LONDON MATHS & SCIENCE COLLEGE

Cyber Security Policy (Examinations)

Protecting examination systems, confidential assessment material and candidate data

Document reference	LMSC/CYB/01
Title	**Cyber Security Policy (Examinations)**
Version	1.0
Status	New. Based on the JCQ sample centre cyber security policy template and adapted to LMSC's systems. Appendix A is the IT and Cyber Incident Response Procedure cross-referenced by the Examination Policy.
Effective date	[insert date of approval]
Review date	30 September 2027, and on each 1 September thereafter
Policy owner	Principal / Head of Centre
Operational leads	IT Lead (technical controls) · Examinations Officer (awarding organisation systems)
Approved by	Proprietor
Applies to	All staff, invigilators, contractors and any authorised user with access to LMSC systems, awarding organisation systems, candidate data or confidential assessment material

Table of Contents

No table of contents entries found.

1. Purpose

1.1 This policy sets out how London Maths & Science College protects the systems, confidential assessment material and candidate data connected with the delivery and administration of examinations, and what happens when something goes wrong.

1.2 It exists because the largest single risk to examination security at a small centre is no longer physical. A question paper taken from a cabinet is one paper; a compromised awarding organisation account can expose an entire series.

2. Scope

2.1 This policy applies to every person with access to LMSC systems, awarding organisation systems, candidate data or confidential assessment material — staff, senior leaders, invigilators, assessors, contractors and any other authorised user.

2.2 It applies to devices owned by LMSC and to any personal device used to access those systems.

2.3 It sits alongside the centre's Data Protection and Confidentiality Policy, which governs personal data generally. Where an incident engages both, both apply.

3. Regulatory context

3.1 This policy is written to comply with the JCQ General Regulations for Approved Centres and the JCQ cyber security guidance for centres, revised August 2025, and follows the structure of the JCQ sample centre cyber security policy template. It also gives effect to the UK GDPR and the Data Protection Act 2018.

3.2 JCQ's guidance requires that staff who access awarding organisation systems complete cyber security training **each year**. Section 7 gives effect to that requirement.

3.3 The operative versions are those current for the academic year. From 1 September 2026 the Examinations Officer re-checks this policy against the 2026/27 documents and the current JCQ cyber security guidance, and records the date of that check.

3.4 Technical measures follow National Cyber Security Centre guidance, which is advisory rather than mandatory, and is identified as such where relied on.

4. Roles and responsibilities

Role	Post-holder	Responsibility
Principal / Head of Centre	Eman Ahamed	Owns this policy. Decides on escalation, and personally notifies the awarding organisation where confidential assessment material may be compromised. Accountable for the annual training requirement being met.
IT Lead / Network Administrator	Ahsanul Farhan	Technical controls, patching, backups, monitoring, account provisioning and removal. First technical responder in an incident. Preserves logs and device images at the direction of the Investigation Manager.
Examinations Officer	Anis Zaman	Awarding organisation system accounts: who holds them, that multi-factor authentication is enabled, and that access is removed when a person changes role or leaves. Maintains the System Access Register at Appendix B.
Data Protection Officer	Eman Ahamed	Assesses whether an incident is a reportable personal data breach and, if so, notifies the ICO. Independence of this role is under review — see LMSC/ERR/01 note 3.
All users	—	Complete annual cyber security training. Report anything suspicious the same day. Do not share credentials.

4.1 Where an incident involves the Head of Centre, or the Head of Centre is unavailable, reports go to the Proprietor. Where it involves the IT Lead, the Head of Centre appoints an alternative technical responder.

5. Systems in scope

5.1 The systems below are in scope. The Examinations Officer maintains the System Access Register at Appendix B, recording who holds an account on each, whether multi-factor authentication is enabled, and when access was granted and removed.

System	Holds	Controls that apply
AQA secure extranet and Centre Services	Entries, results, secure downloads, access arrangements online	Named individual accounts only. Multi-factor authentication mandatory. Listed on the Appendix B register. Access removed on the day a person leaves.
Management information system	Candidate records, entries, seating plans, registers	Role-based access; administrator accounts named on the register.
Centre email	Candidate data, correspondence with AQA	Multi-factor authentication. Candidate data sent only to verified addresses. Financial and identity documents never sent unencrypted.
File storage and backup	Access arrangement evidence, NEA work, examination records	Access restricted by role. Encrypted at rest. Backups tested at least annually and the test recorded.
Website policy store	Published policies	Publishing restricted to named users. Withdrawn documents removed and the removal dated — see LMSC/STP/01.
Messaging used operationally	Session communications	WhatsApp is named in the contingency procedure. It is not a record of record and must not carry candidate data or assessment content — see clause 6.6.

6. Controls

6.1 Access and accounts

- Accounts are individual and named. Shared or generic accounts are not used for any system holding candidate data or confidential assessment material.
- Credentials are never shared, including between key holders and between the Head of Centre and the Examinations Officer.
- Multi-factor authentication is enabled on every awarding organisation system and on centre email, without exception.
- Passwords follow National Cyber Security Centre guidance — three random words, unique to each system, and never reused from a personal account.
- Access is granted on the basis of role and removed on the day a person changes role or leaves. Removal is recorded on the Appendix B register.
- Administrator accounts are held by the smallest number of people that makes the centre workable, and are reviewed at the start of each academic year.

6.2 Technical measures

- Supported operating systems and software only; security updates applied promptly.
- Anti-malware protection on every device with access to examination systems.
- Firewall at the network boundary, configured and reviewed by the IT Lead.
- Devices encrypted at rest and locked when unattended.
- Backups taken regularly, held separately, and restore-tested at least once each academic year with the test recorded.

6.3 Confidential assessment material held electronically

6.3.1 Secure download and print is the highest-risk activity the centre undertakes electronically. **Material is downloaded only by a named key holder, only on a centre device, and only in the secure room.**

6.3.2 Printed material passes immediately into the secure storage facility and is logged in the same way as material delivered physically — see LMSC/SSK/01 and LMSC/LOG/01.

6.3.3 Downloaded files are deleted from the device and the recycle bin once printed, and the deletion is recorded.

6.3.4 Confidential assessment material is never emailed, never placed in general file storage, never held on a personal device, and never printed on a shared or networked printer outside the secure room.

6.4 Candidate data

- Candidate data is shared only with those who need it, and only through systems in scope.
- Access arrangement evidence, which includes health information, is held with access restricted to the SENCo, the Examinations Officer and the Head of Centre.
- Identity documents are not copied or retained — see the Candidate Identity Verification Procedure.

6.5 Artificial intelligence

6.5.1 Confidential assessment material, live question paper content, candidate personal data and candidate work must not be entered into any publicly available artificial intelligence tool. This mirrors LMSC/MMP/02 clause 14.3.

6.6 Messaging

6.6.1 WhatsApp is named in the centre's contingency procedure as an emergency communication channel. It may be used to raise the alarm quickly. **It must not carry candidate data, assessment content or images of either, and it is not the record of record** — decisions communicated by messaging are written up on the relevant log the same day.

7. Training and awareness

7.1 Every person with access to an awarding organisation system completes cyber security training **each academic year**, before that access is used for a live series. This is a JCQ requirement, not a centre preference.

7.2 All other users with access to candidate data complete the same training annually.

7.3 Training is recorded on LMSC/TRN/01 Appendix A, with the individual declaration at Appendix B and the cumulative record at Appendix C. The scheduled session sits in the training calendar for the week commencing 22 March 2027, and for any new user before their access is enabled.

7.4 Training covers phishing and social engineering, credential handling, safe use of removable media, secure download and print, recognising an incident, and how to report one.

7.5 A person who has not completed the current year's training does not access awarding organisation systems. The Examinations Officer checks the training record against the access register before each series.

8. Incident reporting and response

8.1 Anything unexpected is an incident until it is shown not to be. A suspicious email, a device behaving oddly, an unexpected password reset, a file that cannot be opened, an account locked without explanation — all are reported. **The centre would far rather investigate ten false alarms than miss one real incident.**

8.2 The route below is the IT and Cyber Incident Response Procedure referred to in the Examination Policy. The full procedure, contacts and record form are at Appendix A.

Step	Action	Who	Timing and detail
1	**Report**	Anyone	Report to the IT Lead and the Head of Centre. Same day, in every case, however minor it appears. Do not investigate it yourself and do not attempt to fix it.
2	**Contain**	IT Lead	Isolate the device from the network, disable the affected account, force a credential reset. Do not wipe or reimage anything — evidence is preserved.
3	**Assess**	Head of Centre with IT Lead and EO	Three questions: could confidential assessment material be compromised? Could candidate personal data be compromised? Could awarding organisation system access be compromised? Any yes triggers step 4.
4a	**Notify the awarding organisation**	Head of Centre	Where confidential assessment material may be compromised, or awarding organisation system access may be compromised: notify without delay, before the internal investigation is complete. This is not held over pending certainty.

Step	Action	Who	Timing and detail
4b	**Assess data breach**	Data Protection Officer	Where personal data may be compromised, assess whether it is reportable. A reportable breach is notified to the Information Commissioner's Office within 72 hours of the centre becoming aware of it.
4c	**Report externally**	IT Lead	Where a criminal act is suspected, report to Action Fraud and, for a significant incident, to the National Cyber Security Centre.
5	**Record**	IT Lead	Open a Cyber Incident Record at Appendix A. Every action, decision and notification is entered with the time it happened.
6	**Investigate**	Per LMSC/MMP/02 clause 7.4	Where malpractice or maladministration is suspected, the Investigation Manager is appointed under the routing table in the Malpractice Policy — not by default by the person whose systems are involved.
7	**Review**	Head of Centre	Within ten working days of resolution: what allowed it, what changes, and who is told. Recorded and retained.

8.3 The obligation at step 4a is absolute. Where the security of confidential assessment material may have been compromised, the awarding organisation is informed **without delay** — before the centre knows the full extent, before the cause is established, and whether or not the centre believes the risk has been contained. Waiting for certainty is itself the failure.

8.4 No person deletes, wipes, reimages or 'tidies up' anything connected with an incident. Evidence is preserved for the Investigation Manager appointed under LMSC/MMP/02.

9. Compliance, audit and review

9.1 The Examinations Officer reviews the System Access Register at the start of each academic year and before each examination series, and confirms that every account listed is still required and that multi-factor authentication remains enabled.

9.2 The IT Lead confirms annually that backups have been restore-tested, that devices are patched and encrypted, and that the firewall configuration has been reviewed.

9.3 The Head of Centre reviews this policy annually in September, following publication of the JCQ documents, and the Proprietor approves it. It is also reviewed after any incident.

9.4 Records made under this policy are retained in accordance with the Record Retention Policy and produced to an inspector on request.

10. Associated documents

Examination Policy · Exam Security Policy · LMSC/SSK/01 · LMSC/LOG/01 · LMSC/MMP/02 · LMSC/COI/01 · LMSC/TRN/01 · LMSC/STP/01 · Candidate Identity Verification Procedure · Exam Contingency and Emergency Evacuation Procedure · Data Protection and Confidentiality Policy · Record Retention Policy

APPENDIX A

IT and Cyber Incident Response Procedure

This appendix is the procedure cross-referenced by the Examination Policy. It is kept with the examinations records and a copy is held off-system, so that it can be read when the systems it concerns are unavailable.

Contacts

Contact	Who	Details
Head of Centre	Eman Ahamed	[insert direct number]
IT Lead	Ahsanul Farhan	[insert direct number]
Examinations Officer	Anis Zaman	[insert direct number]
Proprietor	[insert name]	[insert direct number]
AQA — centre support	Awarding organisation	[insert number and email from AQA centre services]
Information Commissioner's Office	Personal data breach	Report within 72 hours of becoming aware, where reportable
Action Fraud / NCSC	Criminal act or significant incident	[insert reference numbers once obtained]

The seven steps

Report — Contain — Assess — Escalate — Record — Investigate — Review. The table at clause 8.2 sets out who does each and when. Two rules override everything else: report the same day, and notify the awarding organisation without delay where confidential assessment material may be affected.

> **If an incident occurs during an examination series, the Head of Centre decides whether any affected session can proceed. That decision is taken with the awarding organisation, not ahead of it, and is recorded on the Incident Log at LMSC/LOG/01.**

Cyber Incident Record

Incident reference	
Date and time discovered	
Discovered by	
Date and time reported to IT Lead and Head of Centre	
What happened	
Systems and accounts affected	
Confidential assessment material at risk? (Yes / No)	
Candidate personal data at risk? (Yes / No)	
Awarding organisation system access at risk? (Yes / No)	
Containment actions and times	
Awarding organisation notified — date, time, by whom, response	
ICO notified — date, time, reference	
Action Fraud / NCSC — date, reference	
Investigation Manager appointed under MMP/02 cl.7.4	
Outcome	

Post-incident review — date, changes made	

Completed by: _____ Role: _____ Date: _____

Reviewed by Head of Centre: _____ Date: _____

APPENDIX B

System Access Register

Maintained by the Examinations Officer. Reviewed at the start of each academic year and before each examination series. Access is removed on the day a person changes role or leaves, and the removal is dated here.

Name	Role	System	MFA enabled	Access granted	Access removed

Reviewed — every account listed is still required, and multi-factor authentication is enabled on every awarding organisation system: Yes / No

Examinations Officer: _____ Date: _____ Series: _____

Head of Centre: _____ Date: _____