Hasab
ሐሳብ ኮንሰልታንሲ

Safeguarding & Child Protection POLICY

VERSION II

2026

Digital Safeguarding and Child Protection Policy

Company: Hasab Consultancy & Training PLC

Platform: Freedom Learning K-12

Effective Date: September 2026

1. Purpose

This policy outlines the absolute commitment of Hasab Consultancy & Training PLC to protecting K-12 students, their parents, educators, and all other users from harm within the digital environments of the Freedom Learning platform. It defines our comprehensive standards for safety, privacy, and inclusivity in the design, delivery, and moderation of our educational technology services.

2. Scope

This digital safeguarding and child protection policy strictly applies to:

- All Hasab Consultancy & Training PLC employees, developers, contractors, administrators, and partners.
- All digital platforms, mobile applications, video conferencing tools, and third-party integrations provided under the Freedom Learning K-12 ecosystem.
- All K-12 students enrolled in or utilizing the platform for educational purposes.
- Parents, caregivers, educators, tutors, and school administrators interacting with the platform.

3. Safeguarding Commitment

Freedom Learning is committed to:

- Designing safe, inclusive, age-appropriate, and engaging learning experiences for all K-12 developmental stages.

- Protecting children from abuse, exploitation, cyberbullying, grooming, and inappropriate contact by peers or adults.
- Maintaining strict professional boundaries between educators and students within all digital communication channels.
- Providing highly visible, accessible, and child-friendly mechanisms for reporting concerns.
- Protecting students' personal, academic, behavioral, and health-related information from misuse or unauthorized access.
- Ensuring absolute compliance with relevant local and international data protection and child safety laws.

4. Legal and Regulatory Compliance

Hasab Consultancy & Training PLC aligns the Freedom Learning platform with the highest international standards, including:

- General Data Protection Regulation (GDPR) and relevant local data privacy laws.
- Children’s Online Privacy Protection Act (COPPA).
- United Nations Convention on the Rights of the Child (UNCRC).
- Web Content Accessibility Guidelines (WCAG) and Universal Design for Learning (UDL) Guidelines.

5. Key Safeguarding Risks in K-12 Online Learning

- **Inappropriate Educator-Student Contact:** Blurring of professional boundaries, unauthorized private messaging, or inappropriate relationships.
- **Cyberbullying & Peer-to-Peer Abuse:** Harassment, exclusion, or harmful interactions via chat, forums, collaborative documents, or video breakout rooms.
- **Inappropriate Content:** Accidental or intentional exposure to violent, sexual, or developmentally inappropriate material.

- **Online Grooming & Intrusion:** Bad actors (internal or external) attempting to contact minors for exploitation, including "Zoombombing" or unauthorized classroom access.
- **Privacy and Data Misuse:** Unauthorized sharing of academic records, behavioral profiles, or sensitive student data with third-party advertisers or unvetted applications.
- **Algorithmic Bias & Academic Profiling:** Over-reliance on automated systems that may unfairly categorize or disadvantage certain students.

6. Protective Design Features & Moderation

Freedom Learning applies strict "Safety by Design" principles:

- **Role-Based Access Control (RBAC):** Strict permissions ensuring adults can only access classrooms and student data relevant to their specific educational role.
- **Monitored Communications:** Profanity filters and automated flagging systems for inappropriate text, supplemented by human moderation in community spaces.
- **Secure Video Conferencing:** Waiting rooms, disabled private peer-to-peer chat during live lessons, and enforced recording policies (where legally permitted and consented).
- **Safe Reporting Tools:** "Report a Concern" buttons built directly into the student dashboard, allowing for easy and anonymous reporting.
- **Zero-Targeting Policy:** Absolute prohibition of targeted advertising, behavioral profiling, or selling of student data.

7. Roles and Responsibilities

7.1 Executive Management

- Provide overall oversight and officially approve policies.
- Allocate the necessary resources for effective platform moderation.

- Ensure absolute legal compliance across all operations.

7.2 Designated Safeguarding Lead (DSL)

- Lead comprehensive safeguarding training for all staff.
- Receive and thoroughly investigate escalated concerns.
- Coordinate incident response and liaise directly with local authorities when necessary.

7.3 Product & Technical Team

- Integrate robust privacy and safety features directly into the platform's code.
- Secure servers against unauthorized access and breaches.
- Ensure any integrated third-party educational tools meet strict internal safeguarding standards.

7.4 Educators & Tutors

- Maintain strict professional boundaries with students at all times.
- Actively moderate live digital sessions and classrooms.
- Immediately report any suspected bullying, abuse, or student distress to the DSL.

7.5 Parents & Caregivers

- Supervise their child's physical learning environment whenever possible.
- Engage actively with the platform's built-in parental controls.
- Promptly report any platform or safety concerns to the school or platform administrators.

8. Training and Capacity Building

- All staff, educators, and developers must complete mandatory digital safeguarding and child protection training during onboarding, with an annual refresher.
- Training includes identifying signs of digital abuse, understanding online grooming, managing cyberbullying, and enforcing professional digital boundaries.
- Educators receive specialized training on managing secure live online classrooms and utilizing moderation tools effectively.

9. Incident Reporting and Response Procedures

Reporting Channels:

- Dedicated safeguarding email: safeguarding@freedom.edu.et
- In-app "Report Concern or Comment" button (accessible on every student and teacher page).
- Anonymous web form and Whatapp and Telegram Chat bots available in the Help Center.

Response Timeline:

- **Acknowledgment:** Within 24 hours of receipt.
- **Triage & Internal Investigation:** Commences immediately; initial findings within 72 hours.
- **Escalation to Authorities:** Immediately upon suspicion that a child is at risk of significant harm or if a crime has been committed.
-

Confidentiality:

All reports are handled with the utmost sensitivity. Information is shared strictly on a "need-to-know" basis to protect the victim and the integrity of any investigation.

10. Data Protection and Privacy

- We collect only the minimum personal and academic information necessary to deliver our K-12 educational services.
- We mandate explicit parental/caregiver consent for data collection for users under the legal age of digital consent in their respective region.
- We provide transparent, easy-to-read privacy notices explaining exactly how data is used.
- We utilize enterprise-grade encryption for data in transit and at rest.
- We enforce a strict data retention and secure deletion policy when a student leaves the platform or upon graduation.

11. Monitoring, Audit, and Review

- The DSL and Technical Team will conduct quarterly audits of platform safety logs, flagged chat histories, and incident reports to identify emerging risks.
- This policy will be reviewed annually, or immediately following any significant safeguarding incident, change in legislation, or major platform update.

Policy Declaration

Freedom Learning K-12, owned and operated by Hasab Consultancy & Training PLC, unequivocally believes that every child has the right to learn in a safe, secure, and supportive environment. We are committed to fostering a digital ecosystem where academic excellence thrives alongside the highest standards of child protection, privacy, and digital well-being.