BRANNEL SCHOOL

EXCELLENCE | CREATIVITY | COMMUNITY

Cyber Security Policy

2025-26

Purpose of this Policy

This policy sets out the measures the CELT Schools will take to protect exam-related data, digital systems, and processes from cyber threats. This includes measures required to comply with JCQ regulations, DfE Cyber Security Standards, and best practice from the National Cyber Security Centre (NCSC).

- DfE cyber security standards highlight the need for robust governance, strong security controls, incident management and data protection to reduce risk in schools.
- NCSC stresses that cyber security must be a high priority for all schools, with dedicated training and practical safeguards.

This policy applies to:

- All systems used for examinations (entries, access arrangements, scripts, results).
- All staff involved in exams administration and invigilation.
- All devices used to access exam data, including school-owned and authorised personal devices.
- All digital storage locations holding exam-related information.

Role and responsibilities

Head of centre

- Compliance with JCQ regulations and industry best practice.
- Implementation of cyber security controls including password policies, updates, backups, and incident response planning.
- Immediate contact with awarding bodies in the event of a cyber incident that could affect learner data or exam delivery.
- Oversight of regular cyber risk assessments, aligned with DfE cyber security standards.

Exam Officer

- Follow best practice for managing personal and sensitive data used in examinations.
- Complete certified cyber security training (The Exams Office).
- Keep all exam accounts secure through strong passwords, secrecy of account details, regular monitoring, and reviewing connected applications.
- Identify and reporting phishing or suspicious activity immediately.

IT Network Managers

- Maintain firewalls, antivirus and filtering/monitoring systems.
- Ensure timely software patching and updates, including preparation for end-of-life systems.
- Conduct regular backups of exam data and testing data restoration.
- Support the Exams Officer in securing storage locations and user accounts.

Invigilators and Exams Staff

- Must complete school-mandated cyber awareness training.
- Must follow guidance for handling digital exam materials and reporting concerns.

Cyber Security Controls

Account & Password Manage

- Strong, unique passwords required for all exam systems.
- Multi-Factor Authentication (MFA) must be enabled where available.
- Passwords must not be shared and must be updated if exposure is suspected.

Device & Network Security

- All devices accessing exam data must be patched and secure.
- Unsupported operating systems (e.g., Windows 10 after Oct 2025) must not be used.
- School network must use secure filtering and monitoring to reduce cyber-incident risks, as recommended by DfE standards.

Data Access & Storage

- Access to exam systems restricted to authorised staff only.
- Sensitive files must be encrypted and stored on secure school servers or approved cloud systems.
- Permissions reviewed termly by the ICT Manager and Data Manager.

Email Security & Phishing Protection

- Staff must remain alert to phishing attempts; cybercriminals increasingly target schools.
- Suspicious emails must be reported to ICT and not opened.

Backups

- Daily automatic backups of exam-related data must be maintained.
- Recovery procedures tested at least once per year.

Training and Awareness

- All staff handling exam information must complete cyber security training delivered or approved by the school.
- Annual refresher training is required for the Exams Officer.
- Training must cover phishing, password hygiene, data handling, and incident reporting.

Compliance with DfE and JCQ Requirements

- The school will follow the DfE Cyber Security Standards, including governance, security control implementation, incident readiness, data protection and patching.
- JCQ regulations require that exam data is securely stored, accessed and transmitted, compliance is mandatory for all staff involved.

Incident Response Procedure

In line with DfE best practice, the school will maintain and test an incident response plan. If a cyber incident occurs:

1. Contain the incident (disconnect affected devices).
2. Report immediately to:

- ICT Manager
- Head of Centre
- Exams Officer
- Awarding bodies (if assessment data is affected).

3. **Document** the breach (time, systems affected, data at risk).
4. **Notify authorities** where necessary
5. **Recover** using clean backups.
6. **Review** and update controls post-incident.

Monitoring, Review & Continuous Improvement

- This policy will be reviewed annually or after any significant cyber incident.