Hungerhill School: Exam Centre Cyber Security Policy

Responsible Committee/Individual	Local Governing Board
Author	Trust IT Manager
Target Audience	Staff involved in examination administration and those with access to awarding organisation systems
National Centre Number	36280
Date Policy Agreed	Summer 2026
Review Date	Summer 2027
Headteacher Signature	K Crayford
Local Governing Board Representative Signature	

1. Purpose

This addendum sets out how Hungerhill School, as an examination centre, applies cyber security controls to protect:

- Awarding organisation systems
- Examination materials and data
- Candidate information relating to examinations

This document should be read alongside the Trust Digital Safety Policy, which provides the overarching technical, organisational, and procedural cyber security framework for all Trust systems.

2. Scope

This addendum applies only to:

- Staff who access awarding organisation systems (e.g. AQA, Pearson, OCR, WJEC)
- Staff involved in examination administration, including:
    - Head of Centre
    - Examinations Officer
    - Seniors leaders with exam oversight
    - Trust ICT staff with relevant access

This addendum applies to JCQ-regulated qualifications only and does not alter the Trust-wide Digital Safety Policy.

3. Roles and responsibilities overview

Head of Centre

- Overall responsibility for compliance with JCQ regulations
- Ensures appropriate cyber security arrangements are in place for examinations

Examinations Officer

- Manages awarding-body system access
- Ensures exam materials are handled securely
- Reports any suspected security incidents related to examinations

Trust ICT Department

- Provides and maintains secure systems in line with the Trust Digital Safety Policy
- Supports incident response and system recovery where required

Staff

- Follow Trust cyber security controls
- Complete annual cyber security training
- Report any suspected security incidents immediately

4. Cyber Security Training

All staff who access awarding organisation systems must complete annual cyber security training. For this centre, this requirement is met through the Trust's mandatory annual training programme, which uses the National Cyber Security Centre (NCSC) Cyber Security Training for School Staff, as referenced by JCQ.

Records of training completion are retained by the Trust and are available for inspection.

5. Access to Awarding Organisation Systems

- Access is restricted to authorised staff only
- Individual user accounts must be used (no shared accounts)
- Strong passwords and multi-factor authentication are enforced in line with Trust policy
- Access is reviewed periodically and removed promptly when no longer required

6. Secure Handling of Exam Materials and Data

- Digital exam materials must be accessed and stored only on Trust-approved systems
- Exam data must not be saved to personal devices or personal cloud storage
- USB storage is avoided and, where exceptionally required, must be encrypted
- Transmission of exam-related data must use Trust-approved platforms

7. Incident Management (Exams)

Any suspected or actual cyber security incident involving:

- Awarding organisation systems
- Examination materials
- Exam-related data

Must be reported immediately in accordance with the Trust Digital Safety Policy.
Where relevant, this will include notification to:

- The appropriate awarding organisation
- JCQ, where required

A post-incident review will be carried out to identify any necessary improvements.

8. Review and Approval

This addendum will be reviewed annually or in response to changes in JCQ regulations or cyber security guidance.

Approved by: Head of Centre

Date: April 2026

Next review due: Summer 2027