THE HAVEN

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

Cyber Security Policy

Document	Cyber Security Policy
Version	04.26
Status	live
Last reviewed	29 April 2026
Next review	29 April 2027
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: v01.26

1. Policy Statement and Purpose

The Haven is committed to safeguarding learners, families, and staff in all digital environments. As a hybrid-flexible provider, our reliance on technology for learning, communication, and administration requires strong cyber security practices.

This policy sets out The Haven's approach to **preventing, detecting, and responding to cyber risks** including unauthorised access, data breaches, malware, phishing, and misuse of systems.

It complements and should be read alongside:

- **Data Protection, Confidentiality & Privacy Policy v10.25
  > **
- **Staff Conduct Policy v10.25**
- **Child Protection and Safeguarding Policies
  > **
- **Prevent Duty Policy v01.26_
  > **
- **Navigating the Digital Age of Consent_ A Guide for Parents at The Haven v10.25
  > **

2. Statutory Guidance

This policy is aligned with:

- UK GDPR and Data Protection Act 2018
- Children's Code (Age Appropriate Design Code)
- Online Safety Act 2023
- Keeping Children Safe in Education 2026 (KCSIE)
- National Cyber Security Centre (NCSC) guidance for schools
- Independent School Standards (Part 3: Welfare, Health and Safety of Pupils) — adopted as a voluntary benchmark; The Haven is not a DfE-registered independent school and these Standards do not apply to it as a matter of law

3. Scope

This policy applies to:

- All The Haven staff, contractors, volunteers, and governors
- All learners and parents/carers engaging in remote or in-person learning
- All devices, systems, platforms, and accounts used for The Haven's educational provision

4. Roles and Responsibilities

- **Governing Board**: Provides oversight, ensuring cyber security is resourced and reviewed.
- **Principal & DSL**: Accountable for safeguarding implications of cyber risks. *Monitor safeguarding implications of cyber risks. The DPO retains overall accountability for technical and legal compliance. Termly joint DSL/DPO checks review incident logs and control effectiveness.*
- **Data Protection Officer (DPO)**: Leads on compliance with UK GDPR and cyber incident reporting.
- **IT/Systems Lead**: Manages technical controls (firewalls, encryption, backups, MFA).
- **All Staff**: Follow safe digital practices, report concerns promptly.
- **Learners & Parents/Carers**: Adhere to Remote Learning & Online Safety & Acceptable Use v01.26 (linked).

5. Implementation

5.1 Preventive Measures

- Use of multi-factor authentication (MFA) for staff accounts
- Encryption of devices and data in transit
- Approved platforms only (Google Meet, Google Classroom, Google Workspace for Education, TutorCruncher)
- Strong password policy: minimum 8 characters, rotated annually
- Regular software updates and security patching
- Secure disposal of IT assets (in line with ICO guidance)

5.2 Monitoring and Detection

- Logging and monitoring of system access
- Alerts for unusual login behaviour or attempted breaches
- Regular vulnerability scans and penetration testing (annual minimum)

5.3 Training and Awareness

- Annual staff cyber security training (with safeguarding emphasis)
- Learner education on phishing, scams, and safe digital conduct (age-appropriate)
- Parent workshops/webinars linked to Navigating the Digital Age of Consent_ A Guide for Parents at The Haven v10.25 guidance

6. AI tools and the Diamond AI Posture

Cyber security and AI risk are increasingly entangled. The Haven follows a **Diamond AI posture** — *work with AI; do not offload decisions to AI; do not defer entirely from AI* — and applies it to cyber security in the following ways:

- **Approved AI tooling only.** AI tools used in Haven systems (assistive AI in Google Workspace, education-grade AI tutoring tools where adopted, AI features in Google Classroom or Google Meet) must be reviewed and approved under the Responsible Use of AI Policy v10.26 and a DPIA Digital Platforms entry maintained.
- **No offloaded security decisions.** AI may assist with anomaly detection, log triage, or phishing classification. Decisions to suspend an account, isolate a device, or notify the ICO remain with the Data Protection Officer and the Head.
- **Identifiable data never enters public AI.** Staff must not paste learner-identifiable, safeguarding-sensitive, or commercially confidential data into public AI tools (e.g. consumer ChatGPT, Claude.ai, Gemini consumer tier). Education-tier tools with appropriate data-processing agreements may be used per the AI policy.
- **AI-generated threats.** Staff are trained to recognise AI-generated phishing, deepfake video calls (especially in safeguarding contexts), and AI-generated impersonation of senior leaders. Verification protocols apply when authorising sensitive actions on the basis of any digital communication.

7. Incident Response

Any suspected cyber incident (phishing, breach, unauthorised access, malware) must be:

- Reported immediately to the DPO and DSL
- Logged in the Cyber Incident Register
- Investigated within 24 hours
- Reported to ICO within 72 hours if a personal data breach has occurred (per UK GDPR)
- Communicated to affected families if there is a high risk to rights and freedoms

(Full procedures are set out in The Haven's Incident Response Plan – to be published alongside this policy.)

8. Safeguarding Links

Cyber risks are safeguarding risks. A breach may expose learner data, create opportunities for grooming, or enable identity theft. All incidents will be assessed for safeguarding implications and, where necessary, escalated in line with The Haven **Child Protection and Safeguarding Policy v01.26**.

9. Monitoring and Review

- **Termly** DSL/DPO checks on incident log and control effectiveness
- **Annual** full review by DSL, DPO, and Governing Board to remain compliant with statutory guidance
- **Immediate interim review** following significant incident, NCSC alert, or government update

---