

Cloughside College

Cyber Security Policy

Incorporating Examinations and Assessments

Cloughside College

Cyber Security Policy

Incorporating Examinations and Assessments

Document control

| | |
|---------------|--|
| Author | David King |
| Approved by | Governing Body / Board (as applicable) |
| Version | 1.0 (draft) |
| Date approved | 10.03.2026 |
| Review date | 10.03.2027 |

1. Purpose and principles

Cloughside College will protect exam and assessment information, awarding organisation systems access, and personal data from cyber threats. This policy sets minimum controls and behaviours to reduce the risk of unauthorised access, data loss, disruption to examinations, and malpractice.

This policy is aligned with:

- JCQ General Regulations for Approved Centres (current year) and JCQ Guidance for centres on cyber security.
- JCQ Instructions for Conducting Examinations (ICE) and awarding organisation instructions for secure materials downloads and printing.
- Ofqual expectations for secure delivery of regulated qualifications and awarding organisation requirements.
- National Cyber Security Centre (NCSC) guidance for education and staff training resources.
- UK GDPR and the Data Protection Act 2018.

2. Scope

This policy applies to all staff (including temporary staff and invigilators), governors, and contractors who access, handle, store, transmit, print, or administer any exam or assessment materials, candidate data, or awarding organisation systems. It covers all Cloughside sites and any approved off-site arrangements where examinations are conducted.

3. Definitions

| Term | Meaning |
|-------------------------------|---|
| Awarding organisation systems | Secure portals and online services used for exam entries, question paper downloads, results, and post-results services. |
| Exam-related information | Candidate data, entries, timetables, access arrangements, secure materials (including electronic question papers), and assessment administration records. |
| Compromise | Any actual or suspected unauthorised access, disclosure, alteration, loss, encryption, or disruption affecting systems or data. |

4. Roles and responsibilities

These roles apply specifically to cyber security for examinations and assessments and sit alongside the centre Cyber Response Plan.

| Role | Key responsibilities |
|------|----------------------|
|------|----------------------|

| | |
|--|--|
| Head of Centre (Headteacher) – Cybersecurity Incident Lead (CIL) | Overall accountability for compliance with JCQ cyber security requirements. Ensures procedures exist to secure awarding organisation user accounts, confirms annual training completion evidence is retained, and ensures incidents affecting awarding organisation systems are reported immediately to the relevant awarding organisation(s). |
| Exams Officer | Maintains secure processes for awarding organisation portals, downloads and printing of electronic question papers, access control to exam materials, and ensures exam-related devices and accounts are included in the asset register. |
| Technical Support Coordinator (e.g., DSL or nominated SLT) | Works with the IT support provider to contain incidents, considers safeguarding implications, and supports secure working practices where learner data is involved. |
| IT Support Provider (In4Tech Ltd.) | Implements technical controls (patching, malware protection, monitoring, backup and restore), supports incident response and recovery, and advises on improvements. Maintains incident records and supports post-incident review. |
| Data Protection Officer (DPO) | Advises on data protection obligations, including whether an incident constitutes a reportable personal data breach (ICO reporting where required). |
| All staff and invigilators | Complete annual cyber security training if they access awarding organisation systems or handle exam-related information, follow this policy, and report suspicious activity immediately. |
| Governors | Oversee and review cyber security arrangements and policy compliance. |

5. Governance, assurance and evidence

Cloughside will maintain an auditable evidence pack for JCQ inspection, including:

- A current, approved Cyber Security Policy for examinations and assessments.
- Certificates showing annual cyber security training completion for relevant staff.
- An up-to-date asset register of devices and user accounts used for examinations and assessment administration.
- Records of security reviews (MFA checks, leaver access removal checks, privileged access review).

- Evidence of backup and recovery testing for assessment administration systems (at least annually).
- Incident logs and post-incident reviews where applicable.

6. Training and awareness

JCQ requires annual, up-to-date cyber security awareness training for members of centre staff who access awarding organisation systems. Cloughside will ensure relevant staff complete annual training covering: strong unique passwords, MFA, phishing and social engineering, secure handling of exam materials, and reporting routes. Training certificates are retained for inspection.

Acceptable training routes include NCSC training or a JCQ-aligned certificated course (for example, The Exams Office cyber security training and assessment module).

7. Account and access security for awarding organisation systems

- Named account ownership: accounts are allocated to specific staff and are not shared.
- Mandatory multi-factor authentication (MFA) for all awarding organisation accounts and related email accounts.
- Strong, unique passwords for every account; no reuse across accounts.
- Account recovery options are secured and reviewed (recovery email and phone numbers protected with MFA where possible).
- Least privilege: access rights limited to role need; reviewed termly and immediately after staffing changes.
- Leavers and role changes: access removed promptly.
- Connected apps are reviewed and removed when no longer required.
- Accounts are monitored for suspicious activity; suspected compromise is escalated immediately.

8. Device security and asset management

Cloughside will maintain a register of all devices and user accounts used for examinations and assessment administration.

- Up-to-date operating system and security patches.
- Up-to-date anti-malware protection and centrally managed security configuration where available.
- Disk encryption for laptops and portable devices that may contain exam-related information.
- Automatic screen lock and strong authentication for all devices.
- Restricted administrator rights; admin privileges only where required and time-limited where possible.
- Secure remote access only via approved methods with MFA and logging.
- Shared devices: do not save passwords in browsers; clear browser data after use or use private browsing.

9. Network, filtering, monitoring and logging

- Web filtering and monitoring are in place to block malicious sites and alert to suspicious activity.
- Firewall rules and segmentation protect key services (MIS, safeguarding systems, exam administration devices).
- Email security controls reduce phishing risk (spam filtering, link scanning, attachment controls where supported).
- Security logs are retained and reviewed proportionately, with agreed escalation routes with the IT support provider.

10. Secure handling of exam materials and electronic question papers

Controls must prevent unauthorised access during download, printing, collation, and storage.

- Only authorised staff access secure materials download areas.
- Download and print from a trusted, patched device on a secure network, using staff accounts protected by MFA.
- Do not forward secure materials by email or store them in personal cloud services.
- Store downloaded files only in approved secure locations with restricted access.
- Printing and collation are supervised by authorised staff; unattended printers are not used for secure materials.
- Temporary electronic copies are deleted securely immediately after printing and quality checks unless awarding organisation instructions require otherwise.
- Where secure materials are stored physically, storage meets JCQ secure storage expectations and local exams procedures.

11. Data protection and retention

Exam-related personal data must be handled in line with UK GDPR and the Data Protection Act 2018. Access is limited to staff with a defined role in exams administration or delivery. Secure transfer routes are used when sharing data with awarding organisations. Retention and secure disposal follow awarding organisation requirements and the centre retention schedule.

12. Third-party suppliers and cloud services

Before using any third-party or cloud service for exams or assessments, Cloughside will verify that the supplier meets recognised cyber security standards and ensure an appropriate data processing agreement is in place where personal data is processed.

- Supplier access (support accounts, remote access tools) is reviewed and uses MFA.
- Suppliers notify Cloughside promptly of security incidents affecting Cloughside data or services.
- Exam administration systems are included in business continuity planning, including supplier dependencies.

13. Backup, recovery and business continuity for exams

Assessment administration systems are included within disaster recovery and business continuity plans and recovery processes are tested at least annually.

- Nightly backups for critical systems (exam entries, access arrangements, timetables, candidate data, MIS reports used for exams, and secure exam admin documentation).
- Offline or immutable backups are used where feasible to protect against ransomware.
- Backups are tested regularly to confirm restorability and validate recovery objectives for exams-critical systems.
- Exam time-critical workarounds are documented (offline contact lists, printed seating plans, contingency printing routes).

Prioritisation (for restoration following a major incident)

- Tier 1 (0–8 hours): Network connectivity and identity management; awarding organisation access; exam timetable and seating plans; safeguarding systems needed for exam-day welfare; secure communications.
- Tier 2 (24–72 hours): MIS and attendance; teaching and learning platforms; shared drives needed for coursework/controlled assessment.
- Tier 3 (3–7 days): Finance and HR systems; parent communication platforms.
- Tier 4 (1–3 weeks): All other services.

14. Incident reporting, escalation and JCQ notifications

Any suspected cyber incident must be reported immediately. The priority is to protect candidate data, maintain the integrity of assessments, and minimise disruption.

Immediate actions for staff:

- Stop and report: do not continue to click, reply, or authenticate prompts you did not initiate.
- If safe, disconnect affected devices from the network (unplug cable or disable Wi-Fi).
- Contact SLT immediately (in person or by phone) and give a short description of what you observed.

Escalation and external reporting (managed by the Cyber Response Team):

- Activate the centre Cyber Response Plan and engage the IT support provider for containment and recovery.
- Cybersecurity Incident Lead (CIL) notifies the relevant awarding organisation(s) immediately where there is actual or suspected compromise of awarding organisation systems.
- Data Protection Officer (DPO) assesses whether the incident constitutes a reportable personal data breach and, where required, submits any ICO notification within statutory timescales.

- The IT support provider supports technical evidence gathering and, where appropriate, supports reporting to NCSC and Action Fraud, in liaison with the CIL.
- Inform the local authority and governors as required by governance arrangements.

15. Exams disruption and contingency

- Secure and evidence candidate entries, timetables, and access arrangements.
- Maintain secure access to awarding organisation systems for urgent communications.
- Ensure secure printing capacity for question papers and exam materials, including a fall-back device and printer route.
- Implement local contingency arrangements for exam sessions, including manual registers and alternative communication routes.
- Maintain a Business Continuity Folder with paper copies needed for exam delivery.

16. Compliance, testing, monitoring and review

This policy is reviewed at least annually and after any significant cyber incident.

Compliance is monitored through:

- Annual training completion checks with certificate retention.
- Termly access reviews for awarding organisation accounts.
- Annual review of the exams and assessment asset register.
- Annual backup and recovery test for exams-related systems.
- Spot checks during peak exam periods for secure download and printing practices.

Optional assurance activities (where proportionate and supported):

- Annual cyber incident tabletop exercise (drill) focused on exam disruption scenarios.
- Vulnerability scanning or external assurance activity through the IT provider (where appropriate for risk and budget).

Appendix A: Exams and assessment cyber asset register template

Maintain a register of all devices and user accounts used for examinations and assessment administration.

| Asset type | Device/account name | Owner | Location/site | Purpose | MFA enabled (Y/N) | Patch status (date) |
|------------|---------------------|-------|---------------|---------|-------------------|---------------------|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Appendix B: Annual training evidence log

| Name | Role | Training route (NCSC / Exams Office / other) | Date completed | Certificate stored (path/location) |
|------|------|--|----------------|------------------------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Appendix C: Exams cyber incident log (minimum fields)

| Date/time detected | Detected by | Description | Systems affected | Immediate actions taken | Notifications made (AO/NCSC/ICO/etc.) | Outcome and lessons learned |
|--------------------|-------------|-------------|------------------|-------------------------|---------------------------------------|-----------------------------|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Appendix D: Incident contacts (roles and supplier details)

Keep named internal contacts in the Cyber Response Plan so the policy does not need re-issuing when staff change.

IT Support Provider (In4Tech Ltd.)

- Helpdesk: 0808 275 2233
- Support email: support@in4tech.co.uk

- Emergency/out-of-hours: 0808 275 2233 (confirm out-of-hours coverage with supplier)

External reporting routes (as applicable)

- Action Fraud: 0300 123 2040
- Information Commissioner's Office (ICO): 0303 123 1113
- NCSC incident reporting route (as applicable)

Appendix E: Reference documents

- JCQ General Regulations for Approved Centres (current academic year).
- JCQ Guidance for centres on cyber security (current academic year).
- JCQ Instructions for Conducting Examinations (ICE) (current academic year).
- Awarding organisation instructions for secure materials, downloads, printing and storage.
- Cloughside College Cyber Response Plan (current version).
- Cloughside College data protection and acceptable use policies.
- NCSC guidance for schools and staff cyber security training.