

THE HAVEN

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

Child Protection and Safeguarding Policy

Document	Child Protection and Safeguarding Policy
Version	08.26
Status	live
Last reviewed	26 August 2026
Next review	29 April 2027
Owner	Designated Safeguarding Lead
Approved by	Proprietor

Approved Date: April 2026 (content revised August 2026 — see version history)

Review Date: April 2027

Coordinator: the Designated Safeguarding Lead

Nominated Governor: the Safeguarding Governor

Version: 01.26

Statement of Intent

The Haven is committed to safeguarding and promoting the physical, mental, and emotional wellbeing of every learner. As a flexible online learning ('hyflex') education provider, we recognise that safeguarding responsibilities apply across all digital spaces, including live online sessions, recorded lessons, chat functions, and communication platforms.

We adopt a whole-school preventative approach to safeguarding and child protection, ensuring robust systems are in place for learners, families, and staff across all virtual and digital environments.

This policy ensures:

- All stakeholders understand their safeguarding responsibilities under current UK legislation.
- Learners are taught to recognise and report unacceptable behaviour in both physical and online spaces.
- Staff are trained to identify learners at risk of abuse, neglect, or exploitation.
- Safer recruitment practices are embedded.
- A culture of openness, vigilance, and early intervention is fostered.

The Designated Safeguarding Lead (DSL) role is held by the Head; the Deputy DSL (DDSL) role is held by the SENCo. Current postholders' contact details are shared with staff and families at induction, and the DSL is always reachable at dsl@autisticgirlsnetwork.org. Both are trained to the appropriate level and are available during core operating hours.

Clarification on Digital Environments and Application

This policy applies to all virtual learning environments and digital communication platforms used by The Haven, including learning management systems, video conferencing tools, chat channels, and secure storage spaces. All safeguarding expectations, responsibilities, and reporting procedures apply equally across all digital contexts.

Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

Legislation

- Children Act 1989
- Sexual Offences Act 2003
- Female Genital Mutilation Act 2003 (as inserted by the Serious Crime Act 2015)
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Apprenticeships, Children and Learning Act 2009
- Equality Act 2010
- The Education (School Teachers' Appraisal) (England) Regulations 2012 (as amended)
- Anti-social Behaviour, Crime and Policing Act 2014
- Counter-Terrorism and Security Act 2015
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- The Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018
- Voyeurism (Offences) Act 2019
- Domestic Abuse Act 2021
- Marriage and Civil Partnership (Minimum Age) Act 2022

Statutory guidance

- Home Office (2023) 'Prevent duty guidance: Guidance for specified authorities in England and Wales'
- DfE (2023, last updated May 2025) 'Working Together to Safeguard Children'
- DfE (2018) 'Disqualification under the Childcare Act 2006'
- DfE (2026) 'Keeping children safe in education 2026'
- HM Government (2020) 'Multi-agency statutory guidance on female genital mutilation'

- HM Government (2023, updated August 2025) 'Channel Duty Guidance: Protecting people susceptible to radicalisation'
- Home Office and Foreign, Commonwealth and Development Office (2022, updated August 2025) 'Multi-agency statutory guidance for dealing with forced marriage and Multi-agency practice guidelines: Handling cases of forced marriage'

Non-statutory guidance

- DfE (2015) 'What to do if you're worried a child is being abused'
- DfE (2017) 'Child sexual exploitation'
- DfE (2018) 'Information sharing'
- DfE (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2021) 'Teachers' Standards'
- DfE (2023) 'Recruit teachers from overseas'
- DfE (2022) 'Working together to improve school attendance'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'
- Department of Health and Social Care (2022) 'Virginity testing and hymenoplasty : multi-agency guidance'

It is also aligned with:

- DfE guidance for remote education delivery: Providing remote education: guidance for schools Updated 2024
- Local safeguarding partner arrangements (by location of learner or provision)

Scope and platforms in use

The Haven delivers learning in **hyflex environments** (see definitions): live online lessons, occasional in-person activities, and asynchronous resources. The following platforms are in scope and governed by this policy and linked procedures: **Google Classroom** (core VLE), **Google Meet** (live sessions), **Google Workspace**, **TutorCruncher** (administration and the safeguarding record), and **email**.

No external community chat platforms are used for learner communication unless expressly authorised by the DSL and configured to Haven standards.

Definitions (key terms)

- **Hyflex environment:** Hybrid-flexible delivery where learners may attend live online, attend in person (where offered), or access recorded/asynchronous learning. Safeguarding duties apply continuously across all modes.
- **Child-on-child abuse:** Abuse by children towards other children, including bullying; sexual harassment/violence; upskirting; harmful sexual behaviour; initiation/hazing; and online abuse (group chats, DMs, file-sharing).
- **Anonymous reporting:** Routes that allow concerns to be raised without disclosing identity (see Section 4).
- **LADO:** Local Authority Designated Officer for allegations about adults who work with children.

- **MASH/Front Door:** Local authority single point of contact for safeguarding referrals (children at risk of significant harm).

Types of abuse (what we watch for)

The Haven recognises categories of abuse, as defined in Keeping Children Safe in Education (2026):

- Physical abuse
- Emotional abuse
- Cyberbullying, online exclusion, and trauma linked to digital isolation.
- Criminal Child Exploitation (CCE), including county lines involvement.
- Child Sexual Exploitation (CSE), including online grooming or coercion.
- Sexual abuse – contact and non-contact acts, grooming, or coercion, including digital exploitation and child sexual exploitation (CSE).
- Neglect
- Child-on-child abuse – abuse committed by one learner against another, including online or sexual harassment; consensual or non-consensual sharing of sexualised content; and activities involving harassment, abuse, or humiliation used as a means of initiating a person into a group.
- Domestic abuse – any incident or pattern of controlling, coercive, threatening, degrading, or violent behaviour observed between family members or partners.
- Female Genital Mutilation (FGM) of genital organs for non-medical reasons.
- Online abuse – grooming, exposure to harmful content, or creation of AI-generated or digitally manipulated imagery.

Contextual Safeguarding

The Haven adopts a contextual safeguarding approach, recognising that learners' experiences online extend beyond their home environment.

- Many of our learners have SEND profiles, or transient educational histories with gaps in information.
- These factors increase vulnerability to harm, isolation, or exploitation in digital spaces such as chat groups, gaming environments, and social media platforms.
- Staff are trained to consider each learner's broader digital context, understanding that signs of abuse or neglect may present differently in online settings.
- Trauma, loneliness, and digital disinhibition can heighten risk and require sensitive, relational safeguarding responses.
- Contextual safeguarding underpins The Haven's proactive approach: curiosity, documentation, and consistency of response across the entire digital ecosystem.

Digital Safety and RSHE

- The DfE *Filtering and Monitoring Standards* apply to devices and networks a setting owns or manages. 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 and receives no automated alerts. Control is exercised over Haven-managed accounts and platforms; the limits of that perimeter, and the controls that stand in their place, are recorded in the *Risk Assessment — Learner Access from Personally-Owned Devices*.
- Responsibility for technical oversight and cyber security rests with the Systems Architect, working with the Data Protection Officer, in line with the DfE *Cyber Security Standards for Schools and Colleges* and current DfE guidance on generative AI in education.
- The Haven's curriculum includes explicit RSHE content on online safety. Teaching addresses the four areas of online risk: content, contact, conduct, and commerce. Following *Keeping Children Safe in Education 2026*, generative AI is treated as a risk factor within contact and conduct — including harmful interactions with AI chatbots and companion-style systems, and the creation or sharing of nudes and semi-nudes that have been digitally altered or wholly generated using AI. Learners are supported to navigate misinformation, AI risks, sextortion, and digital misogyny.

Roles and Responsibilities

All staff:

- Must understand safeguarding can happen in both online and offline spaces
- Receive annual and contextual training, including online safety, filtering, and monitoring
- Are responsible for escalating concerns immediately to the DSL

Governors:

- Provide strategic leadership and oversight
- Ensure safeguarding is embedded across all hybrid delivery models

DSL:

- Oversees implementation of safeguarding practices in hyflex environments
- Maintains contact with local safeguarding partners, online safety regulators, and police where required
- Ensures staff are competent in digital safeguarding, incident reporting, and triage
- Leads safeguarding response to online and onsite concerns

Online and Hyflex Considerations

The Haven operates across multiple platforms.

Therefore:

- Monitoring of learner behaviour and communication must be proportionate, GDPR-compliant, and effective

- Staff will be trained in digital safeguarding tools and protocol for capturing, reporting, and escalating online incidents
- Learners are taught explicitly about digital safety, privacy, and respectful online behaviour
- The Designated Safeguarding Lead reviews online safety concerns and platform-level settings termly to identify safeguarding trends. The Systems Architect and the Data Protection Officer maintain and configure the technical systems. There is no automated alerting on learner device use; concerns reach the DSL through disclosure, staff observation and the reporting routes set out in this policy.

Managing disclosures & reporting (how to act, how to tell us)

If a child discloses to you:

- **Listen; don't investigate.** Reassure; avoid leading questions; note exact words where possible.
- **Do not promise secrecy.** Explain you may need to share information to keep them safe.
- **Ensure immediate safety.** If at imminent risk: call **999**.
- **Tell the DSL immediately** (or Deputy DSL if DSL unavailable).
- **Record within 1 working hour.**

How anyone can report a concern (including anonymous):

- **DSL team (core hours):** tammy@autisticgirlsnetwork.org or cathy@autisticgirlsnetwork.org
- **Anonymous reporting (racism & discrimination):** Anonymous reporting form — racism and discrimination (routed to the DSL; reviewed daily).
- **Other anonymous safeguarding concerns:** Anonymous reporting form — safeguarding concerns (routed to the DSL).
- **Out of hours / emergency: 999** (immediate risk)

Recording safeguarding concerns (what to write, where)

Use the Haven safeguarding log/system. Record: date/time; who was present; **verbatim** wording where possible; context (online/offline/platform); observed impact; immediate actions taken; who you informed/escalated to.

- **Don't** store notes on personal devices or send via personal email. All reports must be factual, dated, stored securely under UK GDPR and reviewed termly by the DSL.
- **Don't** promise secrecy; if requested, record that you explained why you could not.
- Upload relevant screenshots/links and any **lesson recording timestamps** (see Section 6).
- Patterns of recurring concern will be flagged for early intervention.
- All records are digital and maintained in The Haven's safeguarding record system, currently TutorCruncher. The system in use is named here deliberately; if it is replaced, this policy is updated at the same time.
- All safeguarding chronologies, family communications, and records of intervention are maintained within the same system.

- Staff receive training to ensure consistency, curiosity, and compliance in all safeguarding documentation.

Lesson recordings as evidence (when and how they're used)

All live lessons are recorded for quality, training, and safeguarding. Where a concern arises, the DSL may **extract, secure, and disclose** relevant clips as evidence to statutory agencies e.g., MASH/Front Door, Police) or the **LADO** for allegations about adults who work with children.

Access is strictly controlled; retention follows Haven's **Data Protection, Confidentiality & Privacy Policy v10.25** schedule (UK GDPR / DPA 2018).

Escalation pathways (DSL actions and LADO route)

The DSL (or Deputy DSL) will:

- **Child protection (non-staff):** Contact **MASH/Front Door** via published routes and thresholds; follow local procedures; record all actions/decisions.
- **Allegations about adults who work with children:** **Consult the LADO within 1 working day.
> **
- **Out of hours:** Use the local **Emergency Duty Service** for urgent situations and record actions.
- The DSL will maintain a log of referrals and their outcomes.
- The DSL will contact the home school of an AP learner to inform them of all safeguarding concerns, sending the safeguarding report form via email.
- Contact details for relevant LADOs are listed in the appendix.
- Concerns regarding learners or families will follow Social Care escalation routes as appropriate.

Early Help and multi-agency work (what “early help” means here)

The DSL coordinates Early Help so learners receive support at the right time. We work with: Family Hubs; CAMHS; School Nursing; Education Welfare; SEND services; Youth Justice; Police Public Protection; and voluntary/community partners. The DSL will:

- Undertake or contribute to Early Help assessments and plans;
- Share information lawfully and proportionately;
- Escalate to **MASH/Front Door** when thresholds are met; attend strategy meetings; contribute to child protection plans.

Safer recruitment (summary + cross-references)

Haven uses safer recruitment for onsite and online roles: safeguarding-signalled adverts; structured shortlisting; online footprint checks where appropriate; **enhanced DBS with barred-list**; identity/right-to-work/qualification verification; prohibition and, where relevant, overseas checks; **two references verified pre-start**; Single Central Record maintained and audited.

Associated policy: *Safer Recruitment and Use of Volunteers Policy v01.26* (read alongside this policy).

Out-of-hours provision & lone working (cover and boundaries)

Out-of-hours provision refers to any online activity conducted beyond normal operating times (e.g. evening or weekend sessions). Where Haven runs activities outside core hours, a **safeguarding-competent lead** is on call.

If DSL/Deputy DSL are unavailable, a named senior leader trained to DSL standard provides cover. Staff must comply with the *Lone Working Policy v10.25*, including venue risk assessments, agreed check-ins, and approved communication channels. For urgent concerns: ensure immediate safety → **999** if required → notify on-call safeguarding lead → record immediately on the safeguarding log in TutorCruncher → follow Emergency Duty Service as needed.

Who the Designated Safeguarding Lead is, and how to reach them

This published policy names the **role**, not the individual. The names and contact details of the current Designated Safeguarding Lead and Deputy Designated Safeguarding Lead are displayed prominently in TutorCruncher, where learners, families, staff and commissioning partners see them on signing in. They are also given at learner and family induction, in staff induction and training, and to commissioners in contracting.

The role is named rather than the person on the public site because publishing an individual's name on an open website makes it searchable against them personally. This is a deliberate decision of the Proprietor, not an omission, and it does not affect anyone's ability to find out who to contact.

Filtering & monitoring (leadership oversight)

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, arrangements are reviewed at least once every academic year and the review is recorded — when the checks took place, what was checked, what was identified and what was done about it.

What is reviewed reflects what The Haven actually controls: administrative settings on Haven accounts, platform configuration, restrictions on external contact, and the checking of resources before they are shared. The Haven does not operate device-level filtering or automated monitoring of learners, and does not claim to. The safeguarding response to that limitation is educational and relational rather than technical, and is set out in the *Risk Assessment — Learner Access from Personally-Owned Devices*.

Training

Training for all staff includes:

- Review of this policy and DfE (2026) 'Keeping children safe in education 2026'
- Introduction to the DSL, reporting routes, and safeguarding culture.
- Recognising safeguarding concerns that may arise both within and outside work contexts.
- Understanding safeguarding in an online environment:
 - awareness of how safeguarding principles apply in virtual classrooms and digital communication.
 - recognising signs of abuse, neglect, or distress that may be less visible online.
 - understanding the impact of learners' home environments, and maintaining appropriate professional conduct in all online interactions.
- Use of digital safeguarding platforms and protocols

- ensuring all staff are confident in using the organisation's online systems for logging, reporting, and escalating safeguarding concerns.
- understanding data protection, confidentiality, and secure digital communication when handling sensitive information or contacting learners.
- Managing disclosures online
- equipping staff to respond appropriately and sensitively if a learner makes a safeguarding disclosure during an online session, in chat, or through other virtual channels.
- Following agreed reporting procedures immediately, to record information accurately, and to ensure the Designated Safeguarding Lead (DSL) or Deputy DSL is informed without delay.

Student Induction Includes:

- Education on staying safe online and recognising digital risks.
- Information on lesson recording and data privacy.
- Clear explanation of how to report concerns and access support in the online learning space.

Attendance and Alternative Provision Reviews

The Haven distinguishes between absence and 'missing from education'. Where learners access alternative provision, placements are reviewed at least half-termly to ensure that safeguarding, engagement, and curriculum needs are met

DSL oversight ensures consistent risk assessment and communication with families.

Monitoring and Review

This policy will be reviewed annually or upon significant change in legislation, regulation, or operational model. Feedback from learners, staff and parents will inform updates.

Full appendices including specific safeguarding issues and operational guidance will be maintained and updated as annexes to this policy.

APPENDIX A

LADO / Allegations Contact Details by Local Authority

Local Authority	Contact Details
South Lanarkshire (Scotland)	Handled via Child Protection / Social Work. Phone: 0303 123 1008.
Forth Valley (Scotland)	Stirling: 01786 471177 Falkirk: 01324 506070 Clackmannanshire: 01259 225111 Out of Hours: 01786 470500.
North Yorkshire	Duty LADO: 01609 798005 Email: lado@northyorks.gov.uk

Local Authority	Contact Details
Birmingham	LADO Team: 0121 675 1669 Email: ladoteam@birminghamchildrenstrust.co.uk
Norfolk County Council	LADO: 01603 223473 Education Duty Desk: 01603 307797 Email: LADO@norfolk.gov.uk
Somerset	Somerset Direct: 0300 123 2224 Email: sdinputters@somerset.gov.uk
East Sussex	LADO: 01273 481544 Email: ESSCP.Contact@eastsussex.gov.uk
Wiltshire Council	LADO: 0300 456 0108 (Option 6) Email: LADO@wiltshire.gov.uk
Worcestershire	Duty LADO: 01905 846221 Email: LADO@worcestershire.gov.uk
Suffolk County Council	LADO: 0300 123 2044 Email: LADO@suffolk.gov.uk
Monmouthshire (Wales)	
Central Bedfordshire	LADO: 0300 300 8142 Email: LADO@centralbedfordshire.gov.uk
West Berkshire	LADO: 01635 503153 Email: LADO.LADO@westberks.gov.uk
East Hampshire (Hampshire County Council)	LADO: 01962 876364 Email: LADO@hants.gov.uk
London Borough of Hounslow	SAAM Duty Desk: 020 8583 5730 LADO: 020 8583 4933 / 020 8583 3423 Email: lado@hounslow.gov.uk

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.