MHS
Reigate

E Safety Policy

September 2025

Governor responsibility	Academic
Owner/Author	Headteacher
Date & version	September 2025 V2
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 (KCSIE) 2025**, the **Education (Independent School Standards) Regulations**, the **Data Protection Act 2018**, the **UK GDPR**, and relevant guidance from the **Department for Education (DfE)**, **UKCIS**, **ICO**, and **Ofcom**.

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 the UK GDPR and Data Protection Act 2018.

3. Roles and Responsibilities

- **Designated Safeguarding Lead (DSL):** Lead responsibility for safeguarding and child protection, including online safety. Oversees filtering and monitoring (F&M), reports to governors, and coordinates incident responses.
- **Deputy DSLs:** Support the DSL in monitoring, training, and incident response.
- **Chief Operating Officer (COO) & Network Manager:** Ensure technical implementation of F&M systems, compliance with DfE Digital & Technology Standards, and cyber security.
- **Governors:** Hold leaders to account for robust online safety practice, including an annual review of F&M.
- **Staff:** Embed safe online practice in teaching, supervise pupils’ use of technology, ensure professional use of digital communication, and report concerns immediately.
- **Pupils:** Use school systems responsibly, avoid plagiarism, uphold copyright rules, follow acceptable use policies, and report concerns. They must comply with rules on mobile devices, images, and cyberbullying.
- **Parents/Carers:** Support good online safety practice, follow school rules on digital/video images, accessing school systems, and use of personal devices.
- **Community Users/Contractors:** If given access to school networks/devices, must sign acceptance of online safety policies.

4. Filtering & Monitoring (F&M)

- The school maintains appropriate, proportionate F&M in line with DfE standards.
- Systems are reviewed annually and tested for effectiveness.
- Over-blocking will be avoided to ensure learning is not unreasonably restricted.
- Leaders and DSLs must understand how systems operate and how to escalate concerns.

5. Use of Generative AI

This policy covers AI-enabled harms including deepfake sexual imagery, nudification apps, and AI-assisted doxing. These are safeguarding concerns and may be criminal offences. All staff must escalate immediately to the DSL (Michelle Catterson).

- Only approved AI tools that meet DfE's Generative AI: Product Safety Expectations (2025) may be used.
- No personal, sensitive, or safeguarding data (e.g., pupil names, SEN details, incidents) may be entered.
- Students may use AI under supervision for learning purposes and must credit AI assisted work.
- Staff may use AI for lesson resources/admin with accuracy checks and in line with data minimisation principles.
- The school will maintain an AI risk assessment and a register of approved AI tools, reviewed annually.

6. Mobile Phones & Personal Devices

- In line with DfE guidance (2024), pupils are prohibited from using mobile phones during the school day (including breaks) unless specifically instructed (e.g. use of cameras in art).
- Searching, screening, and confiscation will follow DfE guidance and the school Behaviour Policy.
- Wearable AI devices (e.g. smart glasses, audio assistants, heads-up displays) are prohibited on site unless authorised for SEND accessibility, with risk assessment and parental consent. Covert recording/live streaming is forbidden.

7. Education & Curriculum

Online safety will be embedded in PSHEE, computing, and wider curriculum. Teaching will cover:

- Mis/disinformation and critical thinking.
- AI generated content.
- Sextortion and online exploitation.
- Sharing nudes/semi-nudes (including AI-generated imagery).
- Grooming and inappropriate online contact.
- Self-harm content and harmful challenges.
- Respectful communication, digital resilience, plagiarism, and copyright.
- Deepfake awareness and manipulated media
- Doxing as a form of online abuse
- Risks of AI-enabled covert recording and live streaming

Curriculum will be adapted for SEND learners.

8. Staff Training

- All staff receive annual training on online safety, F&M, AI, reporting procedures, and KCSIE updates.
- Induction training includes online safety for new staff.

9. Parent/Carer Engagement

- Parents receive updates on emerging risks, including implementation of the Online Safety Act (2025).
- The school shares resources to help families support safe technology use at home.
- Incidents involving AI (deepfakes, doxing, covert recording, hostile live streams) will be treated as safeguarding matters. Evidence must be preserved and reported to the DSL (Michelle Catterson). Where appropriate, incidents will be escalated under the Online Safety Act (Ofcom takedown routes) and to law enforcement/CEOP.

10. Responding to Incidents

- The school follows UKCIS "Sharing Nudes and Semi-Nudes" guidance (2024 update).
- Incidents may include AI generated sexual imagery, sextortion, cyberbullying, or grooming.
- Staff must not view imagery unnecessarily, must report immediately to the DSL, and preserve evidence.

11. Data Protection & Children's Privacy

- The school complies with UK GDPR/DPA 2018 and the ICO's Children's Code (AADC).
- All online services used are assessed for compliance (profiling off by default, geolocation disabled, transparency, and data minimisation).

12. Monitoring & Review

This policy is reviewed annually or sooner if guidance/legislation changes. The DSL and COO report to governors on:

- Effectiveness of F&M.
- Training and curriculum updates.
- Incident trends and responses.
- AI and new technology risk assessments.

Governors will also receive an annual Online Safety & AI Risks report, including updates to the AI Register, AI tool assessments, incident trends, and student voice feedback.

Associated Policies

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- SEND 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)

Approved by Governors: September 2025

Next Review: September 2026