

THE HAVEN

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

Data Protection Impact Assessment — Consolidated

Referral processing, operations, and the migration to Google Workspace

Document	Data Protection Impact Assessment — Consolidated
Version	08.26
Status	live
Last reviewed	16 August 2026
Next review	16 August 2027
Owner	Data Protection Officer
Approved by	Proprietor + Data Protection Officer + Designated Safeguarding Lead

One assessment for The Haven's processing of learner, family, referrer, commissioner and staff data, from first enquiry through online delivery, including the consolidation of the delivery stack onto Google Workspace and the planned retirement of legacy platforms.

Document	Data Protection Impact Assessment — The Haven (consolidated)
Scope	End to end: referral and intake (register-your-interest → referral form → placement decision), operations (TutorCruncher), delivery (Pencil Spaces/Canvas legacy; Google Workspace target), staff and safer-recruitment processing (Single Central Record), and the platform migration itself
Status	Approved by the Proprietor (16 August 2026) and published. The Data Protection Officer's and Designated Safeguarding Lead's confirmations are outstanding; risk scores remain indicative until the DPO confirms or amends them.
Version	v08.26
Controller	Autistic Girls Network (registered charity 1196655 in England and Wales; SC054837 in Scotland), operating The Haven
Legal basis for DPIA	UK GDPR Article 35 (high-risk processing involving children's data and special-category data)
Review	On completion of the Google Workspace migration, then annually, and before any significant change to processing takes effect

Executive summary

The Haven is a specialist online education provision for neurodivergent young people, operated by the Autistic Girls Network charity. It launched in September 2025, is pursuing accreditation under Ofsted's Online

Education Accreditation Scheme (OEAS), and is not a DfE-registered independent school. This consolidated DPIA covers the full processing lifecycle: from a commissioner's, school's or professional's first contact through the referral form, to placement and online delivery, together with the staff-side safer-recruitment processing behind the Single Central Record.

The assessment is deliberately framed around a moment of transition. The Haven is consolidating its delivery stack onto a new Google Workspace Business Plus tenant: Pencil Spaces is being replaced by Google Meet on cost grounds; Canvas (Instructure) is being replaced by Google Classroom following a ransomware incident at the vendor in which The Haven lost its hosted courses; and TutorCruncher, the current operations platform, is to be retired in a separately planned migration. Referral and SCR data currently flows through Google Forms in the charity's existing workspace. The migration is itself a processing risk and is assessed here alongside steady-state processing.

The processing is high-risk on ICO criteria on several independent grounds: children's data, special-category data (health, neurodivergence, ethnicity, gender identity and sexual orientation, safeguarding records), criminal-offence data (staff DBS and barred-list checks; LADO information), an online service to children, vulnerable data subjects, and data whose breach could expose children to harm. A DPIA is therefore mandatory under Article 35 UK GDPR.

The consolidated risk register at Step 5 holds twenty risks. Indicative pre-mitigation and residual ratings are proposed for each; these are for the DPO to confirm or amend. Three risks are rated High before mitigation: field-level visibility of special-category data in Google Forms response sheets (H1), the breadth of the single-stage referral form (H2), and the retirement of TutorCruncher with its accumulated learner records and free-text lesson reports (H7). None is assessed as remaining High after the proposed mitigations. Any residual high risk that cannot be reduced triggers prior consultation with the ICO under Article 36.

Step 1 — Identify the need for a DPIA

1.1 Screening

Indicator	Engaged?	How
Special-category data	Yes	Health, diagnoses, medication, neurodivergence and EHCP status, ethnicity, gender identity, LGBTQI+ identification, safeguarding and risk information
Vulnerable data subjects	Yes	All learners are children; the cohort is by design neurodivergent, frequently with EBSNA histories and prior harm in mainstream settings
Online service to children	Yes	Fully online provision; ICO Children's Code applies to all learner-facing surfaces
Systematic monitoring	Planned	Filtering and monitoring of learner accounts required before learner onboarding on the new tenant; own child DPIA
Evaluation, scoring or profiling	Yes	Structured risk-rating matrix (eleven safeguarding domains) completed at referral; attendance and engagement tracked in delivery
Data matching / combining datasets	Yes	Referrer, parent/carers, school-of-origin and commissioner data combined; records span Google Forms/Sheets, TutorCruncher and the new Workspace during transition
Data whose breach risks physical harm	Yes	Safeguarding records and risk ratings for at-risk children, including contact restrictions and court orders

Indicator	Engaged?	How
Criminal-offence data	Yes	Staff DBS, barred-list, prohibition, section 128 and overseas checks (SCR); LADO information
Innovative technology	Limited	No AI components process learner data at present; Gemini/NotebookLM off for all OUs pending policy, DPIA and training
Automated decision-making with significant effect	No	Placement and all learner-affecting decisions are human-made
Children's data for marketing or profiling	No	Parent/carers mailing-list opt-in only; no marketing use of learner data

Screening result: full DPIA required.

1.2 Article 9 / DPA 2018 Schedule 1 conditions

Special-category data is expected to be processed under Article 9(2)(g) — substantial public interest (safeguarding of children and individuals at risk), supported by DPA 2018 Schedule 1 Part 2 conditions and an Appropriate Policy Document, which The Haven must adopt (risk H20); Article 9(2)(a) — explicit consent, for photo and publicity use only; and Article 9(2)(c) — vital interests, in emergencies. Criminal-offence data (LADO information; staff DBS outcomes and SCR entries) is processed under Article 10 with the corresponding Schedule 1 conditions, including the employment condition for staff checks.

Two points for the DPO to settle. First, the published referral form cites Article 6(1)(e) (public task) with 9(2)(g); as a charity, The Haven is unlikely to hold a public-task basis in its own right, although commissioning local authorities do. The working view in this draft is that 6(1)(f) legitimate interests (with 6(1)(c) where statutory duties bite) is the better fit for The Haven's own processing — the DPO should confirm, and the notices should then be aligned (risk H4). Second, whether ethnicity and LGBTQI+ monitoring fields sit under 9(2)(g) equal-opportunities monitoring or explicit consent should be confirmed per field (Appendix B).

Step 2 — Describe the processing

2.1 Nature — referral and intake

Referral runs through a single Google Form (55 questions), linked from the register-your-interest page and completed by local authorities, schools and professionals. It collects, in one pass: referrer and commissioner business contact data; learner identity (full name — with initials invited as an option — date of birth, gender identity, pronouns, ethnicity, home address, local authority); parent/carers and social-worker contact details; contact restrictions and court orders; other agencies involved; health and safeguarding information (allergies, medical conditions and diagnoses, medication and self-administration, additional support needs); a structured risk-rating matrix covering eleven safeguarding domains, including self-harm and suicidal ideation, exploitation, online risk and grooming; an education and learning profile including EHCP status, attendance and time out of education; referral purpose and requested provision; commissioning and finance details; and consent declarations. Responses feed a Google Sheets response sheet in the charity's existing workspace, with queries handled through a role-based admissions inbox.

Two features of this design carry most of the intake risk: the form is single-stage, so special-category and risk data arrives before any placement decision exists (H2), and Google Forms cannot enforce field-level visibility on the response sheet (H1). The form's consent items are single-option confirmations completed by the

referrer rather than the family, and the privacy notice on the form cites a lawful basis that differs from the published privacy policy (H4, H5).

2.2 Nature — operations (TutorCruncher, current state)

TutorCruncher (a UK processor) is the current operations platform, holding client (parent/carer), learner, tutor and affiliate records, scheduling, lesson reporting and billing. Beyond built-in contact and billing fields, the configured custom fields include, for learners: legal and preferred name, date of birth, gender, ethnicity, LGBTQI+ identification, neurodivergence, EHCP status and review date, LADO details, local authority, school history, attendance and engagement notes, regulation and communication preferences, and free-text profile fields; for clients: relationship to learner, safeguarding worries declared, digital-safety concerns at home and notes, preferred check-in method, distress-response preference, mailing-list and WhatsApp-community opt-ins; and for tutors: date of birth, gender, ethnicity, DBS certificate number and dates, barred-list, prohibition, section 128 and overseas checks, safeguarding and Prevent training dates, and first-aid status. The system holds in the order of 165 client records, 75 learner records, 15 tutor records and 13,000+ free-text lesson reports. TutorCruncher is to be retired in a separately planned migration (H7); its safer-recruitment fields duplicate the SCR (H11).

2.3 Nature — delivery and the platform migration

Delivery is consolidating onto a dedicated Google Workspace Business Plus tenant on the provision's own domain, with the public website and policy site untouched on a separate domain. Pencil Spaces (live lessons; a US-based processor) is being replaced by Google Meet; Canvas (Instructure) has been replaced by Google Classroom after a vendor ransomware incident in which The Haven's hosted courses were lost; curriculum content moves over time into a private GitHub repository holding institutional knowledge only, never learner data. On the new tenant: every lesson is recorded as a standing safeguarding measure — recording rights are restricted to staff accounts, viewer download and copy are disabled, automatic transcription provides the host-held record of what was said, and access is controlled under the Lesson Recording — Operational Controls policy (host's Drive, shared once with the Head of School and the SENCo); access control is least-privilege and relationship-based; safeguarding, finance, HR and governance are walled domains; third-party OAuth access is blocked by default; Gemini and NotebookLM are off for all organisational units pending the Haven AI Policy, a DPIA and training; and Google Vault provides retention, eDiscovery and audit export. A UK-based filtering and monitoring tool for learner accounts is required before learner onboarding and carries its own child DPIA (Appendix C).

2.4 Nature — staff and safer recruitment (Single Central Record)

The Single Central Record expected under KCSIE 2026 is built natively in Google: staff complete a Google Form at onboarding (identity and right-to-work verification dates, DBS certificate number, issue and expiry dates and the date the certificate was seen by the DSL, barred-list, prohibition, section 128 and overseas checks, safeguarding, Prevent, SEND/inclusion and first-aid training dates), feeding a secured Google Sheet in the HR shared drive, access-restricted to the leadership group. This is Article 10 criminal-offence data processed for the employment and safeguarding conditions. Two clean-ups are flagged: training certificates are currently invited to a named individual's mailbox rather than a role inbox (H12), and the same checks are duplicated in TutorCruncher tutor fields (H11).

2.5 Scope

Aspect	Detail
Data subjects	Prospective and enrolled learners (children, typically 12–17); parents and carers; social workers and key workers; referrers and commissioner contacts (business data); staff, volunteers and contractors (including DBS / SCR criminal-offence data)
Volume	At July 2026: ~165 client records, ~75 learner records, ~15 staff records in TutorCruncher; 13,000+ lesson reports; referral volume continuous through term time
Storage	Google Forms/Sheets in the charity workspace (referral, SCR — moving to the Haven tenant); TutorCruncher (UK; until retirement); Pencil Spaces (US; until exit complete); Google Workspace Business Plus tenant (target); GitHub (institutional content only); off-tenant encrypted backup (to be selected)
Sources	Referrers and commissioners (Article 14 collection); parents and carers; school of origin; the learner (in delivery); staff (SCR); systems (attendance, audit)
Retention	To be consolidated in a Records Retention Schedule (H20). Published notice says learner records up to 6 years after leaving; the target architecture sets 7-year Vault retention with safeguarding-domain files longer; sector practice retains safeguarding records to the learner's 25th birthday. These must be reconciled. No retention rule exists for unsuccessful referrals (H13); TutorCruncher's DPA provides deletion within 10 business days of cessation.

2.6 Context

The Haven's cohort is by design vulnerable: neurodivergent young people, predominantly autistic, many with co-occurring ADHD, dyslexia, anxiety or PDA-profile presentations, many with EBSNA histories and prior harm in mainstream education. Families and professionals approaching The Haven are often in distress, and the data-subject relationship carries an inherent power asymmetry — the provision holds the placement the family seeks — which raises the standard for proportionate, transparent handling. All of The Haven's online surfaces are within scope of the ICO Children's Code. Because referrals are made by professionals rather than families, Article 14 transparency obligations do the heavy lifting and are currently under-served (H15).

2.7 Purposes

The Haven processes this data to: (1) assess whether the provision is appropriate for the young person; (2) plan and deliver the placement, including reasonable adjustments, regulation-first engagement and safeguarding cover; (3) communicate with families, professionals and commissioning local authorities; (4) meet statutory obligations (KCSIE 2026, the Online Safety Act 2023, the Equality Act 2010, the SEND Code of Practice 2015) and OEAS accreditation criteria, including equal-opportunities monitoring; (5) make safeguarding referrals where required; (6) operate safer recruitment and the Single Central Record; and (7) give commissioners proportionate attendance, progress and safeguarding assurance. Marketing is not a purpose of the learner processing; the parent/carer mailing list is a separate, opt-in purpose (H18).

Step 3 — Consultation

Internal: this draft is prepared for review by the Data Protection Officer, the Designated Safeguarding Lead and the Proprietor, with trustees of the operating charity sighted as required. The DPO's review completes the risk scoring at Step 5; the DSL and Proprietor own the safeguarding-relevant configuration decisions (Vault retention periods, safeguarding-group membership, break-glass thresholds, filtering and monitoring tool selection), which remain drafts until they sign them off.

External: the provision's parent and learner community provides feedback through established check-in routes, and learner and parent voice should be consulted on the refreshed privacy notices — including a learner-readable notice in an age-appropriate register — before the new tenant onboards learners. Sector context (including the ransomware incident at the former LMS vendor) directly informed the decision to consolidate onto Google Workspace rather than adopt another external LMS. The DPO advises whether any residual risk warrants prior consultation with the ICO under Article 36.

Step 4 — Necessity and proportionality

4.1 Lawful bases, by process activity

Bases are mapped to process activities rather than datasets. Items marked "DPO to confirm" carry the working view of this draft. The Haven should not rely on the referrer's consent declarations as its lawful basis (H5): they are confirmations of the referrer's authority and agreement to protocols, not data-protection consent from the data subjects.

Process activity	Article 6 basis	Article 9 / 10 condition
Register-your-interest enquiries and referral intake	6(1)(f) legitimate interests — DPO to confirm (form currently cites 6(1)(e))	9(2)(g) per the APD for health, SEND and safeguarding content
Placement decision and enrolment records	6(1)(f)	9(2)(g) where engaged
Delivery of education (lessons, assessment, attendance)	6(1)(f); 6(1)(c) where statutory — DPO to confirm	9(2)(g) where engaged
Safeguarding operations and referrals	6(1)(c); 6(1)(f)	9(2)(g); Article 10 for criminal-offence data (LADO)
Equal-opportunities monitoring (ethnicity; LGBTQI+ where retained)	6(1)(f)	9(2)(g) equality-monitoring limb — DPO to confirm vs explicit consent
Photo / publicity use	6(1)(a) consent	9(2)(a) explicit consent (the only consent-based learner processing)
Emergency disclosure	6(1)(d) vital interests	9(2)(c)
Billing, commissioner invoicing and family-paid placements	6(1)(b); 6(1)(c) for tax records	n/a
Staff employment, DBS and SCR	6(1)(b); 6(1)(c)	9(2)(b) employment; Article 10 per Sch 1
Commissioner reporting	6(1)(f); 6(1)(c) where statutory	9(2)(g) where engaged
Parent/carer mailing list and community WhatsApp	6(1)(a) consent (opt-in), with operable withdrawal	n/a

4.2 Data minimisation

The current referral form does not stage its collection: identity, special-category and risk data arrive together, at first contact, before any placement decision exists, and several sensitive questions are mandatory regardless of relevance. The staged pattern — contact-only expression of interest, a deliberately light first form, and full detail only after a discovery conversation and provisional offer — satisfies the minimisation

principle far better and is recommended as mitigation for H2. Each retained field should be assessed against "could the placement decision be made without this?" and the outcome recorded in a field schema. In delivery, minimisation is architectural on the new tenant: least-privilege, relationship-based access, walled domains, and no AI components receiving learner data.

4.3 Children's Code conformance

The target architecture conforms by design in most respects: default-private learner accounts, internal-only sharing for the Learners organisational unit, no advertising, no nudge techniques, no profiling for commercial purposes, and privacy-protective defaults (recording restricted to staff accounts, viewer downloads disabled, recordings never shared with learners or families, and access limited to the host, the Head of School and the SENCo). The material gaps are transparency and involvement: there is no learner-readable privacy notice, and learners are not currently party to the referral in which their data is shared (H15). A fifteen-standard self-assessment should be completed and appended before learner onboarding on the new tenant; the filtering and monitoring child DPIA carries the proportionality analysis for monitoring.

4.4 International transfers

Google may process data in the United States; transfers rest on UK adequacy (the UK-US Data Bridge) where applicable, otherwise the IDTA / UK Addendum via Google's standard terms. Pencil Spaces states that its service runs on servers based in the United States: while it remains in use, a Transfer Risk Assessment is required given children's data, and its exit should include deletion confirmation (H8, H17). TutorCruncher is UK-based; its standard DPA restricts transfers outside the UK/EEA without consent. The WhatsApp parent/carer community involves Meta's consumer service processing parent phone numbers outside the tenant (H14). A TRA is completed for each US-touching processor and held with the DPO.

4.5 Processors, due diligence and Article 28

Due diligence proceeds questionnaire-first, then executed DPAs — retrieved from the processor where published and reviewed by the DPO before reliance — then the RoPA update and the refreshed privacy notices, all before the new tenant onboards learners.

Processor	Processing	Status
Google (Workspace Business Plus)	Target delivery layer; Forms/ Sheets for referral and SCR	DPA review by the DPO; education-grade lockdowns configured manually on a commercial edition and documented
TutorCruncher Ltd (UK)	Operations: client, learner, tutor records; scheduling; lesson reports; billing	Live; published DPA template (10-business-day deletion on cessation) — countersigned copy to be held; retirement planned (H7)
Pencil Learning Technologies, Inc. (US)	Live lessons (legacy); US-hosted	Being replaced by Meet; DPA and TRA while in use; deletion confirmation on exit (H8)
Instructure (Canvas) (exited)	Former LMS; courses lost in vendor ransomware incident	Exit due diligence: confirm scope of any personal data affected; obtain deletion confirmation (H6)
Payment processors (via TutorCruncher)	Family-paid billing	Per TutorCruncher sub-processor terms; revisit at migration
SiteGround / Cloudflare / registrar	Website hosting, DNS, registration	Minimal personal data; controls documented in the architecture specification

Processor	Processing	Status
GitHub	Institutional repositories; curriculum knowledge layer	No personal data by design
Off-tenant backup provider	Independent encrypted backup	Not yet selected; DPA before use
Filtering and monitoring vendor	Systematic monitoring of learner accounts	Not yet selected; UK residency required; own child DPIA before learner onboarding

Step 5 — Consolidated risk register

All ratings are indicative and are the DPO's to confirm or amend. The register should be mirrored into the Data Protection Risk Register.

#	Risk and impact on individuals	Key mitigations	Pre	Residual
H1	Field-level visibility cannot be enforced in Google Forms / Sheets — any response-sheet user sees all fields, including special-category data and the risk matrix (referral) and criminal-offence data (SCR)	Response sheets restricted to two named accounts; sensitive columns split to a separately-permissioned sheet; sensitive-fields register reviewed quarterly; structural fix on migration into the domain-walled Drive architecture	High	Medium
H2	Single-stage referral form collects full identity, health, risk and finance data at first contact, before any placement decision exists; several sensitive fields mandatory	Stage the intake (light referral → conversation → full detail by individualised link after a provisional decision); field-by-field necessity review in a field schema; mandatory flags reviewed	High	Medium
H3	Referral and SCR data lives in the charity's shared workspace while the Haven tenant stands up — broader-than-necessary internal access during transition	Migrate forms and response sheets to the Haven tenant with least-privilege access; access list documented and reviewed; interim access audit	Medium-high	Low-medium
H4	Transparency materials inconsistent and partly out of date: policy cites contract basis, legacy domain and 6-year retention; form cites 6(1)(e) and "GDPR (2018)"; architecture sets 7-year Vault retention; no learner-readable notice	Single refreshed notice set aligned to confirmed bases and the Records Retention Schedule; learner-readable notice published before new-tenant onboarding; "UK GDPR" corrected throughout	Medium-high	Low
H5	Referral-form consent declarations are single-option confirmations completed by the referrer, conflating referrer authority with data-protection consent	Reword as referrer acknowledgements; record actual lawful bases; contact the family directly with the privacy notice (Article 14); gather true consents from the family	Medium	Low

#	Risk and impact on individuals	Key mitigations	Pre	Residual
H6	Legacy LMS vendor ransomware incident — scope of any personal data affected not formally closed out	Exit due diligence: written vendor confirmation of data categories affected, deletion, breach-notification position; record the assessment	Medium-high	Medium
H7	TutorCruncher retirement: learner records and 13,000+ free-text lesson reports to migrate or delete; over-export, orphaned copies, lost safeguarding context	Written migration plan with data mapping; minimum export into the domain-walled target; deletion under the DPA's cessation clause with written confirmation; DSL triage of safeguarding-relevant content	High	Medium
H8	Pencil Spaces processes children's data on US-based servers while in use	Complete the exit to Meet; DPA + TRA for the interim; account closure with deletion confirmation; no new learner data into the platform	Medium-high	Low-medium
H9	Safeguarding content accumulates in general-purpose fields (LADO details, safeguarding worries, digital-safety notes, lesson reports) outside the safeguarding domain wall	Migrate safeguarding content to the safeguarding drive (DSL-managed); field guidance for staff; lesson-report guidance (facts, no speculation, signpost to the concern route)	Medium-high	Medium
H10	TutorCruncher access is role-based — administrators see all records, including sensitive custom fields	Minimise admin accounts pending retirement; access review; relationship-based access is architectural in the target tenant	Medium	Low-medium
H11	Criminal-offence data duplicated between the SCR sheet and TutorCruncher tutor fields	Single canonical SCR in the HR drive; duplicates removed at migration; access restricted; APD and Sch 1 conditions documented	Medium-high	Low-medium
H12	SCR training certificates invited to a named individual's mailbox rather than a role inbox	Route to a role-based collaborative inbox feeding the HR drive; update the form text	Medium	Low
H13	No retention rule for unsuccessful referrals — special-category and risk data about children who never join persists indefinitely	Adopt a 28-day deletion rule; calendar trigger and monthly checklist; annual audit reported to the DPO; automate on the new tenant	Medium-high	Low-medium
H14	Parent/carer WhatsApp community: parent phone numbers processed by a consumer messaging service outside the tenant	Genuine opt-in with operable withdrawal; participant-visibility settings reviewed; group rules published; evaluate a tenant-native alternative	Medium	Low-medium
H15	Learners and families not party to the referral: Article 14 transparency under-served	Family pack with privacy notice on receipt of referral; learner-readable notice; learner voice at the intake conversation; acknowledgement fields on refreshed forms	Medium	Low-medium

#	Risk and impact on individuals	Key mitigations	Pre	Residual
H16	Meet recordings/transcripts capture learner image and voice; every lesson is recorded as a standing safeguarding measure, so volume is high and 7-year Vault retention of recordings may be disproportionate	Mandatory recording documented in the Declaration and the Lesson Recording — Operational Controls policy; recording rights staff-only; viewer download/copy disabled; access restricted to the host, the Head of School and the SENCo; DPO to advise on the recordings retention class (e.g. a shorter class unless pulled into a safeguarding file); transparency in notices	Medium	DPO to set
H17	International transfers (Google US; Pencil Spaces US) without completed transfer assessments	UK adequacy / Data Bridge analysis; IDTA / UK Addendum; TRA per US-touching processor; UK/EU residency options exercised where available	Medium	Low-medium
H18	Mailing-list opt-in collected inside admissions/operations records — purpose mixing	Separate marketing consent record; no learner data in marketing; suppression honoured immediately; purpose separation in the RoPA	Low-medium	Low
H19	No filtering and monitoring solution for learner accounts; systematic monitoring, once introduced, is itself high-risk	UK-residency tool selected against documented criteria before learner onboarding; dedicated child DPIA; transparency; human review of alerts	Not scored — child DPIA	Not scored
H20	Governance artefacts incomplete: APD, Records Retention Schedule, LIA, RoPA update, executed processor DPAs	Complete on the agreed sequence (questionnaires → DPAs → RoPA → notices) before the new tenant onboards learners; DPIA register maintained in the governance drive	Medium-high	Low-medium

Step 6 — Mitigation approach

Three structural points sit behind the register. First, the largest single mitigation is the migration itself, done well: the target architecture makes the key controls architectural rather than procedural — least privilege, relationship-based access, walled domains, immutable audit through Vault, third-party OAuth blocked by default — controls that fail safe rather than depending on vigilance. The corollary is that the transition period carries elevated risk (H3, H6, H7, H8), and the migration plan is treated as a data-protection artefact, not just an IT plan.

Second, the intake redesign (H1, H2, H5, H13) stages the collection, restricts the response stores, keeps special-category detail behind a real decision point, and puts a deletion rule behind every referral that does not proceed. Third, transparency is brought up to the standard the cohort deserves (H4, H15): one coherent notice set, aligned bases, and a learner-readable notice published before learners are onboarded onto the new tenant. Mitigation owners and completion dates are tracked in a companion actions record; the DPO's confirmation of the indicative scores completes this step.

Step 7 — Operational commitments

1. Referral and SCR response sheets restricted to two named accounts; access reviewed termly and on any staff change; audit-log review between reviews.

2. A 28-day deletion workflow for referrals that do not proceed — calendar trigger, monthly checklist, annual audit reported to the DPO.
3. Two-factor authentication mandatory on all staff accounts; hardware keys on admin accounts; break-glass access notifies the DSL and is reviewed within five working days.
4. The staged intake pattern once adopted: full health, risk and finance detail only by individualised link after a provisional decision.
5. A sensitive-fields register held with the DPO and reviewed quarterly.
6. Photo / publicity consent gathered from families (not referrers), recorded in a consent register checked before any use; withdrawal honoured immediately.
7. Workspace audit log reviewed monthly; Alert Center digest reviewed weekly by leadership.
8. Due-diligence questionnaires, executed DPAs, and TRAs for US-touching processors before the new tenant onboards learners.
9. The TutorCruncher retirement executed under a written migration plan with DSL triage of safeguarding-relevant content and written deletion confirmation.
10. Deletion or return confirmations obtained from every exited platform (Pencil Spaces, Canvas) and filed in the governance drive.
11. No AI component receives identifiable learner data; Gemini and NotebookLM remain off pending the Haven AI Policy, a signed DPIA and staff training.
12. The filtering and monitoring tool selected, and its child DPIA completed, before any learner is onboarded onto the new tenant.
13. The learner-readable privacy notice published and surfaced before learner sign-in; families receive the privacy notice directly on receipt of any referral.
14. DPIA review on completion of the migration, annually thereafter, and before any significant change takes effect; field schemas re-captured against the live forms at each review.

Step 8 — Sign-off

The DPO's advice, and whether it is followed, is recorded here on completion of their review of the indicative risk scores. Safeguarding-relevant configuration remains draft until the DSL and the Proprietor sign it off. This DPIA does not require submission to the ICO unless residual risk exceeds the acceptable threshold and cannot be mitigated; any such residual high risk triggers prior consultation under Article 36.

Role	Outcome	Date
Proprietor — The Haven	Approved — sign-off recorded in the policy library's document control	16 August 2026
Data Protection Officer — Autistic Girls Network / The Haven	Pending — review of the indicative risk scores outstanding	
Designated Safeguarding Lead — The Haven	Pending — safeguarding-relevant configuration remains draft until signed off	
Trustee representative — Autistic Girls Network (as required)	As required	

Appendix A — Data flow

Current state. Public website (register-your-interest) → referral Google Form (55 questions, single stage) → response sheet in the charity workspace → admissions triage via the role-based admissions inbox. Referral accepted → client, learner and placement records in TutorCruncher → scheduling and lesson reports in TutorCruncher → live lessons in Pencil Spaces (exiting) / Google Meet. Staff onboarding → SCR Google Form → secured sheet in the HR area. Referral not accepted → no deletion rule currently defined (H13).

Target state (post-migration). Light referral form → conversation → full detail by individualised link → response stores inside the Haven tenant with least-privilege access → placement record in the domain-walled Drive architecture. Delivery on the Haven tenant: Classroom, Meet (every lesson recorded as a standing safeguarding measure; staff-only recording rights), Calendar, Vault; curriculum knowledge in a private GitHub repository holding no learner data. Safeguarding content in the safeguarding drive only (DSL-managed); SCR canonical in the HR drive; commissioner reporting proportionate and portfolio-level. No placement → deletion within 28 days. Leavers → retention per the Records Retention Schedule; secure destruction thereafter.

Appendix B — Lawful-basis mapping (field categories)

Field category	Article 6	Article 9 / 10
Referrer / commissioner business-contact and finance data	6(1)(f); 6(1)(b)	n/a
Learner identity, contact, education status, provision requested	6(1)(f)	n/a
EHCP status and review dates; neurodivergence; sensory and regulation needs	6(1)(f)	9(2)(g)
Health: allergies, conditions and diagnoses, medication, support needs	6(1)(f)	9(2)(g)
Risk-rating matrix; contact restrictions and court orders; agencies; safeguarding worries; LADO	6(1)(c); 6(1)(f)	9(2)(g); Article 10 for LADO content
Ethnicity (monitoring)	6(1)(f)	9(2)(g) equality monitoring — DPO to confirm
Gender identity, pronouns, LGBTQI+ identification	6(1)(f)	9(2)(g) — DPO to confirm limb and necessity per field; treat pronouns as pastoral, not monitoring, data
Photo / publicity	6(1)(a)	9(2)(a) explicit consent
Parent/carers mailing list; WhatsApp opt-in	6(1)(a)	n/a
Staff identity, right to work, qualifications, training	6(1)(b); 6(1)(c)	9(2)(b) where engaged
Staff DBS, barred-list, prohibition, section 128, overseas checks (SCR)	6(1)(c)	Article 10; DPA 2018 Sch 1 per the APD

Appendix C — Companion and child DPIAs

This consolidated DPIA does not discharge: the filtering and monitoring tool selection (before any learner is onboarded onto the new tenant); learner account provisioning on the Haven tenant; the TutorCruncher

decommission and data migration plan (H7); any Gemini for Workspace or NotebookLM enablement; any new third-party AI tool, per the Haven AI Policy authorisation process; the parent/carer community WhatsApp review, if retained beyond the migration (H14); and any new placement type or commissioning arrangement processing new data classes. Each needs its own DPIA or addendum before go-live of that element, hung off this parent document and filed in the DPIA register in the governance drive.

This document names no individuals; every owner is a role, per the Haven vault convention. Prepared with AI assistance. Approved by the Proprietor on 16 August 2026; the DPO's confirmation of the risk scores and the DSL's sign-off of safeguarding-relevant configuration remain outstanding and are recorded at Step 8 when complete.

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.