مـــدرســـة الإبـــداع
الـعـلـمـي الـدولـيـة
INTERNATIONAL SCHOOL
OF CREATIVE SCIENCE

DIGITAL SAFEGUARDING POLICY

2025 - 2026

International School of Creative Science – Nad Al Sheba

Digital Safeguarding Policy

Academic Year 2025-26

Document Information			
Created Date August 2025			
Created by:	Principal	Reviewed by:	Principal
Review Cycle:	One Year	Next Review:	August 2026
Principal: Ataullah Parkar			

Table of Contents

1. Purpose, Ethos and Legal Alignment

At ISCS NAS, safeguarding extends beyond the physical environment to the digital spaces where children learn, communicate and create. Our ethos, rooted in Islamic values and the Barakah culture, frames digital behaviour as an amanah (trust): integrity in online conduct is expected both in public and in private. We educate pupils to act with honesty, self-discipline and respect; we expect adults to model the same.

This policy sets out how we protect pupils online and manage digital technologies across the school. It aligns with UAE Federal Law No. 3 of 2016 (Wadeema's Law – Child Rights Law), UAE Federal Decree-Law No. 45 of 2021 (Personal Data Protection Law), UAE Federal Decree-Law No. 34 of 2021 (Cybercrime Law), KHDA requirements, BSO standards, and the latest Keeping Children Safe in Education (KCSIE 2025) including online safety, filtering/monitoring, safer recruitment, information sharing and record-keeping standards.

2. Scope

This policy applies to students, all staff, governors, volunteers, contractors, visitors, and third-party providers using or providing access to the school's networks, devices, platforms and data.

3. Definitions (plain language)

- **Digital safeguarding:** protecting children from harm online through education, proportionate controls, monitoring, and effective response.
- **Filtering:** blocking access to harmful, illegal or inappropriate content.
- **Monitoring:** identifying concerning patterns/keywords/behaviours on school systems to enable timely pastoral/safeguarding support.
- **Personal data:** any information that identifies an individual; handled according to UAE data protection law and school policy.

4. Risk Landscape and Rationale

Following KCSIE 2025, we plan for four, overlapping online risk domains—content, contact, conduct, commerce—and explicitly include misinformation, disinformation and conspiracy content. We teach pupils to question provenance, recognise manipulation, and respond safely (report/seek help). We also address grooming, sexual/extremist content, cyberbullying, gaming risks, scams/phishing/in-app purchases, image-based abuse, deepfakes/AI-generated content, and over-sharing of personal data.
We recognise the impact of digital use on wellbeing, including screen time, online pressures, body image, sleep and self-esteem. Staff remain alert to these factors, provide pastoral support and signpost pupils to wellbeing resources as part of our safeguarding response.

5. Roles, Governance and Accountability

5.1 Principal

Holds ultimate accountability; ensures staffing, systems and budgets support this policy.

5.2 Designated Safeguarding Lead (DSL) [Ataullah Parkar]

Leads digital safeguarding; oversees practice, case management, thresholds, external referrals; assures the quality of records including the rationale for decisions; briefs SLT and governors termly (or sooner if risks escalate).

5.3 Safeguarding Governor [Hesham Abdeen]

Provides independent challenge and oversight; receives DSL reports (termly); assures BSO-aligned annual audits of digital safety, including filtering/monitoring and data protection practice.

5.4 Designated Digital Safeguarding Lead (DDSL) [Seeni Hussaina]

Owns the operational detail of filtering, monitoring, MDM, risk assessments for new technologies (e.g., AI tools), and staff/parent technical briefings; works in tandem with the DSL.

5.5 IT Network & Data Team

Implements and reviews filtering/monitoring to DfE standards; assures cyber controls to DfE Cyber Security Standards; reports weekly trends and immediate alerts to the DSL; maintains secure identity and access management.

5.6 All Staff

Complete Safeguarding Level 1 annually (with e-safety modules); model professional use; use only school systems for pupil images/communications; report concerns within 24 hours; understand what filtering/monitoring does (and does not) do.

5.7 Students

Follow the Pupil AUP; protect personal data and passwords; report concerns promptly.

5.8 Parents/Carers

Support the home–school partnership: enforce boundaries at home; understand school filtering/monitoring; never publish images of other children without permission.

5.9 Third-party/Alternative Provision

We secure written assurance that safeguarding checks, equivalent filtering/monitoring, and suitable supervision are in place; placements are reviewed regularly and ended if risks emerge.

6. Education: Curriculum, Progression and Culture

We deliver a progressive, age-appropriate online safety curriculum across Computing, PSHE and Islamic Education. Pupils learn critical skills (privacy, digital footprint, respectful conduct, media literacy, reporting routes, resilience to false information, and safe creation/use of AI tools). Assemblies, workshops, and student voice activities reinforce key messages; parents receive annual briefings.
Student Voice/Leadership - We actively involve pupils in shaping digital safeguarding practice through student voice mechanisms such as surveys, focus groups and digital leaders.

7. Technical Controls: Filtering, Monitoring, Cyber Resilience

7.1 Filtering (prevention)

We block illegal/harmful content (e.g., pornography, exploitation, extremism, gambling, pro-suicide, hate speech), anonymisers/VPNs and high-risk platforms. Categories and exceptions are reviewed at least termly; urgent blocks can be deployed immediately. Leadership, DSL and IT share oversight to meet DfE Filtering & Monitoring Standards (adapted to our UAE context).

7.2 Monitoring (detection & response)

We monitor school devices/accounts to flag risky patterns/keywords (e.g., self-harm, grooming, radicalisation). Alerts are triaged by the DDSL/DSL; critical indicators are escalated within 1 hour to the DSL for safeguarding action. Staff are trained annually on roles/limits of monitoring—it does not replace vigilance or pastoral relationships.

7.3 Cyber Security

We benchmark against DfE Cyber Security Standards: secure identity management (MFA/strong passwords), patching, backups, incident response, least-privilege access, and staff phishing awareness.

7.4 DSL–IT Regular Review

The DSL/DDSL and IT Network Team meet at least monthly to review MDM, filtering, monitoring and cyber security reports, ensuring oversight of patterns, urgent issues and system effectiveness.

8. Devices, Platforms and Accounts

Managed devices only (students and staff) connect to school Wi-Fi via MDM; pupils lack admin rights. Staff capture any pupil work/images only on school-issued devices; storage is restricted to Microsoft 365 school accounts. Data handling follows UAE law and school policy.

8.1 Remote / Hybrid Learning Protocols

In any period of remote or hybrid learning, staff and pupils follow the same safeguarding expectations as on site. Lessons are delivered via approved school platforms only; cameras, recordings and chat functions are used in line with published school guidance. Parents are briefed on supervision and environment standards to ensure safe learning from home.

9. Mobile Phone and Personal Technology Policy (practice and rationale)

Students - To reduce distraction, unauthorised recording, exposure to harmful content and contact risks, students may not carry smartphones in school. Any device brought must be handed to administration at arrival and collected at dismissal. Breaches are handled under behaviour/safeguarding procedures and, where relevant, UAE law.

Staff - Personal phones are not visible or used in lessons. The school provides secure devices for capturing learning; all images/videos are stored only within school Microsoft 365. Moving pupil data/images to personal devices/accounts is a disciplinary matter and may constitute an offence under UAE Cybercrime Law.

10. Artificial Intelligence and Emerging Technologies

We apply a risk-assessment gateway to new tools (e.g., generative AI). Approval considers: age-appropriateness; data processing; content filters; bias; explainability; misuse potential (e.g., deepfakes); and classroom supervision. Use must align with DfE expectations for filtering/monitoring and product safety guidance for generative AI referenced by KCSIE 2025. Pupils are taught safe, ethical AI use and are prohibited from using AI to produce harmful or deceptive content.

11. Safer Use of Images, Social Media and Communications

Staff–pupil communications and file-sharing occur only via school systems. We obtain and record parental consent parameters for photography/video; consent can be withdrawn. We never post pupil images with full names; we avoid content that enables geo-identification. Parents are reminded not to post images of other children without permission and to avoid defamation or unlawful content per UAE law.

Our digital safeguarding approach respects cultural and Islamic values, including modesty, dignity and respectful language online. Staff, pupils and parents are expected to uphold these values in digital communication and content sharing.

12. Early Help, Attendance, Alternative Provision

We recognise absence/withdrawal from learning—online or in person—can signal harm. Staff follow school procedures for early help and escalate concerns to the DSL. Where alternative provision or online provision is used, we retain safeguarding responsibility, verify provider checks, and review placements regularly.

13. Reporting Concerns, Managing Incidents and Record-Keeping

Routes to report. Any student/parent/staff member may report: to a trusted adult, the class/form teacher, the DSL, or via [school reporting form]. Anonymous reports are reviewed with the same seriousness.

Response standards. Critical indicators (e.g., self-harm, grooming, exploitation, extremist content): DSL within 1 hour. All other concerns: logged and triaged within 24–48 hours. Records are kept securely; the DSL ensures that the rationale for decisions is recorded and that information is shared proportionately with those who need to know.

External notifications. Where thresholds are met or the law may be breached, the DSL consults with senior leaders and initiates notifications to KHDA and/or relevant authorities in line with UAE legislation and school procedures.

14. Staff Training and Induction (including Level 1)

All staff complete Level 1 Safeguarding annually; e-safety (online risks, filtering/monitoring expectations, reporting) is embedded and refreshed every year. DSL/DDSL undertake advanced training on online risks, AI, cyber, record-keeping and supervision. Governors, including the Safeguarding Governor, receive induction and regular refreshers on digital safeguarding, data protection and oversight responsibilities.

15. Safer Recruitment and Staff Conduct (digital elements)

Online searches are undertaken on shortlisted candidates as part of due diligence; findings are handled lawfully, proportionately and recorded. Low-level concerns and allegations processes reference digital boundaries; patterns are reviewed to prevent harm (applied within UAE regulatory context).

16. Information Sharing with Parents/Carers

We proactively explain to parents: what pupils do online at school; which platforms are used; who they interact with (staff/peers); and how filtering/monitoring works (capabilities and limitations). We provide practical home-safety guidance and annual e-safety updates to maintain a strong home–school partnership.

17. Data Protection, Privacy and Records

We comply with UAE Personal Data Protection Law; our privacy notices, retention schedules, DPIAs and incident response plans are maintained and reviewed. To strengthen practice, our procedures also draw on recognised toolkits (e.g., DfE data protection) adapted for our context.

18. Audit, Assurance and Continuous Improvement

Termly: DSL report to the Safeguarding Governor (trends, incidents, training completion, system updates). Annually: a BSO-aligned Digital Safeguarding Audit (policies; curriculum; staff/pupil/parent feedback; filtering/monitoring effectiveness; cyber resilience; recruitment and induction; alternative provision checks). After Action Reviews follow significant incidents to capture lessons learned and update practice. Policy Review: at least annually, or earlier if legislation/technology changes.

Appendices (operational detail)

Appendix A — Pupil Acceptable Use Policy (AUP)

Principles in practice: use devices for learning; protect privacy; be kind online; ask for help; never share passwords; never post/share images of others without consent; report worries immediately. Progressively differentiated by phase with examples and short scenarios.

Appendix B — Staff ICT Acceptable Use Agreement

Core expectations: professional communications only on school systems; no storage of pupil data/images on personal devices/accounts; no personal phone use in class; multi-factor authentication; strong passwords; locking devices; reporting losses/breaches immediately.

Appendix C — Parent Digital Code of Conduct

At home: device rules, screen-time boundaries, safe search, age-appropriate platforms, modelling respectful conduct, and reporting pathways. Online: do not post images of other children; avoid defamatory content; respect UAE law.

Appendix D — Filtering & Monitoring Statement

What we block; how exceptions are controlled; how monitoring works; who sees alerts; how quickly we respond; how long logs are retained; how we communicate limits (monitoring ≠ surveillance of private life).

Appendix E — AI and New Technology Risk Assessment Template

Purpose, audience, data flows (DPIA), content checks, age appropriateness, misuse scenarios, staff supervision, off-boarding/retention.

Appendix F — Incident Response Flow (with timescales)

Concern identified → immediate safety actions (if needed) → DSL within 1 hour if critical → record with rationale → parents (where appropriate) → external notifications (if thresholds met) → support plan → review.

Appendix G — Data & Records (Privacy, Retention, Security)

High-level retention table (e.g., safeguarding records retained per school policy/UAE requirements; alert logs for a defined period); secure storage and access; breach response; staff responsibilities.

Appendix H — Roles & Training Matrix

Who completes what (Level 1; DSL/DDSL advanced; governor induction; IT technical standards; annual refreshers), with evidence sources and deadlines.

Appendix I — Alternative Provision / External Clubs Checklist

Safeguarding checks; staff vetting assurance; filtering/monitoring parity; site addresses; review schedule; escalation routes.