



CHILTERN
LEARNING
TRUST



Lea Manor High School

Cyber Security Policy (Exams) 2026/27

Date Reviewed	Body
October 2026	Jess Pather Headteacher
Next review date: October 2027	To be reviewed: Annually

Together we succeed

1. Introduction

Lea Manor High School is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

Awarding bodies are committed to maintaining the highest standards of cyber security to safeguard sensitive information provided by centres, including personal student data, and to protect the integrity of secure assessments. Centres and centre staff have a critical role to play in maintaining and improving cyber security.

BEST PRACTICE

Cyber Security Awareness and Training

- Make sure all staff who have responsibility for the administration or delivery of examinations receive annual, up-to-date cyber security awareness training, with practical advice on protecting assessment systems and recognising attacks such as phishing or social engineering.
- Attackers often target school or college staff to gain access to assessment systems by tricking them through deceptive messages or phone calls.

Device Security and Asset Register

- Maintain an up-to-date register of all computers, devices, and user accounts used for examinations and assessment administration.
- All devices should be secured with up-to-date anti-malware and software updates. Keeping a full register ensures that all technology used is regularly reviewed, patched, and secured, reducing the risk of overlooked vulnerabilities being exploited.

Create strong unique passwords

- Use a password creation approach such as three random words to generate suitably secure passwords. Research shows that password length is a more valuable defence than complexity.
- Never use easily guessable information such as birthdays, singular names or common words for a password. Attackers can easily discover these and will frequently try to find out this sort of information.
- Always use a strong unique password for every account used and never use the same password across any other account. When passwords are reused, a single account breach puts all accounts with the same shared password at immediate risk. Attackers frequently use breached email and password lists to try to gain access to other services.
- Where possible, use a dedicated password manager to create and store strong, unique passwords for your work accounts. This reduces the risk of forgetting complex passwords or reusing weak passwords, which attackers can exploit through guessing or credential stuffing attacks. Password

managers are more secure than writing passwords down or storing them in your browser without appropriate controls.

Keep all account details secret

Each person who needs access to a system should request their own user account and never share an account assigned for their use with anyone else. Remember that anything done with an account assigned to someone will be attributed to that person in the first instance. Summary

Never share login/password details or additional factor/authentication codes with anyone else. Attackers will often try to trick people into sharing those details with them by pretending to be from their awarding body, a technical support team or other organisation.

2. Scope

This policy applies to all staff, students, governors, and any third parties who have access to Lea Manor High School IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	<i>Overall responsibility for policy implementation and cyber security strategy.</i>
IT Manager/Team	<i>Ash Westcar Implement technical controls, monitor systems, respond to incidents, manage access and updates.</i>
Data Protection Officer	Michael Dolan: <i>Ensure compliance with data protection law, advise on data handling, and oversee data breaches.</i>
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre. Stay alert for all types of social engineering/phishing attempts Care should be taken if unsolicited or unexpected emails, instant messages, or phone calls are received asking for account credentials or personal or confidential information.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

Role	Responsibilities
BROMCOM (MIS)	Before using any third-party or cloud service for exams or assessments, check that the supplier meets recognised cyber security standards and put a data processing agreement in place. Attackers may target suppliers or cloud platforms, or data could be mishandled. Carrying out these checks and having a formal agreement helps keep sensitive assessment information secure and ensures your centre remains legally compliant.

4. Technical Security Measures

Lea Manor High School implements the following security measures, scaled to our size and needs: [amend as appropriate]

- Firewalls and network security controls.
- Anti-virus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.
- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers.

5. User Account Management

- Password governance must follow NCSC Guidance:
 - <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>
 - <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>
- Access control and permissions are based on job roles and reviewed regularly.
- Accounts are promptly disabled when users leave.
- Account activity is monitored and audited.
- Records of cyber training must be retained for all staff and be available for inspection.

6. NCSC and DFE

Centres should stay informed about the latest security threats and trends in account security and educate staff on how to identify phishing attempts, secure devices and protect systems and data.

Both the National Cyber Security Centre (NCSC) and the Department for Education (DfE) have published up-to-date guidance, which all centres should follow. This guidance covers the steps schools and colleges need to take to keep assessment and learner data safe, and to reduce the risk of problems caused by cyber-attacks. This guidance covers the steps schools, colleges and other educational establishments need to take to keep assessment and learner data safe, and to reduce the risk of problems caused by cyber-attacks.

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to IT immediately.
 - a. Steps for identifying and reporting incidents: [Outline procedure]
 - b. Incident response team: [List team members and roles]
 - c. Communication plan for stakeholders – [e.g. relevant awarding body, National Cyber Security Centre (NCSC), etc.]
 - d. Include referral to awarding organisation(s) (if applicable)
 - e. Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary.

8. Compliance and Auditing

- Annual review and update of this policy [Michael Dolan and IT department]
- Regular internal audits: Six monthly
- External audits: [If applicable, specify frequency and type]

9. Policy Review

- This policy will be reviewed annually by a member of the Senior Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.