LONDON MATHS & SCIENCE COLLEGE

www.lmsc.org.uk

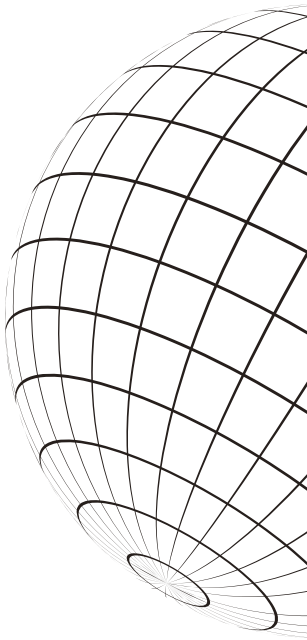
eSafety & Online Safety Policy

London Maths & Science College

167 Commercial Road, London, E1 2DA

info@lmsc.org.uk

ESAFETY AND ONLINE SAFETY POLICY



Legal entity: London Maths & Science College (LMSC) – Limited Company (Companies House No. 16822143)
Registered office / campus: 167 Commercial Road, London, E1 2DA
General contact: info@lmsc.org.uk
Document Owner: Principal / Head of Centre
Approved by: Proprietor / Governing Body
Effective date: 18 February 2026
Review date: 18 February 2027
Version: 1.3

Table of Contents

1. Purpose

London Maths & Science College (LMSC) is committed to providing a safe environment for learning and working, including when learners and staff use technology, online platforms and digital services. This policy sets out LMSC's arrangements for **online safety (eSafety)** across in-person, online and hybrid delivery.

This policy aims to:

- protect learners (including those under 18) from online harm;
- set clear expectations for safe, responsible and lawful use of technology;
- ensure effective **filtering and monitoring** of IT systems and networks;
- define roles, reporting routes and response procedures for online safety incidents; and
- align online safety practice with safeguarding, Prevent, data protection and exam integrity expectations.

Online safety is treated as a **safeguarding** issue.

---

2. Scope

This policy applies to:

- all learners, staff, contractors and visitors using LMSC systems, devices, networks or services;
- use of LMSC technology on-site and off-site (including remote learning and home working); and
- personal devices used for learning or work where they access LMSC platforms and services (BYOD).

This policy must be read alongside LMSC's:

- Safeguarding and Child Protection Policy
- Behaviour Policy and Student Code of Conduct
- Staff Code of Conduct / Safer Working Practice
- Learner and Staff Acceptable Use Policies
- Digital Privacy Policy and Data Protection Policy
- Prevent Policy and Risk Assessment
- IT Incident / Breach Reporting Procedure
- Remote/Hybrid Learning Policy

- Malpractice & Maladministration Policy (including academic integrity and AI expectations)

---

3. Regulatory and guidance framework

LMSC's online safety arrangements reflect:

- **Keeping Children Safe in Education (KCSIE) 2025** (online safety as part of safeguarding systems and staff training/updates).
- DfE **Filtering and Monitoring Standards for schools and colleges (March 2023)** (annual review expectation and governance).
- DfE **Filtering and monitoring – core standard** (digital and technology standards).
- UKCIS **Education for a Connected World (2020)** curriculum framework.
- **Prevent duty guidance** (specified authorities in England and Wales).
- UK GDPR / Data Protection Act 2018 and ICO guidance where personal data is processed.

---

4. Definitions

Online safety / eSafety: Safeguarding and promoting welfare when using technology, online platforms, networks and digital services.

Filtering: Technology that limits access to harmful or inappropriate online content.

Monitoring: Observing or reviewing user activity on systems to identify safeguarding and security risks.

Harmful content: Content that may be illegal, inappropriate, abusive, exploitative, extremist, sexually harmful, violent, hateful, or otherwise unsafe.

---

5. Policy statement

LMSC will:

1. Maintain robust safeguarding arrangements that include online safety.
2. Provide appropriate filtering and monitoring and **review provision at least annually**.
3. Teach learners how to keep themselves safe online through tutorial/pastoral programmes and curriculum opportunities aligned to UKCIS guidance.
4. Provide staff training and at least annual safeguarding/online safety updates, with additional updates as needed.
5. Respond to online safety incidents promptly and proportionately, using safeguarding thresholds and reporting duties.
6. Work with parents/carers and relevant agencies where concerns indicate risk of harm, criminality, exploitation or radicalisation.

---

6. Roles and responsibilities

6.1 Proprietor / Governing Body

- Provides strategic oversight of safeguarding and online safety.
- Receives periodic assurance on online safety risks, incidents, filtering/monitoring effectiveness, training compliance and improvement actions.

6.2 Principal / Head of Centre

- Accountable for implementation of this policy, including resourcing of training, staffing and IT controls.
- Ensures staff understand reporting routes and that online safety is embedded within safeguarding culture and practice.

6.3 Designated Safeguarding Lead (DSL)

- Leads safeguarding, including online safety, and makes decisions on thresholds and referrals.
- Ensures online safety concerns are recorded, risk assessed and followed up, and that multi-agency working occurs where required.

6.4 Deputy Designated Safeguarding Lead (DDSL)

- Supports the DSL and provides safeguarding coverage for urgent online safety concerns.

6.5 Online Safety Lead (named postholder)

- **Online Safety Lead: Eman Ahamed, Principal**
- Coordinates day-to-day online safety practice, including learner education, staff briefings, incident triage (with DSL/IT), and the annual filtering/monitoring review.

6.6 IT Manager / Network Administrator

- Implements and maintains filtering and monitoring controls, device management controls and security configurations.
- Escalates safeguarding-relevant monitoring indicators to the DSL/Online Safety Lead promptly via secure routes.

6.7 All staff and contractors

- Follow Acceptable Use and Staff Code of Conduct.
- Report concerns immediately to DSL/DDSL (and Online Safety Lead for operational follow-up).
- Do not investigate safeguarding matters independently beyond preserving evidence and reporting.

6.8 Learners

- Follow Learner Acceptable Use Rules, Behaviour Policy and exam/assessment integrity expectations.
- Report harmful content, online bullying, threats, grooming, coercion, image-based abuse, or suspicious contact promptly.

---

7. Technology model at LMSC (devices and access)

LMSC operates a mixed model:

- **On-site learning:** Learners use **college-managed devices** on LMSC premises.
- **Hybrid learning:** Learners may use **BYOD** to access LMSC platforms under staff direction.
- **Online learning:** Learners use **their own devices** to access LMSC platforms and learning services.

All access to LMSC learning systems must be through approved platforms and authenticated accounts.

---

8. Risk areas addressed

LMSC's arrangements address (non-exhaustive):

- child sexual exploitation and online grooming;
- sharing nudes and semi-nudes (including coercion and image-based abuse);
- online bullying, harassment, hate incidents and discrimination;
- extremist and terrorist content and radicalisation risk (Prevent).
- self-harm and suicide-related content;
- harmful challenges, misinformation and manipulation;
- privacy breaches, doxxing, impersonation and account compromise;
- phishing, malware and cybercrime;
- misuse of AI tools and unauthorised assistance impacting academic integrity;
- staff professional boundaries and inappropriate contact.

---

9. Filtering and monitoring arrangements

9.1 Standards and governance

LMSC's filtering and monitoring arrangements are designed to meet DfE Filtering and Monitoring Standards and are reviewed **at least annually** and after significant change or serious incident.

The annual review is completed by: **Principal/Online Safety Lead**, **DSL**, and **IT Manager/Network Administrator**, with outcomes reported to governance.

9.2 Core systems used (Google tools)

LMSC uses **Google tools** to support learning, communication and administration, and to support security, filtering and monitoring controls (where features and configuration apply to LMSC-managed accounts and devices). Controls include, as applicable:

- managed accounts and access controls via administrative settings;

- safe browsing and web/content restrictions on managed devices and browsers;
- restrictions and permissions for apps/extensions and file sharing;
- audit logs and security reporting used to identify safeguarding and security concerns; and
- controls for communication tools used with learners.

9.3 College-managed devices (on-site)

For college-managed devices used on premises, LMSC will:

- apply centrally managed configuration and security settings;
- enforce filtering appropriate to learners and risk profile;
- restrict installation of unauthorised software/extensions;
- maintain appropriate logging/audit trails; and
- review alerts and trends as part of safeguarding oversight.

9.4 BYOD and off-site access (hybrid and online learning)

For BYOD/off-site access, LMSC recognises that full device-level control is not always possible. LMSC therefore applies layered controls:

- access is restricted to approved platforms and authenticated accounts;
- staff set clear expectations for safe conduct, recording rules and communications boundaries;
- safeguarding reporting routes are reinforced in every online programme and induction; and
- where a concern arises, LMSC will take proportionate action, which may include restricting account access, resetting credentials, or requiring supervised access.

9.5 Monitoring use and privacy

Monitoring information is used for **safeguarding and security** purposes, not routine performance management. Access to monitoring data is restricted to authorised staff on a need-to-know basis and handled in line with the Digital Privacy Policy.

---

10. Acceptable use and professional conduct

10.1 Staff expectations

Staff must:

- use only LMSC-approved platforms for teaching and learner communications;
- maintain professional boundaries (no personal social media "friending" or private messaging outside authorised platforms);
- ensure content shared is appropriate, lawful and aligned to curriculum;
- follow secure credential practice and never share passwords; and
- store/share learner data only through approved systems.

10.2 Learner expectations

Learners must:

- use LMSC systems responsibly for education;
- not bypass filtering or attempt unauthorised access;
- not record or distribute images/recordings of staff or learners without permission and a clear educational purpose;
- not share harmful content or harass/abuse others; and
- report concerns promptly.

10.3 Mobile phones and personal devices

Rules for phones/devices on site are enforced through the Behaviour Policy and Learner Acceptable Use Rules. Where safeguarding risk is suspected, evidence preservation procedures apply (Section 13).

---

11. Curriculum, learner education and awareness

LMSC educates learners about online safety through:

- induction and tutorial programmes;
- targeted sessions on risk themes (e.g., online relationships, coercion, sexting/image-based abuse, extremist content, self-harm content);

- embedding digital literacy and safe practice within STEM/Business learning; and
- reinforcement prior to assessments/exams (academic integrity, AI use rules, plagiarism and unauthorised assistance).

Curriculum planning draws on UKCIS "Education for a Connected World" themes (self-image, relationships, reputation, bullying, information literacy, wellbeing, privacy/security, copyright).

---

12. Remote and hybrid learning safeguards

For online/hybrid delivery, LMSC will:

- use approved video/learning platforms with appropriate moderation settings;
- control meeting access, screen sharing and chat functions as appropriate;
- set clear expectations for learner behaviour and respectful communication;
- apply clear rules about recording and sharing content; and
- provide clear routes for learners to report concerns during remote learning.

---

13. Reporting and incident response procedures

13.1 Immediate reporting routes

All online safety concerns must be reported **immediately** to the **DSL** or **DDSL**, including:

- grooming/exploitation or coercion concerns;
- threats of violence, hate crime, extremist content concerns;
- self-harm/suicide content suggesting immediate risk;
- sharing nudes/semi-nudes involving under 18s;
- serious harassment, stalking or blackmail.

13.2 Evidence preservation

Staff must:

- **not** forward or redistribute harmful images/content;
- preserve necessary evidence safely (e.g., screenshots of URLs/usernames) only to support safeguarding action;
- follow DSL instructions on secure storage of evidence.

Where nudes/semi-nudes are involved, staff must follow safeguarding procedures and avoid searching, storing or sharing images beyond what is strictly necessary for safeguarding action, as directed by DSL.

13.3 Triage, actions and referrals

The DSL/DDSL will:

- record the concern and risk assess;
- decide actions (support plan, parental contact, behaviour sanctions, restriction of account access, referral to external agencies, police, social care, or Prevent pathways where appropriate).
- ensure timely support for learners (pastoral support, counselling referral, safety plan and adjustments).

13.4 Allegations involving staff

Concerns about staff conduct online are handled under LMSC procedures for managing allegations, in line with safeguarding expectations and appropriate reporting routes.

---

14. Cyber security expectations

LMSC requires:

- strong passwords/passphrases and secure credential handling;
- multi-factor authentication where available for critical systems;
- prompt account removal or access change for leavers and role changes;
- patching and endpoint protection on managed devices;
- phishing awareness and prompt reporting of suspicious communications.

Cyber incidents are reported immediately via the IT incident route, and to DSL where safeguarding risk may be present (e.g., sextortion, compromised learner accounts, threatening communications).

---

15. Data protection and privacy

Online safety practice must be consistent with UK GDPR and the Data Protection Act 2018. Monitoring and logs are handled confidentially, lawfully and proportionately. LMSC's Digital Privacy Policy sets out data rights and contact details.

---

16. Working with parents/carers

Where appropriate and in the learner's best interests, LMSC will:

- share online safety guidance and expectations;
- communicate significant incidents and safety planning with parents/carers, unless doing so would increase risk or compromise safeguarding action; and
- provide routes for parents/carers to raise concerns.

---

17. Staff training and awareness

LMSC ensures:

- all staff receive safeguarding training including online safety at induction and at least annual updates.
- role-specific training is provided for DSL/DDSL, Online Safety Lead and IT staff, including incident handling and filtering/monitoring review responsibilities.

---

18. Monitoring, audit and review

- Online safety risk, incidents, training completion and the annual filtering/monitoring review outcomes are reported through SMT and to governance.
- This policy is reviewed annually, and sooner if required due to significant system changes, serious incidents, or national guidance updates.

---

19. Policy approval and review record

Version	Approved by	Approval date	Effective date	Review date	Summary of changes
1.2	Proprietor / Governing Body	18 Feb 2026	18 Feb 2026	18 Feb 2027	Expanded filtering/monitoring, remote learning safeguards, AI and incident procedures
1.3	Proprietor / Governing Body	18 Feb 2026	18 Feb 2026	18 Feb 2027	Named Online Safety Lead; specified Google tools and LMSC device model (managed devices/BYOD)

LONDON
MATHS & SCIENCE
COLLEGE

Contact

London Maths & Science College
167 Commercial Road,
London, E1 2DA
info@lmsc.org.uk
www.lmsc.org.uk