm.

7. Digital Platforms: Risk & Continuity

Core systems:

- TutorCruncher – administration, billing, communications
- Google Meet – live teaching and interaction
- Google Classroom – learning platform, resources and assignments
- Google Workspace – secure storage and safeguarding records
- Google Classroom – courses, discussions, assignments

Backup Plan

- TC outage → Google Sheets + Gmail manual processes
- PS outage → Google Meet + asynchronous packs
- GWS outage → Encrypted offline backups + SLT secure channel
- Annual “Plan B” continuity drill led by DSL/SLT.

8. Data Protection in Partnership with Local Authorities

Where Local Authorities (LAs) commission provision, The Haven will:

1. Data Sharing

- Share attendance, safeguarding, and progress data securely via agreed channels.
- Ensure data is minimised, relevant, and transferred using encrypted systems.

2. Privacy Notices

- Provide learners, families, and commissioning authorities with a clear privacy notice outlining what data is collected, why, and how long it is kept.

3. Joint Responsibility

- Recognise that LAs may act as data controller in some contexts, with The Haven as processor, or both as joint controllers.
- Ensure data processing agreements are in place where required.

4. Monitoring and Review

- The DPO will review data sharing with LAs annually.
- Any updates to UK GDPR, ICO guidance, or LA protocols will trigger an immediate review.

9. Data Security and Breaches

- Confidential records are stored securely — paper files locked; digital data encrypted and backed up off-site.
- Breaches are logged in the Cyber Incident Register.
- The DPO notifies the ICO within 72 hours where required and coordinates safeguarding assessment with the DSL.
- Individuals affected are informed where risk of harm exists.
- Root causes are analysed, and training provided to prevent recurrence.

10. Safeguarding Integration

Data protection supports safeguarding, not limits it.

- Staff may share information without consent if necessary to protect a child.
- All data-sharing decisions are recorded, with rationale and legal basis.
- Learner autonomy and trauma-informed principles guide all communications.

11. Retention, Publication & Images

- Data is retained only as long as necessary.
- Lesson video/audio recordings are limited to educator feeds for training and quality assurance.
- Student voices may be captured but not identified.
- Parental consent is obtained for any publication of images or recordings.

12. Monitoring and Review

- *Joint DSL/DPO reviews of incidents, breaches, and privacy compliance are recorded for governance assurance.*
- Annually: Cross-check with Cyber Security Policy v01.26, Incident Response Plan, and KCSIE.
- Immediately: Interim review following Ofsted, NCSC, ICO, or DfE updates.

This PDF was generated from the published policy at policies.thehavenonline.school on 26 August 2026. The website is the authoritative, most current version of this policy.