LONDON MATHS & SCIENCE COLLEGE

www.lmsc.org.uk

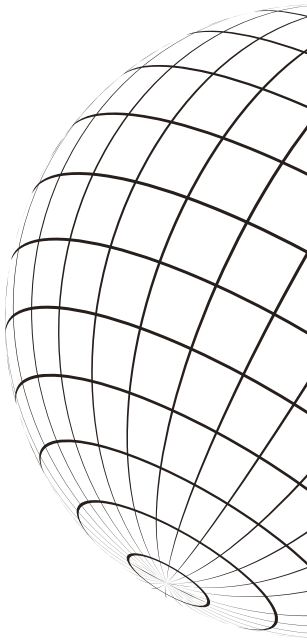
Digital Privacy Policy

London Maths & Science College

167 Commercial Road, London, E1 2DA

info@lmsc.org.uk

DIGITAL PRIVACY POLICY



Legal entity: London Maths & Science College (LMSC) – Limited Company (Companies House No. 16822143)
Registered office / campus: 167 Commercial Road, London, E1 2DA
Privacy contact: support@lmsc.org.uk
Data Protection Lead (Senior Responsible Lead): Eman Ahamed, Principal (LMSC does not designate a statutory Data Protection Officer unless required by processing activities; the Principal acts as the senior lead for data protection compliance.)
Document Owner: Principal / Head of Centre
Approved by: Proprietor / Governing Body
Effective date: 18 February 2026
Review date: 18 February 2027
Version: 1.2

Table of Contents

1. Purpose

London Maths & Science College (LMSC) is committed to protecting personal data and respecting privacy when using digital systems for teaching, learning, assessment, examinations, safeguarding, operations and communications.

This policy sets out how LMSC:

- collects, uses, shares and protects personal data in digital contexts;
- complies with UK data protection and e-privacy law;
- manages privacy risks in online/hybrid learning and education technology; and
- enables individuals to exercise their information rights.

This policy supports LMSC's wider obligations for safeguarding, examination integrity and awarding organisation compliance, including Cambridge International.

---

2. Scope

This policy applies to:

- learners (including applicants, current learners and leavers);
- parents/carers (where relevant);
- staff, contractors, volunteers and governors/proprietors;
- visitors; and
- all digital systems and services used or provided by LMSC, including the website, MIS, VLE/LMS, email, messaging, video conferencing, online assessment tools, cloud storage, access control systems and CCTV (where applicable).

It applies to processing on-site and off-site (including home working and online/hybrid learning).

---

3. Legal and regulatory framework

LMSC processes personal data in accordance with:

- **UK GDPR** and the **Data Protection Act 2018**.
- ICO guidance on transparency and providing privacy information ("right to be informed").
- **PECR** requirements for cookies and similar technologies and certain electronic communications.
- ICO guidance on CCTV and video surveillance.
- ICO guidance on individual rights.

---

4. Data protection principles

LMSC applies the UK GDPR principles:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

---

5. Roles and responsibilities

5.1 Proprietor / Governing Body

- Provides oversight of data protection governance, risk and resourcing.
- Receives periodic assurance reporting on compliance, incidents and improvement actions.

5.2 Principal / Head of Centre (Data Protection Lead: Eman Ahamed)

- Holds overall accountability for data protection compliance and effective implementation of this policy.
- Ensures privacy risk is considered in strategic planning, procurement and digital delivery decisions.
- Ensures that data breaches and high-risk processing issues are escalated appropriately.

5.3 Bursar / Director of Finance & Operations

- Oversees operational security arrangements, supplier assurance, procurement controls and cyber security governance.
- Ensures secure retention/disposal arrangements are in place for digital assets and records.

5.4 HR & Compliance Officer

- Maintains staff training compliance records and supports policy management, audit readiness and retention processes.
- Supports staff data handling in recruitment, employment and leaver processes.

5.5 IT Manager / Network Administrator

- Implements technical controls (access management, patching, backups, endpoint security, logging/monitoring, secure configuration).
- Ensures account provisioning/de-provisioning and access reviews are completed and evidenced.

5.6 Exams Officer / Cambridge Exams Coordinator

- Ensures candidate data is handled securely for exam entries, access arrangements, results and post-results services.
- Ensures exam systems access is controlled and audit trails are maintained.

5.7 All staff, contractors and volunteers

- Must follow LMSC policies and instructions, complete required training, protect credentials, and only access/process personal data necessary for their role.
- Must report suspected data incidents immediately via LMSC incident reporting arrangements.

---

6. What personal data LMSC processes in digital systems

6.1 Learners and applicants

- identity and contact details; admissions and enrolment records;
- attendance, timetable and progress data;
- academic work, assessment and feedback records;
- examination entries and results; access arrangements information;
- pastoral and safeguarding information (subject to enhanced controls);
- finance/payment records where applicable;
- digital activity data in LMSC systems (e.g., login records, access logs, device/security logs).

6.2 Parents/carers (where relevant)

- contact details, communications, meeting records and (where applicable) consent preferences.

6.3 Staff/contractors

- recruitment and HR data (including qualification evidence, references, training records, DBS evidence/status information where applicable);
- payroll-related data;
- system access and audit logs.

6.4 Website and online services

- cookie and similar technology data and website analytics, subject to PECR requirements and cookie preference settings.

6.5 Special category data

LMSC may process special category data (e.g., health/SEND information, ethnicity, safeguarding-related information) under an appropriate lawful basis and an additional condition under the Data Protection Act 2018, with heightened safeguards (strict access controls, need-to-know handling, and secure record keeping).

---

7. Lawful bases for processing

LMSC uses one or more lawful bases under UK GDPR, commonly:

- **legal obligation** (e.g., safeguarding, examination administration, employment obligations);

- **contract** (e.g., learner agreements, employment contracts, contracted services);
- **legitimate interests** (e.g., security monitoring, service improvement), supported by a documented balancing assessment where appropriate;
- **consent** where required (e.g., certain communications and non-essential cookies).

Where special category data is processed, LMSC identifies and records the additional condition relied upon and applies enhanced protections.

---

8. Digital privacy in teaching, learning and online/hybrid delivery

LMSC will:

- use digital platforms that have been assessed for privacy and security (including supplier due diligence and appropriate contracts);
- configure platforms with privacy-friendly settings by default;
- ensure staff use approved communication channels and do not use unauthorised personal accounts for learner communications;
- manage lesson recording with clear purpose, access controls and retention rules (recordings are not made routinely unless required for an identified educational purpose);
- provide learners with clear expectations on acceptable use, digital conduct and academic integrity (including the ethical use of technology and AI).

Where a platform or activity is likely to create a higher privacy risk (e.g., extensive monitoring, use of biometrics, large-scale special category data, or new technologies), LMSC will complete a documented privacy risk assessment/DPIA before implementation.

---

9. Examination and awarding organisation data (including Cambridge)

LMSC processes candidate data to administer qualifications and examinations, including entries, access arrangements, results, post-results services and certification.

Personal data may be shared securely with awarding organisations and exam service providers where required for:

- registration and candidate identification;
- assessment delivery, moderation and results issuance;
- post-results services and appeals; and
- malpractice/maladministration investigations where required by awarding organisation regulations.

Only necessary data is shared, and access to exam systems and candidate data is restricted to authorised staff.

---

10. Cookies, website analytics and electronic communications

10.1 Cookies and similar technologies

LMSC provides clear cookie information and operates cookie preferences in line with PECR requirements, including obtaining consent where required for non-essential cookies and similar technologies.

10.2 Electronic communications

LMSC follows PECR rules for certain electronic marketing and ensures users can manage preferences and opt out where required.

---

11. Data sharing and third-party processors

LMSC may share personal data with:

- awarding organisations and exam-related services used by LMSC;
- safeguarding partners and statutory agencies when necessary;
- IT and cloud suppliers acting as data processors;
- professional advisers (e.g., auditors, legal advisers) where necessary.

Where suppliers process data on LMSC's behalf, LMSC ensures:

- appropriate contracts and data processing terms are in place;
- security measures and access controls are sufficient and proportionate;
- processing is limited to documented instructions; and
- supplier performance and compliance are monitored.

---

12. International data transfers

Where a supplier transfers data outside the UK, LMSC will ensure appropriate safeguards are in place (e.g., UK adequacy regulations or contractual safeguards and associated risk assessment) and will document the arrangements.

---

13. Information security and access control

LMSC applies technical and organisational measures appropriate to risk, including:

- role-based access control and least-privilege access;
- strong authentication and credential management;
- encryption where appropriate;
- patching, endpoint protection, malware protection and backups;
- secure configuration of cloud services;
- monitoring/logging and incident response arrangements;

- secure disposal of devices/media; and
- staff training and confidentiality expectations.

Safeguarding and other high-risk datasets are protected by enhanced access restrictions and stricter handling rules.

---

14. CCTV and video surveillance

LMSC operates **CCTV** to support site security, the safety of learners, staff and visitors, and the prevention/detection of crime and serious incidents.

LMSC will ensure CCTV is used in line with ICO expectations, including:

- clear signage to inform individuals that CCTV is in operation and the purpose for use;
- appropriate camera positioning to avoid excessive intrusion;
- restricted access to footage to authorised staff only;
- secure storage of footage and controlled sharing (e.g., with police or insurers where lawful and necessary);
- retention for no longer than necessary, in line with LMSC's retention schedule; and
- documented review of CCTV necessity and proportionality, and completion of a DPIA where required.

(Audio recording is not used unless formally authorised and separately assessed; any change would require governance approval, privacy assessment and updated signage/notice.)

---

15. Data retention and disposal

LMSC retains personal data only for as long as necessary for the purposes for which it is processed, and in line with:

- statutory and legal requirements;
- safeguarding record-keeping expectations;
- awarding organisation rules and audit requirements; and
- LMSC's Records Management and Retention Schedule.

When retention periods expire, LMSC securely deletes, anonymises or destroys data using approved methods.

---

16. Individuals' rights

LMSC supports individuals to exercise their rights under the UK GDPR, including:

- the right to be informed;
- access (subject access requests);
- rectification;
- erasure (where applicable);
- restriction of processing;
- data portability (where applicable);
- objection; and
- rights related to automated decision-making and profiling (where applicable).

LMSC will verify identity before releasing personal data and respond within statutory timescales. Where exemptions apply, LMSC will explain the basis in writing.

---

17. Data breaches and incident reporting

All staff must report suspected or actual data incidents immediately via LMSC's incident reporting route.

LMSC will:

- contain, assess and investigate incidents promptly;
- determine whether the incident meets the threshold for reporting to the ICO and/or notifying affected individuals;
- maintain a breach log and record remedial actions; and
- implement lessons learned to prevent recurrence.

---

18. Complaints

Individuals may raise privacy concerns with LMSC using the contact details in Section 19.

Individuals may also complain to the Information Commissioner's Office (ICO) if dissatisfied with LMSC's response.

---

19. Contact details

London Maths & Science College (LMSC)

167 Commercial Road, London, E1 2DA

Email: support@lmsc.org.uk (Privacy / Data Protection)

Data Protection Lead: Eman Ahamed, Principal

Requests should clearly state: "Data Protection Request" or "Privacy Complaint" and include sufficient information for LMSC to verify identity and locate relevant records.

---

20. Monitoring, training and review

- All staff receive data protection and information security awareness training at induction and through annual updates.
- Compliance is monitored through audits, access reviews, incident reviews and supplier assurance checks.
- This policy is reviewed annually, or sooner following significant change to systems, risks or legal requirements.

---

21. Related LMSC policies and documents

- Data Protection Policy / Data Handling Procedure

- Information Security Policy
- Acceptable Use Policy (Staff and Learners)
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Exams Policy (including Cambridge and JCQ compliance)
- Records Management and Retention Schedule
- Incident/Breach Reporting Procedure
- CCTV Policy and CCTV Signage/Information Notice
- Remote/Hybrid Learning Policy and platform guidance

Approval and Review Record

Version	Approved by	Approval date	Effective date	Review date	Summary of changes
1.0	Proprietor / Governing Body	18 Feb 2026	18 Feb 2026	18 Feb 2027	Initial issue
1.1	Proprietor / Governing Body	18 Feb 2026	18 Feb 2026	18 Feb 2027	Expanded digital scope, PECR and children's privacy provisions
1.2	Proprietor / Governing Body	18 Feb 2026	18 Feb 2026	18 Feb 2027	Added full contact details, named Data Protection Lead, CCTV provisions

---

LONDON
MATHS & SCIENCE
COLLEGE

Contact

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