

Child Safety & Safeguarding Policy

How we keep children who use our platform safe, and how everyone working on the platform must act to protect them.

Document owner	Humaira Ahmed — Designated Safeguarding Lead (DSL) & Data Protection Officer (DPO)
Approved by	The Board of Learnaroo Ltd
Applies to	All Learnaroo Ltd staff, contractors and volunteers, and all features of learnaroohub.com
Version	1.0
Effective date	22 June 2026
Review cycle	Annually, or sooner on any KCSIE update or material change to the service
Classification	Public
Contact	support@learnaroohub.com

This policy is published for parents, carers, schools, trusts, auditors and inspectors. It should be read alongside our Privacy Statement and Online Safety Framework.

1. Purpose and scope

LearnarooHub is a learning platform used by children. Their safety is a primary design constraint, not an afterthought. This policy sets out how we protect children who use the platform from harm, and the standard of behaviour we require from everyone working on it. It applies to all Learnaroo Ltd staff, contractors and volunteers, and to every feature of learnaroohub.com. Where we work with schools and trusts, we align our practice with their statutory duties so they can rely on our service within their own safeguarding arrangements.

2. Legal and regulatory framework

We have regard to, and align our practice with, the following:

- Keeping Children Safe in Education 2025 (KCSIE) — statutory safeguarding guidance
- The Children Act 1989 and 2004, and Working Together to Safeguard Children
- The UK GDPR and the Data Protection Act 2018
- The ICO Age Appropriate Design Code (the “Children’s Code”)
- The Online Safety Act 2023

3. Definitions

Child: anyone who has not yet reached their 18th birthday. **Safeguarding:** protecting children from maltreatment, preventing impairment of their health or development, ensuring they grow up with safe and effective care, and taking action to enable the best outcomes. **Online safety:** protecting children from the risks they may face on connected services, grouped by KCSIE as content, contact, conduct and commerce (the “four Cs”).

4. Roles and responsibilities

- **Designated Safeguarding Lead (Humaira Ahmed)** — holds lead responsibility for safeguarding on the platform; receives and acts on concerns; liaises with schools, the NSPCC and statutory agencies where needed; and maintains safeguarding records.
- **Senior leadership / the Board** — accountable for safeguarding governance, resourcing and approving this policy, and for ensuring online-safety risks are understood and managed at leadership level.
- **All staff and contractors** — complete safeguarding awareness training; recognise and report concerns promptly; follow our safe-conduct expectations; and never attempt to handle a serious concern alone.
- **Schools and trusts (as data controllers)** — remain responsible for safeguarding their own pupils; we act on their documented instructions as a data processor.

5. Recognising and reporting concerns

Anyone with a safeguarding concern — a member of the public, a parent, a teacher or a member of staff — should report it without delay by emailing support@learnaroohub.com with “Safeguarding” in the subject line, for the attention of the DSL. Staff must report any concern to the DSL the same day. We do not investigate child-protection matters ourselves: where a child may be at risk we will support, and where appropriate refer to, the relevant school's DSL, local authority children's social care, or the police. **If a child is in immediate danger, call 999.**

6. Safer conduct and recruitment

Staff and contractors are expected to maintain professional boundaries with children at all times and to follow our acceptable-use and safe-conduct expectations. Access to children's data is granted on a least-privilege basis and removed promptly when a person changes role or leaves. Roles with access to children's personal data are subject to appropriate pre-engagement checks.

7. Online safety on the platform

We manage the online-safety risks set out by the DfE (the four Cs) by design:

- **Content:** learning resources are reviewed and published by trusted adults before children see them; there is no open, unfiltered web browsing inside the platform.
- **Contact:** LearnarooHub is not a social network; children cannot be contacted by, or contact, people they are not deliberately connected to through their school or family.
- **Conduct:** the platform follows the ICO Children's Code, with privacy-friendly defaults and age-appropriate language, and no design patterns that pressure children to share more than they need to.
- **Commerce:** we never show advertising to children and never sell, rent or use children's data for marketing.

8. Data protection and information security

Protecting children's information is central to safeguarding. The following controls are in force on the platform:

- **Encryption in transit:** all connections use HTTPS/TLS, enforced with HTTP Strict Transport Security (HSTS).

- **Encryption at rest:** sensitive pupil, staff and parent data — including special-category welfare data and identifiers such as date of birth and Unique Pupil Number — is encrypted in the database, with keys held separately from the data.
- **Searchable without exposure:** identifiers that must be searchable use a one-way “blind index”, so records can be matched without storing the value in readable form.
- **Access control:** server-side, role-based permissions on every request, with strict per-school and per-trust isolation so one organisation can never see another’s data.
- **Secure sign-in:** two-factor authentication is required for all staff and administrator accounts; public self-registration is disabled.
- **Accountability:** security-relevant administrative actions are written to a tamper-evident, append-only audit log.
- **Infrastructure:** hosted on Hostinger Business hosting, which provides a web application firewall (WAF), DDoS protection, malware scanning and regular backups.

We maintain a Data Protection Impact Assessment (DPIA) and a Record of Processing Activities (ROPA), and we are actively working towards Cyber Essentials certification.

9. Data retention

We keep a pupil’s records for as long as they are at the school and for six years after they leave. Financial records are kept for six years. After the applicable period, data is securely deleted or anonymised.

10. Working with schools and trusts

When a school or trust uses LearnarooHub, the school (or trust) is the data controller and decides how pupil data is used; Learnaroo Ltd is the data processor, acting on documented instructions under the UK GDPR. We make a Data Processing Agreement available that sets out roles, security measures and sub-processors. Our hosting provider (Hostinger) is our key infrastructure sub-processor, engaged under its own data-processing terms. We support schools’ audits and inspections and can share our DPIA and ROPA on request.

11. Rights, records, monitoring and review

Individuals can ask to see the data we hold, to correct it, and in many cases to have it deleted; requests should be sent to the DPO at support@learnarohub.com, and complaints may also be made to the Information Commissioner’s Office (ICO) at ico.org.uk. Safeguarding concerns and actions are recorded. This policy is reviewed at least annually, and sooner on any KCSIE update or material change to the service.

12. Company and regulatory details

Legal entity	Learnaroo Ltd
Company registration	[Company number pending incorporation — to be confirmed]
Registered address	[Registered address pending — to be confirmed]
ICO registration	ZA000000 [placeholder — to be replaced with the live ICO reference]
DSL / DPO	Humaira Ahmed, Cambridge — support@learnarohub.com