



Online Safety (E Safety) Policy

September 2025

Governor responsibility	Academic
Owner/Author	Headteacher
Date & version	February 2026 V3
Next review date	September 2026

Moon Hall School Online Safety Policy 2025

1. Introduction

Moon Hall School is committed to safeguarding and promoting the welfare of children. Online safety, formerly referred to as e-safety, is an essential part of this commitment.

This policy aligns with Keeping Children Safe in Education 2025, the Education (Independent School Standards) Regulations, the Data Protection Act 2018, UK GDPR, the Online Safety Act 2023–25, and relevant guidance from the Department for Education, UKCIS, ICO, and Ofcom.

Online safety includes risks arising from websites, platforms, social media and AI-enabled tools. Misuse of AI is treated as an online safety and safeguarding concern.

2. Scope & Objectives

This policy applies to:

- All pupils, staff, governors, volunteers, contractors, and community users with access to school ICT systems
- All use of school technology and online platforms
- All personal devices, including mobile phones, used on the school premises

Objectives:

- Ensure that pupils are appropriately supervised during school activities
- Promote responsible behaviour with regard to online and digital activity
- Take account of legislative guidance, including UK GDPR and the Data Protection Act 2018

3. Roles and Responsibilities

- Designated Safeguarding Lead (DSL): Lead responsibility for safeguarding and child protection, including online safety and AI-related harm. Oversees filtering and monitoring, reports to governors, and coordinates incident responses
- Deputy DSLs: Support monitoring, training, and incident response
- Chief Operating Officer and Network Manager: Ensure technical implementation of filtering and monitoring systems, compliance with DfE Digital and Technology Standards, and cyber security
- Governors: Hold leaders to account for robust online safety practice, including an annual review
- Staff: Embed safe online practice in teaching, supervise pupil use of technology, ensure professional digital conduct, and report concerns immediately
- Pupils: Use school systems responsibly, comply with acceptable use rules, and report concerns
- Parents and Carers: Support safe online practice and follow school rules on digital images, systems access, and personal devices
- Community users and contractors: Must sign acceptance of online safety policies if given network or device access

4. Filtering & Monitoring

- The school maintains appropriate and proportionate filtering and monitoring in line with DfE standards
- Systems are reviewed annually and tested for effectiveness
- Over-blocking is avoided to ensure learning is not unreasonably restricted
- Leaders and DSLs understand system operation and escalation routes

5. Use of Generative AI

This policy covers AI-enabled harms including deepfake imagery, nudification applications, AI-assisted doxing and impersonation. These are safeguarding concerns and may constitute criminal offences.

- Only approved AI tools that meet DfE Generative AI Product Safety Expectations may be used
- No unnecessary personal, sensitive, or safeguarding data may be entered into AI systems
- Students may use AI under supervision for learning purposes and must credit AI-assisted work
- Staff may use AI for lesson resources and administration with accuracy checks and data minimisation
- The school maintains an AI risk assessment and register of approved AI tools, reviewed annually

6. Mobile Phones & Personal Devices

- In line with DfE guidance, pupils are prohibited from using mobile phones during the school day unless specifically authorised
- Searching, screening and confiscation follow DfE guidance and the Behaviour Policy
- AI-enabled wearable devices are prohibited on site unless authorised for SEND accessibility, with risk assessment and parental consent
- Covert recording or live streaming is forbidden

7. Education & Curriculum

Online safety education is embedded in PSHEE, computing and the wider curriculum, and adapted for SEND learners.

- Mis and disinformation and critical thinking
- AI-generated content and deepfakes
- Sextortion and online exploitation
- Sharing nudes and semi-nudes including AI-generated imagery
- Grooming and inappropriate online contact
- Self-harm content and harmful challenges
- Digital resilience, respectful communication, plagiarism and copyright
- Doxing and AI-enabled covert recording or live streaming risks

8. Staff Training

- All staff receive annual training on online safety, filtering and monitoring, AI risks, reporting procedures, and KCSIE updates
- Induction training includes online safety for new staff

9. Parent/Carer Engagement

- Parents and carers receive updates on emerging online risks, including AI-enabled harm
- The school shares resources to support safe technology use at home
- Incidents involving AI are treated as safeguarding matters and escalated appropriately

10. Responding to Incidents

- The school follows UKCIS Sharing Nudes and Semi-Nudes guidance
- Incidents may include AI-generated imagery, sextortion, cyberbullying, or grooming
- Staff must report immediately to the DSL, preserve evidence, and avoid unnecessary viewing

11. Data Protection & Children's Privacy

- The school complies with UK GDPR and the ICO Children's Code
- All online services are assessed for compliance, with profiling off by default and data minimisation applied

12. Monitoring & Review

This policy is reviewed annually or sooner if guidance or legislation changes. The DSL and COO report to governors on filtering effectiveness, training, incident trends, and AI and emerging technology risks.

Governors also receive an annual Online Safety and AI Risks report, including updates to the AI Register and student voice feedback.

Associated Policies

- [Safeguarding and Child Protection Policy](#)
- [Pupil Behaviour Policy](#)
- [SEND Policy](#)
- [Anti-Bullying Policy](#)
- [AI Policy](#)

Advisory Guidance & Resources

- [KCSIE 2025](#)
- [DfE Digital & Technology Standards \(Filtering & Monitoring; Cyber Security\)](#)
- [DfE Generative AI: Product Safety Expectations \(2025\)](#)
- [DfE Mobile Phone Guidance \(2024\)](#)
- [UKCIS “Sharing Nudes and Semi-Nudes” Guidance \(2024 update\)](#)
- [Online Safety Act 2023–25 \(Ofcom Codes\)](#)
- [ICO Children’s Code](#)
- [Teaching Online Safety in Schools – DfE](#)
- [NSPCC Online Safety Resources](#)
- [Love Life: NSPCC resources for young people with learning disabilities](#)
- [Online Safety for Learners with SEND \(KELSI\)](#)