THE HAVEN

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

Online Safety Policy and Acceptable Use

Document	Online Safety Policy and Acceptable Use
Version	10.26
Status	live
Last reviewed	27 October 2026
Next review	29 April 2027
Owner	Designated Safeguarding Lead
Approved by	Proprietor

Date: October 2026
Review Date: April 2027 (or sooner if statutory guidance changes)
Policy Owner: Designated Safeguarding Lead (DSL)
Nominated Governor: Safeguarding Governor
Version: 10.26

1. Policy Statement and Purpose

The Haven is committed to ensuring that children and young people are kept safe when accessing education online. As a primarily online and hybrid provision, digital safety is integral to our safeguarding culture and practice.

This policy sets out how The Haven:

- safeguards learners in online environments;
- ensures platforms are used safely, responsibly, and securely;
- trains staff to manage online risk effectively;
- responds to online safety concerns, cyber incidents, or misuse.

This policy should be read alongside the **Child Protection and Safeguarding Policy v10.26**, **Behaviour and Regulation Policy v10.26**, **Data Protection (UK GDPR), Confidentiality & Privacy Policy v10.26**, and **Managing Allegations Against Staff Policy v10.26**.

2. Scope

This policy applies to:

- all learners, staff, contractors, and volunteers;
- all online, hybrid, and digital learning activity;

- all platforms and tools used for teaching, communication, safeguarding, administration, and assessment.

3. Platforms Used by The Haven

The Haven uses a restricted, approved set of platforms. Use of unapproved platforms for learner contact is not permitted.

3.1 Core Teaching and Communication Platforms

Platform	Purpose	Safeguarding / Safety Controls
Google Workspace for Education (Gmail, Drive, Docs, Sheets, Forms)	Official email, document sharing, safeguarding records, registers	Encrypted at rest and in transit; managed accounts; access controls; audit logs
Google Meet	Live online teaching, meetings	Waiting rooms, host controls, chat moderation, recording controls
Google Classroom (VLE/ LMS)	Curriculum delivery, assignments, feedback	Role-based access; secure log-in; moderated discussion spaces
Google Slides and in-session annotation	Collaborative whiteboarding and live annotation during sessions	Held within the Haven Workspace tenant; access controlled by Haven account; no private messaging
Zoom / Microsoft Teams *(where required)*	External meetings or assessments	Waiting rooms, passwords, restricted chat

3.2 Communication and Engagement Platforms

Platform	Purpose	Controls
School-managed email accounts	Learner–staff communication	Managed accounts; provider-level spam and malware filtering; administrative audit logs

Platform	Purpose	Controls
Telephone / SMS (staff only)	Safeguarding or welfare contact	Logged; no personal numbers used

3.3 Assessment, Administration and Payment Systems

Platform	Purpose
Secure cloud storage	Safeguarding records, EHCP evidence
Online exam platforms	Assessments (where applicable)
Payment / commissioning systems	Invoicing and reporting

This policy applies to all use of the above platforms, whether during teaching, preparation, recording, or communication.

4. Roles and Responsibilities

4.1 Governing Body / Proprietor

- Ensures appropriate policies, oversight, and resourcing for online safety.
- Receives anonymised reports of incidents and audits.

4.2 Designated Safeguarding Lead (DSL)

The DSL:

- holds overall responsibility for online safety and safeguarding;
- responds to online safety concerns involving learners;
- liaises with Local Authorities, commissioners, and external agencies;
- oversees staff training and induction relating to online safety;
- coordinates communication in serious incidents.

4.3 Cyber Security and Platform Incidents

- Operational responsibility for responding to cyber-attacks, data breaches, or platform failures sits with senior leadership, in consultation with:
    - the **DSL** (where safeguarding risk exists),
    - the **Data Protection Officer (DPO)** (for data breaches),
    - platform providers where required.
- Incidents are logged, risk assessed, and escalated appropriately.

4.4 Staff and Tutors

Staff:

- follow the Acceptable Use Agreement (Appendix A);
- use only approved platforms;
- report online safety concerns immediately to the DSL;
- do not engage in private, unsupervised digital contact with learners.

4.5 Learners and Parent Carers

- Learners are supported to use platforms safely and appropriately.
- Parent carers are informed of expectations and responsibilities at induction.

5. Platform Safety, Security and Quality Assurance

The Haven undertakes proportionate due diligence to ensure platforms are safe and appropriate, including:

- use of reputable, education-grade platforms;
- confirmation of data encryption in transit and at rest;
- review of privacy notices and security documentation;
- role-based access and permission settings;
- regular review of safeguarding features and updates.

Access and Accounts

- Learners are issued with school-managed log-ins where appropriate.
- Platforms are accessed via secure log-in credentials.
- Personal accounts are not used for teaching or safeguarding communication.

6. Monitoring and Oversight

- Live sessions are supervised and moderated by staff.
- Platform features (chat, breakout rooms, permissions) are used proportionately.
- Concerns arising from platform use are recorded and reviewed.
- Patterns of concern inform training, platform settings, or policy review.

- “Monitoring” in this policy means human supervision of Haven sessions and review of activity within Haven platforms. It does not mean technical monitoring of learner devices, which The Haven does not carry out. See 9.3.

7. Training and Awareness

7.1 DSL Training Responsibilities

The DSL is responsible for ensuring that:

- staff receive annual safeguarding and online safety training;
- updates are provided in response to emerging risks or incidents;
- induction training includes platform-specific safeguarding guidance.

7.2 Staff Training

All staff receive:

- online safety training at induction;
- annual refresher training covering:
    - safeguarding in online environments,
    - professional boundaries and digital conduct,
    - platform-specific features and risks,
    - responding to online disclosures or incidents;
- additional training when new platforms are introduced.

8. Responding to Online Safety Concerns

Concerns may include:

- inappropriate online behaviour;
- exposure to harmful content;
- cyberbullying or peer-on-peer abuse;
- misuse of platforms;
- data security concerns.

All concerns are:

- reported immediately to the DSL;
- recorded factually;
- escalated according to safeguarding thresholds;
- shared with commissioning schools or LAs where required.

9. Online Safety Act 2023 — duties and alignment

The Online Safety Act 2023 places duties on regulated user-to-user and search services to protect children from illegal content and content harmful to children. While The Haven is itself an education provider rather than a regulated service, our duty of care to learners requires that we operate consistently with the Act and respond proportionately when learners encounter or are affected by content that the Act addresses.

9.1 Categories of harm we recognise

- **Illegal content** — including child sexual abuse material (CSAM, including AI-generated and digitally manipulated imagery), terrorism content, threats to kill, controlling or coercive behaviour, intimate image abuse, and content encouraging self-harm or suicide.
- **Primary priority content harmful to children** — pornography; content that encourages, promotes or instructs self-harm; suicide content; content that encourages eating disorders.
- **Priority content harmful to children** — abusive or hateful content (including based on protected characteristics); bullying content; serious violence; harmful substances content; dangerous stunts and challenges.
- **AI-generated harm** — the Online Safety Act applies equally to AI-generated content. Deepfakes, AI-generated CSAM, AI-generated grooming content, and synthetic intimate imagery are treated identically to non-AI counterparts.

9.2 Our operational response

When a learner discloses, encounters, or appears to have encountered content in any of these categories — on a Haven platform, on an external service, or in their broader online life — staff will:

- Treat the disclosure as a safeguarding concern under the Child Protection and Safeguarding Policy v10.26.
- Escalate to the DSL without delay.
- Where illegal content is involved, follow the escalation route to police or the Internet Watch Foundation as appropriate, and never attempt to view, download, or store the content for evidential purposes — this is a criminal offence and the responsibility of trained law enforcement.
- Support the learner therapeutically and report to commissioning schools / LAs in line with safeguarding agreements.

9.3 Filtering and monitoring

The DfE *Filtering and Monitoring Standards* (2024) apply to devices and networks that a setting owns or manages, including managed devices taken off site. The Haven has no premises, no managed network and does not issue or manage devices: learners take part from devices they or their families own, on home internet connections The Haven does not administer.

The Haven therefore does not filter or monitor learner devices, browsers, home networks, personal accounts or phones, and receives no keystroke, search-term or content alerts. There is no automated safeguarding alerting. What The Haven does control is the Haven-managed account and the Haven-managed platforms: administrative settings on accounts, restrictions on external contact and third-party application access, platform configuration, persistent session chat, and the checking of every link, video and resource before it is shared. The full analysis, including residual risk, is held in the *Risk Assessment — Learner Access from Personally-Owned Devices*.

Responsibility for filtering and monitoring is held by the **Designated Safeguarding Lead**, who is a member of the senior leadership team, supported by the Systems Architect on technical matters. Keeping Children Safe in Education 2026 asks that the annual review be led by the senior leader responsible for filtering and monitoring with the support of the DSL and IT support; at The Haven the DSL and that senior leader are the same person, and the separation of view that the guidance intends is provided by the Systems Architect and by the Safeguarding Governor, who receives the review. In line with Keeping Children Safe in Education 2026, the arrangements that do exist are reviewed at least once every academic year and the review is recorded — when the checks took place, which accounts, platforms and environments were tested, what was identified, and what was done about it — alongside the existing termly proportionality review.

Where The Haven provides or manages devices in future, the DfE standards will apply in full and a filtering and monitoring product will be required before those devices are issued. Any monitoring introduced will be overt: declared to learners and families before it begins, limited to what is necessary, explained in terms the learner can understand, and recorded in the DPIA. The Haven does not deploy covert monitoring.

9.4 Generative AI, and nudes and semi-nudes

Keeping Children Safe in Education 2026 treats generative AI as a risk factor within the contact and conduct categories of the four areas of online risk. The Haven recognises accordingly:

- **Contact** — harmful interactions with AI chatbots and companion-style systems, including systems that simulate intimacy, dependency or friendship.
- **Conduct** — the creation, possession or sharing of nudes and semi-nudes, including images that have been digitally altered or wholly generated using AI.

The Haven uses the term *nudes and semi-nudes* throughout, covering self-generated, AI-generated and altered imagery alike. Incidents are handled under the Child Protection and Safeguarding Policy v10.26 and the DfE guidance *Sharing nudes and semi-nudes: advice for education settings working with children and young people*. Staff do not view, copy, download or store such imagery; the Designated Safeguarding Lead leads the response and escalates to the police or the Internet Watch Foundation where appropriate. A learner who reports an image is supported, not sanctioned.

In-meeting AI assistants and automatic AI note-takers are disabled on Haven platforms. Use of AI by staff and learners is governed by the Responsible Use of AI Policy v10.26.

10. Cyber-Incidents and Data Breaches

In the event of a cyber-attack or data breach:

- immediate steps are taken to secure systems;
- the DSL and DPO are informed;
- risks to learners are assessed;
- notifications are made in line with data protection law;
- lessons learned inform system improvements.

11. Review and Monitoring

- This policy is reviewed annually.
- Termly audits consider incidents, platform use, and training impact.

- Updates reflect statutory guidance and technological change.

Appendix A – Acceptable Use Agreement (Summary)

All staff and learners agree to:

- use only approved platforms;
- communicate respectfully and professionally;
- not share personal contact details;
- not record or distribute content without permission;
- report concerns immediately;
- comply with safeguarding and behaviour expectations.

A full Acceptable Use Agreement is issued and signed at induction.

Appendix B – Responsible Use of AI Policy v10.26 (Summary)

The Haven permits limited, ethical use of AI tools where they:

- support accessibility or workload reduction;
- do not replace professional judgement;
- do not process personal data without approval;
- are transparent and explainable.

AI must **not** be used to:

- generate safeguarding decisions;
- analyse learner behaviour without consent;
- replace relational judgement.

All AI use is overseen by senior leadership and aligned with data protection and safeguarding principles.

12. Related Policies and Guidance

- Child Protection and Safeguarding Policy v10.26
- Online Behaviour and Regulation Policy v10.26
- Data Protection (UK GDPR), Confidentiality & Privacy Policy v10.26
- *Online Safety & Acceptable Use*
- Managing Allegations Against Staff Policy v10.26
- KCSIE 2026
- UK GDPR / Data Protection Act

This PDF was generated from the published policy at policies.thehavenonline.school on 20 November 2026. The website is the authoritative, most current version of this policy.