# THE HAVEN

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

# Internet, Network and Email Policy

Use of The Haven's digital infrastructure

| | |
|---|---|
| **Document** | Internet, Network and Email Policy |
| **Version** | 05.26 |
| **Status** | live |
| **Last reviewed** | 21 May 2026 |
| **Next review** | 21 May 2027 |
| **Owner** | Data Protection Officer |
| **Approved by** | Proprietor + Governing Body |

## 1. Purpose

This policy sets out the expectations for use of The Haven's internet access, network infrastructure, and email systems. It exists to protect learners, staff, data and the integrity of our operations. It consolidates expectations that also appear in the Cyber Security Policy, BYOD Policy, Online Safety Policy and Staff Conduct Policy, and is the single reference point for routine internet, network and email use.

## 2. Scope

This policy applies to all staff, volunteers, contractors, governors and learners using The Haven's digital systems, including:

- The learning management platform and any associated tools.
- The Haven's email and messaging systems.
- Cloud storage, document and collaboration services used in Haven business.
- Any network connection — wired or wireless — used to access Haven systems.
- Access from personal devices, where covered by the BYOD Policy.

## 3. Principles

- Digital infrastructure is provided to support The Haven's mission. Its use should be consistent with that mission.
- Security and privacy are everyone's responsibility, not just the Data Protection Lead's.
- Filtering and monitoring exist to keep learners safe, not to surveil staff.

- Reasonable personal use of the internet by staff during breaks is permitted; the rules below describe what is not.
- Where personal devices touch Haven business, BYOD Policy expectations apply.

## 4. Internet access

### 4.1 Expected use

The Haven's internet access is provided for educational and operational purposes. Acceptable use includes:

- Delivering and accessing learning activities.
- Communicating with colleagues, learners, families, commissioners and partners through approved channels.
- Research connected to teaching, mentoring, professional development or administration.
- Reasonable personal use by staff during breaks, where it does not compromise safety, productivity, or the standards in section 4.2.

### 4.2 Prohibited use

The following uses of The Haven's internet access are prohibited:

- Accessing, downloading or sharing content that is illegal, including child sexual abuse material, terrorist content, or other material whose creation, possession or distribution is unlawful.
- Accessing pornographic, extremist, or other content that would breach the Staff Conduct Policy.
- Activity that breaches copyright, trademark or other intellectual property law.
- Bypassing or attempting to bypass The Haven's filters, monitoring, or security controls.
- Activity intended to compromise the security of The Haven's systems or those of others.
- Activity that contravenes the Online Safety Policy. Breach of this section is treated as a serious matter under the Staff Conduct Policy, and where applicable, the Managing Allegations Policy and the Safeguarding and Child Protection Policy.

### 4.3 Filtering and monitoring

In line with Department for Education filtering and monitoring expectations, The Haven applies appropriate filtering and monitoring to learner-facing systems. The Haven recognises that filtering is never complete, and that monitoring is a safeguarding tool, not a surveillance tool. Concerns identified through monitoring are routed to the DSL and handled under the Safeguarding and Child Protection Policy.

## 5. Network use

The Haven's networks are configured to support secure, reliable access to learning and administrative systems. Standard expectations:

- Network access requires authenticated credentials; credentials must not be shared.
- Devices connecting to The Haven's networks must meet basic security expectations: supported operating system, up-to-date security patches, active malware protection where applicable.
- Multi-factor authentication is required for accounts with access to learner or staff personal data.

- Suspected security incidents — phishing, suspected account compromise, lost devices — are reported immediately to the Data Protection Lead. Detailed cyber security expectations are set out in the Cyber Security Policy.

## 6. Email

### 6.1 Use of Haven email accounts

Every member of staff is issued with a Haven email account. Haven business is conducted via Haven email, not personal email. Specifically:

- Communication with learners and families is conducted only through Haven channels (email, learning platform or approved messaging tools).
- Communication with commissioners, schools, Local Authorities, and statutory partners is conducted through Haven email.
- Haven business is not conducted via personal email accounts. Personal email accounts are not to be used to receive Haven documents or learner data.

### 6.2 Email content standards

- Emails are written professionally, accurately, and respectfully.
- Personal data is shared only on a need-to-know basis. Special category data (including health, safeguarding and SEND data) is shared with particular care.
- Where sensitive material must be shared, encryption or secure-share methods are used in preference to standard email attachment.
- Distribution lists are checked before sending.
- Auto-forwarding from Haven email to a personal account is not permitted.

### 6.3 Phishing and email security

Staff are trained to recognise phishing and similar attacks. Suspected phishing emails are reported to the Data Protection Lead and not forwarded onwards. Staff do not click on suspicious links, enable macros from unknown sources, or open unexpected attachments.

### 6.4 Personal use of Haven email

Reasonable, occasional personal use of Haven email is permitted, provided it does not compromise security, productivity, or the standards in section 6.2. Personal use does not create an expectation of privacy: the Haven email system remains a Haven asset and may be accessed by the Data Protection Lead or Head where there is a legitimate need.

## 7. Learner internet, network and email use

### 7.1 Learner accounts

Learners are provided with accounts on the learning platforms required for their education. Account credentials are issued securely and not shared between learners. Accounts are deactivated at the end of placement.

### 7.2 Expectations of learners

- Learners use Haven systems for learning.
- Learners do not share account credentials, attempt to access others' accounts, or bypass filtering or monitoring.
- Learners do not record, photograph or screenshot sessions, peers, or shared materials (see Mobile Phone Policy — Learners and Declaration: Photos, Videos and Lesson Recordings).
- Learners report concerns about online safety to an educator, mentor or the DSL. These expectations are set out in family-friendly terms in the Family Attendance Agreement, which families and learners sign at admission.

### 7.3 Where a learner's use of systems is a concern

Where a learner's use of Haven systems crosses into a safeguarding concern — exposure to harmful content, contact with someone unsafe, online exploitation, or harmful behaviour towards peers — the response is led by the DSL under the Safeguarding and Child Protection Policy and Online Safety Policy. Routine breaches are addressed under the Relational Behaviour and Regulation Policy.

## 8. Data and retention

Email, document and platform activity may generate records that are personal data. Retention is governed by the Data Retention Policy. Access logs and audit records are retained for the period necessary to investigate concerns and to meet regulatory expectations.

## 9. Personal devices

Where staff use personal devices to access Haven systems, the BYOD Policy applies in full. Personal devices used to access learner or staff personal data must meet the security expectations set out there.

## 10. AI tools

Use of artificial intelligence tools accessed via The Haven's internet — including generative AI for drafting, summarising or analysis — is governed by the Responsible Use of AI Policy. Personal data is not entered into AI tools without explicit approval. Output of AI tools is reviewed by a human before use in any communication or document.

## 11. Roles and responsibilities

- Data Protection Lead: Owns this policy; coordinates security incidents; oversees filtering, monitoring and email security arrangements.
- Head: Approves access and addresses breaches that constitute conduct or safeguarding concerns.
- DSL: Leads safeguarding response where internet, network or email use crosses into safeguarding.
- Line managers: Reinforce expectations in their teams.
- All staff and volunteers: Use systems within the standards set out here; report concerns.
- Learners and families: Use systems as set out in the Family Attendance Agreement.

## 12. Related documents

- Cyber Security Policy
- BYOD Policy
- Online Safety Policy
- Data Protection Policy
- Privacy Notices
- Responsible Use of AI Policy
- Staff Conduct Policy
- Mobile Phone Policy — Staff
- Mobile Phone Policy — Learners
- Safeguarding and Child Protection Policy
- Family Attendance Agreement

## 13. 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 |

---

*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.*