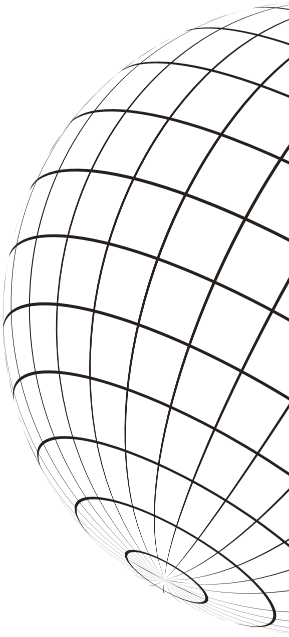
LONDON
MATHS & SCIENCE
COLLEGE

www.lmsc.org.uk

IT, Online Safety & Remote Learning Policy

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

IT, ONLINE SAFETY & REMOTE LEARNING POLICY



London Maths & Science College (LMSC)
Version: 1.0
Status: Approved
Publication Date: 31st October 2025
Next Review Due: 31st October 2026 (annual or following inspection/regulatory change)
Policy Owner: Head of Centre (HoC)
Operational Leads: IT Manager (Technical & Cyber Lead); Vice Principal/Academic (Remote Learning Lead)
Safeguarding Leads: DSL: Eman Ahamed • Deputy DSL: Anis Zaman
Data Protection Officer (DPO): [Name]

1. PURPOSE / RATIONALE

This policy sets out LMSC's arrangements for IT governance, online safety, cybersecurity, and remote/online learning, covering both our in-person and online-only delivery models. It ensures safe, effective use of technology for learners aged 16–19 and adults, and alignment with: - KCSIE 2025, Working Together 2025, Prevent Duty.
- UK GDPR/Data Protection Act 2018.
- Ofsted EIF (safeguarding, quality of education, leadership).
- NCSC cyber security principles for education and the DfE cyber standards (where applicable).
- JCQ GR/ICE/NEA; Pearson CQA & Pearson Online School expectations; Cambridge International regulations for online learning providers (where applicable).
- Equality Act 2010 and WCAG 2.2 AA accessibility expectations for digital content.

2. SCOPE

Applies to all users of LMSC IT systems and services: staff, students, governors/proprietor, contractors, volunteers and visitors. Covers college-owned devices, networks, cloud services, learning platforms, assessment systems, email, messaging, collaboration tools, websites, social media, and Bring Your Own Device (BYOD) used for LMSC purposes.

3. POLICY STATEMENT

LMSC will: 1. Provide secure, reliable and accessible IT systems that support high-quality teaching in-person and online.
2. Safeguard learners through education, filtering/monitoring, and proportionate supervision, with robust incident response.
3. Protect personal data and uphold privacy by design and default.
4. Promote digital citizenship, academic integrity and ethical use of AI.
5. Meet (and aim to exceed) the standards required for Cambridge International Online School and Pearson Online School accreditation, alongside JCQ and awarding-body requirements.
6. Continually assess risks and improve controls.

4. ROLES & RESPONSIBILITIES

Governing Body/Proprietor – Approves policy; receives termly assurance on cyber risk, filtering/monitoring, incidents, DPIAs and remote-learning quality.
Head of Centre (HoC) – Overall accountability; ensures resourcing, training and compliance; signs annual declarations to awarding bodies.
DSL / DDSL – Lead safeguarding online; maintain the Filtering & Monitoring Risk Assessment; oversee incidents, training, visitor/ speaker due diligence; ensure staff understand digital reporting routes.
IT Manager (Technical & Cyber Lead) – Owns network security, filtering/monitoring, identity/access management (IAM), device management (MDM), backups, logging, vulnerability/Patch management, and business continuity.
DPO – Ensures UK GDPR compliance, DPIAs, data processing contracts with suppliers, records of processing, breach handling.
VP/Academic (Remote Learning Lead) – Ensures quality of online pedagogy, curriculum alignment, accessibility, assessment integrity, attendance, and student engagement.
Exams Officer (EO) – Ensures assessment and exam integrity, including remote/online assessments per awarding rules.
SENCo/AAL – Advises on accessibility, assistive technology, Normal Way of Working (NWoW) and remote learning adjustments.
HoDs/Teachers/Tutors – Deliver safe, accessible, well-sequenced learning; enforce the Acceptable Use Policy (AUP); record attendance; escalate concerns.
Students & Parents/Carers (where applicable) – Follow AUP; maintain respectful, safe online conduct; report concerns promptly.

5. ONLINE SAFETY FRAMEWORK

5.1 Education & Culture
- Induction and annual refreshers for students & staff on online safety, digital citizenship, respectful communication, consent, image sharing, harassment/abuse, scams/phishing, mis/disinformation, AI ethics.
- Curriculum embeds online safety in PSHE/tutorials and subject contexts; visiting speakers follow due diligence.

5.2 Filtering & Monitoring
- Age-appropriate web filtering blocks illegal/harmful content (e.g., extremist, pornographic, self-harm, violence).
- Network and device monitoring identifies concerning patterns while minimising intrusion; alerts are triaged by DSL/IT per the Filtering & Monitoring RA (Appendix C).
- Controls apply on-site and, where feasible, to college devices off-site via MDM/secure DNS/agents.
- Exceptions are minimised, time-limited, documented and approved by IT Lead & DSL.

5.3 Reporting & Response
- One-click reporting in platforms and a dedicated email/portal for concerns.
- Safeguarding concerns → DSL immediately; crimes/illegal content → Police/CEOP as appropriate.
- All incidents recorded on the safeguarding/IT incident system with clear hand-offs.

6. REMOTE/ONLINE LEARNING STANDARDS

- 6.1 Platforms & Tools
- - Approved platforms listed in Appendix A with purposes, data categories, legal bases and retention.
- - Single sign-on (SSO) and multi-factor authentication (MFA) used where available.
- - Only approved meeting tools (waiting rooms, lobby, authenticated users, screen-share controls, recording permissions).

- 6.2 Live Lessons & Recordings
- - Staff use college accounts only; professional backgrounds; appropriate dress/conduct.
- - Cameras optional for learners unless pedagogically justified; no recording by learners; staff recordings only where educationally necessary and communicated in advance; storage/retention per policy.
- - Attendance captured; engagement monitored; safeguarding prompts at start (e.g., how to report concerns).
- - Two-adult presence recommended for sensitive sessions where practicable (or post-session review/access to recording by line manager/DSL).
- 6.3 Accessibility & Inclusion
- - Content meets WCAG 2.2 AA where practicable: captions/transcripts, alt text, structured headings, sufficient contrast.
- - Assistive technology supported (screen readers, TTS, dictation); materials provided in accessible formats; flexible deadlines for connectivity/health issues.
- - Reasonable adjustments documented; online proctoring alternatives considered with awarding body if an adjustment is required.
- 6.4 Behaviour & Classroom Management Online
- - Expectations mirror the Behaviour Policy; chat and mic use moderated; inappropriate content triggers removal/reporting.
- - Staff can remove/lock participants, mute all, and end sessions; sanctions follow staged responses.

7. ASSESSMENT & ACADEMIC INTEGRITY (ON-SITE & ONLINE)

- JCQ/awarding-body rules apply to all assessments.
- For online assessment, integrity controls may include: timed windows, question pools, lockdown browsers, controlled resources, identity checks, proctoring where approved/appropriate, and viva voce/process evidence.
- Generative AI use: permitted for ungraded practice with declaration; prohibited in assessed work unless specification allows. Teachers verify authenticity via drafts, logs, version history, and/or orals.
- Malpractice managed under the Malpractice & Maladministration Policy.

8. ACCEPTABLE USE (AUP) – SUMMARY

- Full AUPs in Appendix B (Students) and Appendix D (Staff/Adults). Headline expectations: - Use systems for lawful, educational purposes; respect others; no bullying, harassment, hate speech, or sharing of illegal/explicit content.
- - Protect accounts: unique passwords, MFA, do not share credentials.
- - No unauthorised recording, distribution of images, or posting of confidential material.
- - No bypassing of filters, use of VPNs, proxy or hacking tools.
- - Adhere to software licensing and copyright; cite sources; keep data secure.

- Report concerns, phishing or suspected compromise immediately.

9. CYBERSECURITY & IT OPERATIONS

- 9.1 Identity & Access Management (IAM)
- - Role-based access; least privilege; joiners-movers-leavers process within 24 hours; admin accounts segregated with MFA.
- 9.2 Device & Patch Management
- - College devices enrolled in MDM with encryption, screen-lock, firewall, antivirus/EDR, and forced updates.
- - BYOD permitted only via managed profiles or secure browser; minimum OS/security baseline applies (Appendix E).
- 9.3 Network & Cloud Security
- - Segmented networks (admin/exams/guest); secure DNS; WPA2/3 Enterprise; logging and alerting; vulnerability scans and remedial patching within defined SLAs.
- - Cloud suppliers under contract with DPAs and UK GDPR-compliant hosting/ safeguards; high-risk tools require DPIA before use.
- 9.4 Backups & Continuity
- - Daily encrypted backups for critical systems; tested restores; RPO/RTO targets defined; offline/immutable backup for ransomware resilience.
- - Business continuity integrates with Exams Contingency Plan; failover procedures documented.
- 9.5 Email & Collaboration Security
- - Anti-malware, anti-phishing, SPF/DKIM/DMARC, safe-links.
- - External sharing controlled; auto-forwarding to external domains disabled by default.
- 9.6 Logging, Monitoring & Incident Response

- - Security logs retained; suspicious activity triaged; incidents handled via Cyber Incident Response Plan (Appendix F) with roles (IT, DSL, DPO, Comms).
- - Reportable personal data breaches notified to the DPO; ICO notified within statutory timescales where required.

11. DATA PROTECTION & PRIVACY BY DESIGN

- DPIAs required for new/changed high-risk processing (e.g., proctoring, biometrics, location tracking).
-
- Data retention schedules applied; secure disposal of devices/media; data subject rights routes publicised.
-
- Third-party processors/contracts reviewed annually; cross-border transfers assessed and safeguarded.

12. PREVENT, SAFEGUARDING & EXTERNAL SPEAKERS ONLINE

- Prevent risk assessment includes online radicalisation risk; staff trained to recognise indicators.
- External speakers (webinars/virtual events) vetted; expectations agreed; sessions supervised; content reviewed.
- Platform moderation tools used; concerning content escalated immediately to DSL.

13. QUALITY ASSURANCE FOR ONLINE PROVISION

- Online teaching observed and quality-assured against the TLA Policy; accessibility spot-checks; learner voice gathered each term.
- Service levels: uptime targets, helpdesk response, and escalation paths published (Appendix G).
- Benchmarking against Cambridge International Online School and Pearson Online School standards; gap analyses and action plans maintained.

14. TRAINING & AWARENESS

- Annual mandatory modules: online safety, Prevent, data protection, cyber hygiene, assessment integrity, AI guidance, accessibility & assistive tech.
- New staff induction includes platform security, AUPs, and incident response; students receive onboarding modules.

15. MONITORING, AUDIT & REVIEW

- Termly audits of filtering/monitoring effectiveness, access controls, and incident logs; penetration testing proportionate to risk.
-
- KPIs: incident rates, time-to-patch, phishing test pass rates, uptime, safeguarding alerts handled within SLA, accessibility compliance rate.
-
- Policy reviewed annually or following serious incident/technology or legal change; governance receives a summary report.

16. ASSOCIATED DOCUMENTS & REFERENCES

- LMSC: Safeguarding & Child Protection; Prevent Duty; Behaviour & Discipline; Anti-Bullying; Data Protection & Privacy Notices; Exams Policy; NEA/Controlled Assessment; Malpractice & Maladministration; Access Arrangements & Reasonable Adjustments; Word Processor & Assistive Technology; Risk Assessment; Health & Safety; Business Continuity/Exams Contingency; Staff Code of Conduct.
- External: KCSIE 2025; Working Together 2025; UK GDPR/DPA 2018; Ofsted EIF; NCSC guidance for schools/colleges; JCQ GR/ICE/NEA; Pearson Online School & Cambridge International online provider expectations; Equality Act 2010; WCAG 2.2.

17. APPROVAL & REVIEW RECORD

Version	Date Approved	Approved By (Signature)	Role	Next Review
1	[DD/MM/YYYY]		Head of Centre	[DD/MM/YYYY]

PPENDICES (OPERATIONAL)

APPENDIX A – APPROVED PLATFORMS & TOOLS REGISTER (POPULATE)

Tool/Platform	Purpose	Data types	Legal basis	Storage/ Region	DPIA (Y/N)	DPO notes	Owner	Review due

APPENDIX B – STUDENT ACCEPTABLE USE AGREEMENT (AUP)

Using LMSC devices, accounts and networks
- I will protect my account, use MFA, and never share passwords or let others use my login.
- I will be respectful online, follow staff instructions, and report concerns.
- I will not view, create, upload or share illegal or harmful content; I will not bully or harass anyone.
- I will not try to bypass filters or use VPNs/proxies; I will not install unauthorised software.
- I will keep my personal information private and follow data protection guidance.
- I understand live lessons may be recorded for educational/safeguarding reasons and stored securely.
- I will submit my own work and declare any AI support when allowed; I will not use AI or the internet in a way that breaks assessment rules.
- I understand breaches may lead to sanctions under the Behaviour Policy and restrictions to my account.

Signature/Date

APPENDIX C – FILTERING & MONITORING RISK ASSESSMENT (HEADLINES)

Technical controls in place; categories blocked; exception process; monitoring sensitivity; alert triage; roles/responsibilities (IT/DSL); data retention; DPIA reference; testing schedule; user education.

APPENDIX D – ONLINE LESSON PROTOCOL (STAFF)

Pre-lesson checks; safeguarding reminder; waiting room; disable attendee recording; behaviour norms; camera/mic guidance; how to remove a participant; signposting to help; post-lesson storage of recording (if used), naming convention and retention.

APPENDIX E – BYOD & MINIMUM SECURITY BASELINE

- Supported OS versions; encryption on; passcode/biometric lock; auto-lock ≤ 5 minutes; device not jailbroken/rooted; managed profile where available; approved AV; no local storage of personal data; use only approved apps/browsers; report loss/theft immediately.
- LMSC reserves the right to block/remote-wipe college data on lost BYOD via managed profile.

APPENDIX F – CYBER INCIDENT RESPONSE PLAN (SUMMARY)

- Detect (alerts, reports) → Contain (isolate device/account) → Eradicate (remove malware/reset creds) → Recover (restore from backup) → Notify (DPO/ICO/users/regulators as required) → Review (lessons learned).
- Roles: IT Lead (technical), DSL (safeguarding impacts), DPO (data breach), Comms (stakeholders), HoC (strategic).
- Ransomware playbook highlights; contact list; decision logs.

APPENDIX G – SERVICE LEVELS & SUPPORT

Service	Target	Notes
Helpdesk first response	1 working day	Urgent safeguarding tagged for immediate escalation
Critical incident response	1 hour	24/7 on-call for safeguarding/critical outages (by rota)
Core learning platform uptime	99.5% term time	Excludes planned maintenance

APPENDIX H – RECORDING, PHOTOGRAPHY & MEDIA GUIDANCE

Lawful basis; consent management; storage; access; sharing; takedown requests; prohibition on learner recording others without permission; watermarking and distribution controls where feasible.

APPENDIX I – REMOTE ASSESSMENT INTEGRITY CONTROLS (MENU)

- Identity checks; environmental scan; lockdown browser; device check; live/proctored or record-and-review options; split-screen question banks; time windows; randomisation; academic honesty statement; viva voce follow-up.
- Align chosen controls with awarding-body permissions.

APPENDIX J – DIGITAL ACCESSIBILITY CHECKLIST (STAFF)

Headings/structure • Alt text • Colour contrast • Captions/transcripts • Link text meaningful • Reading order • Keyboard navigation • Large print alternatives • AT compatibility test • Accessible file formats.

APPENDIX K – EXTERNAL SPEAKERS & EVENTS (ONLINE) CHECKLIST

Due diligence (content, affiliation) • Agreement to code of conduct • Supervisor present • Recording/monitoring arrangements • Reporting route • Post-event review.

Printed copies are uncontrolled. The IT Manager and DSL maintain the master version; the DPO maintains the platform register and DPIAs. This policy supports our readiness for Cambridge International and Pearson Online School accreditation

LONDON
MATHS & SCIENCE
COLLEGE

Contact

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