

THE HAVEN

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

Information and Cyber Security Policy

Document	Information and Cyber Security Policy
Version	10.26
Status	live
Last reviewed	21 October 2026
Next review	29 April 2027
Owner	Data Protection Officer
Approved by	Proprietor

Date: October 2026 **Review Date:** April 2027 **Coordinator:** the Data Protection Officer **Nominated Governor:** the Co-Chair of Governors **Version:** 10.26

1. Policy statement and purpose

The Haven exists online. Every lesson, record, conversation and file depends on information systems, so information security is a safeguarding matter and a condition of the provision operating at all.

This policy sets out how The Haven protects the confidentiality, integrity and availability of the information it holds, and how it prevents, detects and responds to cyber risk: unauthorised access, data breaches, malware, phishing, impersonation and misuse of systems. It is the umbrella policy for information security. The detailed rules for particular areas sit in the policies listed in section 16, and where this policy and a more specific policy differ, the more specific policy applies.

It replaces the Cyber Security Policy (v04.26).

2. Statutory and guidance framework

This policy is written to:

- the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025;
- *Keeping Children Safe in Education 2026* (KCSIE), including its expectations on online safety and on filtering and monitoring;
- the Online Safety Act 2023 and the ICO's Age Appropriate Design Code (Children's Code);
- National Cyber Security Centre (NCSC) guidance for schools and small organisations;
- the Department for Education's cyber security standards for schools and colleges, and the Independent School Standards (Part 3), both adopted as voluntary benchmarks. The Haven is not a DfE-registered independent school and neither applies to it as a matter of law; where this policy meets them, it does so deliberately.

3. Scope

This policy applies to:

- all staff, contractors, volunteers, governors and trustees who use The Haven's systems or handle its information;
- learners and parents/carers, in respect of the accounts and platforms The Haven provides to them;
- all information The Haven holds, in any format, and all accounts, platforms, services and devices used to access it.

The Haven has no premises and no network of its own. Its information lives in a small number of cloud services (section 8), is accessed from devices The Haven does not own (section 9), and is handled by a small team. The controls in this policy are designed for that reality: they work at the level of accounts, platform configuration and people, not buildings and network hardware.

4. Roles and responsibilities

Role	Responsibility
Proprietor (the board of trustees of the Autistic Girls Network) and the governing body	Oversight; ensures information security is resourced, reviewed annually and reported on. The nominated governor is the Co-Chair of Governors.
Data Protection Officer	Owns this policy. Accountable for compliance with data protection law, the processor register, data protection impact assessments and breach reporting to the ICO.
Systems Architect	Designs and maintains the technical configuration: tenant settings, access control, device checks, logging and the audit and change records. Provides technical separation from the safeguarding and data-protection roles.
Head / Designated Safeguarding Lead	Accountable for the safeguarding implications of information and cyber risk, including online safety and the senior responsibility for filtering and monitoring under KCSIE 2026. Approves staff access to learner information.
All staff, contractors, volunteers and governors	Follow this policy and the Staff Safer Internet Agreement; keep accounts and devices secure; report concerns and incidents at once.
Learners and parents/carers	Follow the Online Safety & Acceptable Use Policy and the digital agreement.

Where one person holds more than one of these roles, the separation the guidance expects is provided as follows: the Systems Architect holds the technical configuration, the DSL holds the safeguarding judgement, and the Proprietor receives the annual review. Decisions to suspend an account, remove a device, notify the ICO or inform families are taken by the DPO with the Head, never by one person acting alone except in an emergency, and are recorded.

5. Information classification

Information is handled according to its classification. Where in doubt, treat it as confidential.

Class	Examples	Handling
Public	Published policies, the website, the course library homepage, marketing materials	May be shared freely. Still subject to accuracy and brand standards.
Internal	Timetables, lesson resources, staff rotas, meeting notes, internal procedures	Held in Haven accounts and shared drives. Not shared outside The Haven without a reason and a decision by the Head or Systems Architect.
Confidential	Learner and family personal data; attendance and engagement records; EHCP, SEND and medical information; safeguarding records; staff personal and HR data; the Single Central Record; commissioner contracts and finance; credentials and backup codes	Access on a need-to-know basis only. Held in the designated system (section 8). Never in personal accounts, consumer AI tools, unapproved apps or unmanaged messaging. Never shared by link to "anyone". Special category and safeguarding information carries the highest care and is handled under the Child Protection and Safeguarding Policy and the Data Protection Policy.

6. Access control

- **Least privilege.** Each person has the access their role needs and no more. Access to confidential information is granted by role, through organisational units and shared-drive membership, not to individuals ad hoc.
- **Administrator access** to the Google tenant, TutorCruncher and Cloudflare is held by the smallest number of named role-holders the provision can operate with, and is recorded by the Systems Architect. Administrator accounts are separate from day-to-day accounts where the platform allows it, and are never shared.
- **Shared drives.** Manager rights are restricted. Membership is reviewed termly against the staff list (the Shared Drive Access Audit), and the review is recorded.
- **Safeguarding records** are held in TutorCruncher, with access limited to the DSL, the Deputy DSL and those the DSL authorises. The system is named deliberately; if it changes, this policy is updated.
- **Learner access** to the course library and the timetable portal is by Haven Google sign-in only. Learners cannot see one another's records.
- **Reviews.** The Systems Architect reviews administrator roles, third-party app access and shared-drive membership termly, and the full tenant configuration annually, recording each review and any change in the change log and, where relevant, the DPIA.

7. Accounts and the account lifecycle

Joiners. Accounts are created only when the pre-appointment checks in the Safer Recruitment and Use of Volunteers Policy are complete and recorded on the Single Central Record. New staff complete the induction in the Staff Induction Policy, including data protection and cyber security training, and sign the Staff Safer Internet Agreement and the BYOD declaration before they are given access to learner information.

Movers. When a role changes, access is adjusted the same week. Access that is no longer needed is removed, not left in place "just in case".

Leavers. On a person's last working day, the Systems Architect or Head suspends the account, removes shared-drive and administrator access, signs out and removes any registered device, and transfers ownership

of any files or Classroom courses The Haven needs to keep. Accounts are deleted after the retention period in the Data Retention Policy. The leaver checklist is recorded.

Authentication.

- **2-Step Verification is required** on every administrator and staff account, using an authenticator app or passkey. Enrolment is enforced at tenant level. Backup codes for the primary administrator account are printed and held securely by the Proprietor.
- Passwords are long, unique to The Haven and never reused from other services. In line with NCSC advice they are not changed on a schedule; they are changed at once if there is any suspicion of compromise. Passkeys are encouraged.
- Learner accounts use Haven Google sign-in. The requirement for 2-Step Verification on learner accounts is under review; the decision and its reasoning will be recorded in the change log and the DPIA.
- Credentials are never shared, written into documents, or sent by email or chat. Service credentials and API keys are held in the platform's own secret store, never in code or shared files.

8. Platforms and the tenant configuration standard

The Haven's information is held in a small set of approved platforms, each with a data processing agreement, listed publicly on the Service Providers and Data Processors page and in the processor register:

- **Google Workspace for Education:** email, Google Meet for live lessons, Google Classroom as the learning platform, Google Drive for files. The Haven's tenant, with a data region set to Europe and Google's Cloud Data Processing Addendum accepted.
- **TutorCruncher:** enrolment, timetabling and the safeguarding record.
- **Cloudflare:** hosting and sign-in protection for The Haven's own portals and course library.

Any other tool that handles Haven information must be approved under section 10 before use.

The Google tenant is configured to the following standard, set by the Systems Architect and recorded with each change in the tenant change log:

Area	Standard
2-Step Verification	Enforced for administrator and staff organisational units.
Third-party apps	Access to Haven Google data by third-party apps is controlled through API access controls. Approved apps are trusted; unconfigured apps are blocked for learners; staff access is limited to basic sign-in except for approved apps.
Marketplace	Allowlisted apps only. Staff cannot self-install add-ons.
Additional Google services	Off by default. Services that are not covered by the Workspace agreement are enabled only where there is an operational need, with each exception recorded and reviewed annually.
Drive sharing	New files are private by default. External sharing is limited to allowlisted domains. Sharing with "anyone with the link" is not permitted for Haven information and the setting is being withdrawn for staff and learner organisational units.
Devices	Endpoint Verification on every staff device (section 9).

Area	Standard
Data region	Europe.
AI tools	Enabled by organisational unit only for roles approved by the Proprietor (section 13).

The same standard applies to the Haven organisational unit on the charity's tenant, and that tenant is audited on the same cycle.

9. Devices

The Haven owns no devices; staff and learners work from their own. The rules are in the Bring Your Own Device (BYOD) Policy; the risks and residual risks are set out in the *Risk Assessment: Learner Access from Personally-Owned Devices*. In summary:

- Staff devices used for Haven work run a supported, up-to-date operating system with automatic updates on, have a screen lock, and have disk encryption turned on. Endpoint Verification is installed so the device's status is visible to the Systems Architect. Devices that no longer receive security updates are not used for Haven work.
- Haven accounts are accessed through the Haven Google profile, kept separate from personal browsing where the device is shared.
- Haven information is not stored on the device beyond what the platform caches; it stays in the platforms in section 8.
- A lost or stolen device is reported the same day so the Haven account can be signed out remotely and, where endpoint management allows, the Haven data on it wiped. A full remote wipe of a personally-owned device is not something The Haven can do or promises.
- Devices are removed from the tenant when a person leaves (section 7). Stale device entries are removed at the termly review.

10. Suppliers, processors and third-party apps

No tool, app, extension, AI service or platform handles Haven information until:

1. the Head (for classroom tools) or the DPO (for anything handling personal data) has approved it;
2. there is a written data processing agreement, with any sub-processors and hosting region known;
3. it is on the processor register, and the DPIA is updated where learners' data is involved;
4. the Systems Architect has configured access to it in the tenant.

Suppliers are asked what security assurance they hold (such as Cyber Essentials, ISO 27001 or SOC 2) and what their breach-notification commitment is; where they hold none, that is recorded as a risk. Tools that cannot be assessed (no identifiable company, no agreement) are blocked. Tools that are retired are removed from the tenant, their data exported or deleted, and recorded as retired on the processor register.

Personal accounts, free-tier tools and tools signed up to with a Haven email without approval are not permitted for Haven information. The Head keeps the audit of classroom tools in use; the Systems Architect reconciles it against the tenant's app-access report termly.

11. Logging, monitoring and detection

- The Google tenant's audit logs, security report and alert centre are the primary record of sign-ins, administrator actions, sharing and app access. TutorCruncher's access controls and logs cover the safeguarding record.
- The Systems Architect reviews the security report and alerts termly, and investigates unusual sign-in activity, new third-party app grants and changes to sharing settings. Findings are shared with the DPO and DSL.
- The Haven does not manage learners' or staff members' devices or home networks, so the DfE filtering and monitoring standards do not apply to it in the way they apply to a school's own network. Online safety during lessons is achieved through platform settings, supervised live sessions, lesson recording where that applies, and the human oversight described in the Online Safety & Acceptable Use Policy and the risk assessment above. The DSL holds senior responsibility for this and it is reviewed annually.
- The Haven holds **Cyber Essentials** certification, renewed annually, as independent assurance that the basic controls in this policy are in place. It does not run vulnerability scanning or penetration testing of its own, because it operates no infrastructure to scan; it relies on the security assurance of its platform providers and keeps the tenant configuration audit (section 8) as its own assurance.

12. Backups, resilience and continuity

- Information in Google Workspace and TutorCruncher is held redundantly by those providers. Google Vault is not currently configured; the retention of records is governed by the Data Retention Policy, and learner records of long-term value are held in TutorCruncher rather than Drive.
- The Haven's own web applications (the timetable portal, the course library and the policy site) are held in version control under The Haven's own organisation account, so they can be rebuilt from source.
- An independent off-tenant backup provider has not yet been selected; this is recorded in the DPIA as an open action for the DPO and Systems Architect.
- Loss of a platform, an account or a key person is covered by the Business Continuity Plan.

13. AI tools and the Diamond AI posture

Information security and AI risk are 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 as follows:

- **Approved AI tooling only.** AI tools are approved under the Responsible Use of AI Policy, added to the processor register with the terms that apply to the plan in use, and enabled in the tenant by organisational unit for the roles the Proprietor has approved. Staff approved to use AI with Haven accounts sign The Haven's internal agreement on its use.
- **Confidential information never enters consumer AI.** Staff do not put learner-identifiable, safeguarding-sensitive or commercially confidential information into consumer or personal-account AI tools. Approved tools, on Haven accounts, under the agreement, are the only route.
- **No offloaded security decisions.** AI may assist with log triage, anomaly spotting and phishing classification. Decisions to suspend an account, remove a device, notify the ICO or inform families remain with the DPO and the Head.

- **AI-generated threats.** Staff are trained to recognise AI-generated phishing, deepfake video or voice calls, and impersonation of senior leaders or parents. Any request to change bank details, share credentials, move money or release learner information that arrives by message, email or call is verified by a second channel before it is acted on, whoever it appears to come from.

14. Incidents

Any suspected information or cyber security incident (phishing, a compromised account, unauthorised access, malware, a lost device, a mis-sent email, a sharing mistake) is reported at once to the DPO and the DSL, and logged in the Cyber Incident Register kept by the DPO.

Containment, assessment, notification to the ICO within 72 hours where a personal data breach meets the threshold, notification to affected people, record-keeping and lessons learned follow **Part B of the Data Retention Policy and Data Breach Procedure**. That procedure is the incident response procedure for this policy.

Every incident is assessed for safeguarding implications. A breach may expose learner information, create opportunities for grooming or impersonation, or enable fraud. Where there is a safeguarding dimension the DSL leads under the Child Protection and Safeguarding Policy.

Staff who report an incident promptly, including their own mistake, are supported. Delay in reporting is the thing that is treated as a conduct matter, not the mistake itself.

15. Training and awareness

- All staff, contractors and volunteers complete data protection and cyber security training at induction and annually, recorded in the staff training record. The annual session includes phishing and impersonation, safe sharing, personal devices and AI.
- The Safer Internet Agreement and the BYOD declaration are re-issued and re-signed annually at the same session.
- Learners receive age-appropriate education on phishing, scams, passwords and safe digital conduct through the RSHE and online safety curriculum.
- Parents and carers are given the *Navigating the Digital Age of Consent* guide, and digital safety is a regular topic at the Haven Huddles held for parents and carers during term time.

16. Related policies and documents

Data Protection (UK GDPR), Confidentiality & Privacy Policy • Data Retention Policy and Data Breach Procedure • Bring Your Own Device (BYOD) Policy • Internet, Network and Email Policy • Staff Safer Internet Agreement • Online Safety & Acceptable Use Policy • Child Protection and Safeguarding Policy • Responsible Use of AI Policy • Safer Recruitment and Use of Volunteers Policy • Staff Induction Policy • Business Continuity Plan • Data Protection Impact Assessment (Consolidated) • Service Providers and Data Processors • Risk Assessment: Learner Access from Personally-Owned Devices • Tenant change log and audit record (internal) • Processor register (internal).

17. Monitoring and review

- **Termly:** the Systems Architect's review of the security report, app access, shared-drive membership and devices, shared with the DPO and DSL; the DPO's review of the Cyber Incident Register.

- **Annually:** full tenant configuration audit; review of this policy by the DPO, Systems Architect, DSL and Proprietor, with a report to the governing body.
- **Immediately:** after a significant incident, an NCSC or ICO alert, a change of platform, or a change in statutory guidance.

This PDF was generated from the published policy at policies.thehavenonline.school on 22 October 2026. The website is the authoritative, most current version of this policy.