

THE HAVEN

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

Bring Your Own Device (BYOD) Policy

Document	Bring Your Own Device (BYOD) Policy
Version	08.26
Status	live
Last reviewed	26 August 2026
Next review	29 April 2027
Owner	Data Protection Officer
Approved by	Proprietor

Date: August 2026

Review Date: April 2027

Coordinator: Data Protection Officer (DPO)

Nominated Governor: the Co-Chair of Governors

Version: v08.26

Linked Policies:

- Cyber Security Policy v01.26 (v1.0)
- Data Protection, Confidentiality & Privacy Policy v10.25 (v1.0)
- Staff Conduct Policy v10.25
- Responsible Use of AI Policy v10.26
- Child Protection and Safeguarding Policy v01.26
- Grievance and Low-Level Concerns Policies

1. Policy Statement and Purpose

The Haven recognises that many freelance educators, mentors, and contractors use personal devices to access The Haven systems and communicate with learners.

This policy sets out the conditions for such use to ensure **data security, safeguarding, and professional integrity** are maintained at all times.

The goal is to balance flexibility for staff with robust protection for Haven learners, data, and systems.

2. Scope

This policy applies to all staff, freelancers, contractors, and volunteers who use **personally owned devices** (laptops, tablets, or smartphones) to access:

- The Haven systems or data (e.g., Google Workspace, Google Meet, Google Classroom, TutorCruncher)
- Learner or family communications
- Any platform storing or transmitting confidential or safeguarding-related information.

3. Definitions

- **BYOD:** “Bring Your Own Device” — the use of personally owned technology for work purposes.
- **Device:** Any personal computer, tablet, or mobile phone used to access Haven data or systems.
- **Approved Platforms:** Those explicitly authorised by The Haven (e.g., Google Workspace for Education, Google Meet, Google Classroom, TutorCruncher).
- **Sensitive Data:** Any learner, family, staff, or confidential school information covered under UK GDPR.

4. Core BYOD Principles

Security First

- Devices must be **password-protected** and **encrypted**.
- **Multi-factor authentication (MFA)** must be enabled for all The Haven accounts.
- Devices must run **up-to-date operating systems** and security patches.
- Staff must install reputable antivirus/anti-malware protection.
- Devices must **auto-lock after 10 minutes of inactivity**.
- Public Wi-Fi should **not** be used for accessing The Haven systems unless connected via a **VPN**.

Data Handling

- The Haven data must never be stored permanently on personal devices.
- Files should be accessed and saved only within **approved The Haven cloud platforms**.
- Downloads containing sensitive data must be deleted immediately after use.
- No data may be transferred to personal USBs or external drives.

Prohibited Actions

Users **must not**:

- Share devices used for The Haven work with family or friends.
- Use The Haven data for personal purposes.
- Circumvent The Haven’s security controls (e.g., disabling MFA or firewall settings).
- Connect personal devices to unapproved or insecure platforms.
- Use AI tools that process identifiable learner data, unless approved under the Responsible Use of AI Policy v10.26.

- Use AI tools to make safeguarding, pedagogical, behavioural, SEND, or pastoral decisions on the user's behalf. Per the Haven's **Diamond AI posture** (work with AI; do not offload decisions to AI; do not defer entirely from AI), AI tools may assist with pattern-spotting, summarisation or accessibility, but the named role-holder retains professional judgement.

5. Monitoring and Audit

- The Haven reserves the right to **audit BYOD access logs** for compliance.
- The DPO and IT Lead may require confirmation of **encryption and patch status**.
- In case of a security breach or investigation, The Haven may request temporary access to the device for inspection or evidence collection.

6. Reporting and Incident Response

If a device used for The Haven work is:

- Lost, stolen, infected with malware, or suspected of breach,
 > the user must **report immediately** to the **DPO** and **DSL**.

Incidents will be logged in the **Cyber Incident Register** (per Cyber Security Policy v01.26 section 6) and may be reported to the **ICO within 72 hours** if a personal data breach has occurred.

7. Data Ownership and Privacy

- All The Haven-related data remains the property of The Haven.
- Upon termination of contract or project, the user must:
 - Delete all The Haven data from personal devices
 - Sign a **Data Deletion Declaration** (Appendix A).
- The Haven will not access personal, non-work-related content on the device but may verify compliance with data handling standards.

8. Safeguarding and Professional Conduct

- BYOD users must maintain **professional digital boundaries** consistent with the Staff Conduct Policy v10.25.
- Devices used for The Haven sessions must have **neutral, distraction-free backgrounds** and **no visible personal identifiers**.
- Staff must never engage in one-to-one messaging with learners outside approved channels.
- Any safeguarding indicators noticed during online sessions must be recorded and escalated in line with the **Child Protection and Safeguarding Policy v01.26**.

9. Enforcement

Failure to comply with this policy may result in:

- Restricted system access
- Withdrawal of BYOD permissions
- Termination of freelance contract (for serious or repeated breaches)

- Reporting to relevant safeguarding or data protection authorities where necessary.

10. Staff Declaration

I confirm that I have read, understood, and agree to The Haven *Bring Your Own Device (BYOD) Policy*.

I understand my responsibilities to maintain data security, safeguarding standards, and confidentiality when using personal devices for The Haven-related work.

Name (Print)	
Role	
Signature	
Date	

Compliance Note

This *Bring Your Own Device (BYOD) Policy*:

- **Fulfils the NCSC “5 Steps to BYOD Security”** for educational settings.
- **Aligns with KCSIE 2026** on staff digital conduct and online safeguarding.
- **Supports the Haven Cyber Security Policy v01.26** (Sections 5 & 6) on encryption, MFA, and breach response.
- Should be issued alongside the **Staff Safer Internet Agreement v10.25** as part of annual re-induction.

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.