KALEIDOSCOPE LEARNING TRUST

Cyber Security Policy

Version and Date		Author	Committee Responsible	Review frequency	Approval	Next Review Due
1.0	11.09.2025	Mrs R Whyles	Executive Leadership Policy	Bi -Annual	Approved by the Executive Leadership 22.09.2025	22.09.2027
2.0	17.12.2025	Mrs R Whyles	Executive Leadership Policy	Annual	Approved by the Executive Leadership 12.01.2026	12.01.2027

Contents

1. Introduction

Cloughwood Academy 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 and JCQ Regulations.

This Cyber Security Policy details the measures taken at Cloughwood Academy to mitigate the risk of cyber threats under the following sections:

1. Roles and responsibilities
2. Complying with JCQ regulations
3. Cyber security best practice
4. Account management best practice
5. Training

The senior leadership team recognises the need for staff involved in the management, administration and conducting of examinations to play a critical role in maintaining and improving cyber security at Cloughwood Academy. This includes ensuring that all members of centre staff who access awarding bodies' online systems undertake annual cyber security training.

2. The scope of this policy

This policy applies to all staff, students, governors, and any third parties who have access to Cloughwood Academy IT systems and data, with particular focus placed upon those members of staff who are involved in the management, administration and conducting of examinations and assessments.

3. Roles and Responsibilities

Role	**Responsibilities**
Governors / Trustees	Oversee and review cyber security arrangements and policy compliance.
Trust CEO	Overall responsibility for policy implementation and cyber security strategy.
IT Team	Novus Implement technical controls, monitor systems, respond to incidents, manage access and updates. They ensure that an up-to-date device security and asset register is maintained which details all computers, devices and user accounts used for examinations and assessment administration. This ensures that all technology used is regularly reviewed, patched and secured, thus reducing the risk of overlooked vulnerabilities being exploited

Role	Responsibilities
	Novus ensure that all devices are secured with up-to-date anti-malware and software updates They ensure that members of the exam team, supported/led by the IT team, adhere to best practice(s) in relation to: - The management of individual/personal data/accounts - Centre wide cyber security including. • Establishing a robust password policy • Enabling multi-factor authentication (MFA) • Keeping software and systems upto date • Implementing network security measures • Conducting regular data backups • Educating employees on security awareness • Developing and testing an incident response plan • Regularly assessing and auditing security controls • Managing and reporting a cyber-attack which impacts any learner data, assessment records or learner work
Data Protection Officer	CFOO Rebecca Whyles Ensure compliance with data protection law, advise on data handling, and oversee data breaches.
Head of Centre, SLT Link Exams and Exams Officer	To ensure that they follow best practice in relation to the management of individual/personal data accounts To provide evidence of an awareness of best practice in relation to cyber security as defined by JCQ regulations/guidance, including the completion of certificated, annual, up-to-date cyber security awareness training To undertake training on: - The importance of creating strong, unique passwords - Keeping all account details secret - Enabling additional security settings wherever possible - Updating any passwords which may have been exposed - Setting up / an awareness of secure account recovery options - Reviewing and managing connected applications

Role	Responsibilities
	- Reviewing and monitoring account access on a regular basis
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within Cloughwood Academy
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

Cloughwood Academy implements the following security measures, scaled to our size and needs:

- 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.
- Multi- Factor authentication (MFA) for all examination boards
- 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.

6. Staff Training and Awareness

- All staff must complete annual cyber security training and annual refresher training.
- Head of Centre, Deputy Head of Centre and Exams Office must complete additional Exams Office Training "Cyber Security Training' on an annual basis. In line with JCQ requirements.
- Records of cyber training will be retained on Flick Learning and Exams Office for all staff and be available for inspection.
- Incident response training for Online Safety Lead and DSLs
- Simulated phishing or breach drills at least once a year

7. Complying with JCQ Regulations

The Head of Centre / Senior Leader of Exams at Cloughwood Academy ensures that there are procedures in place to maintain the security of user accounts in line with JCQ regulations (Sections 3.20 and 3.21 of the General Regulations for Approved Centre's document) by:

- Developing and maintaining this cyber security policy
- Ensuring that all members of Centre staff who access awarding bodies' online systems undertake annual, certificated cyber security training which includes:
  - the importance of creating strong, unique passwords
  - keeping all account details strictly confidential
  - the critical role of Multi-Factor Authentication (MFA) in protecting against unauthorised access
  - how to properly set up and use MFA for both centre and awarding bodies' systems
  - an awareness of all types of social engineering/phishing attempts
  - the importance of staff quickly reporting suspicious activity, events and incidents
- Downloading and retaining certificates of completed staff cyber training on file
- Implementing and enforcing robust security measures, including:
  - mandatory Multi-Factor Authentication (MFA) for all accounts and systems containing exam-related information, including those that interface between awarding body and centre systems, to enhance security and protect sensitive data
  - regularly reviewing and updating security settings to align with current best practices
- Enabling additional security settings wherever possible
- Updating any passwords that may have been exposed
- Setting up secure account recovery options
- Reviewing and managing connected applications
- Monitoring accounts and regularly reviewing account access, including removing access when no longer required
- Ensuring authorised members of staff securely access awarding bodies' online systems in line with awarding body regulations regarding cyber security and the JCQ document *Guidance for centres on cyber security* (www.jcq.org.uk/exams-office/general-regulations), and that where necessary, they have access to a device which complies with awarding bodies' multi-factor authentication (MFA) requirements.
- Reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body

By adopting industry standard cyber security best practices, the Head of Centre is significantly reducing the risk of cyber-attacks and protecting valuable data and assets within the centre.

8. Incident Response Plan

Purpose

To ensure a structured, coordinated, and timely response to cyber security incidents that may impact systems, data, operations, or individuals across the Trust.

Scope

This plan applies to Cloughwood Academy and staff within the Trust, covering incidents that compromise:

- ICT systems or services
- Confidentiality, integrity, or availability of data
- Data protection obligations (e.g. personal data breaches)
- Trust reputation, operations, or financial systems

Definitions

A cyber security incident includes but is not limited to:

- Malware (e.g. ransomware)
- Phishing or spoofing attacks
- Data breaches (accidental or malicious)
- Unauthorised access
- Denial of Service (DoS) attacks
- Insider threats

Incident Response Team (IRT)

Role	Responsibility
Incident Lead (CFOO)	Overall coordination and reporting to CEO/SLT/Trustees
IT Managed Services (Novus)	Technical investigation, containment and recovery
Data Protection Officer (DPO)	Data breach evaluation and ICO reporting
DSL / Online Safety Lead Louise Hood / Rebecca Whyles	Safeguarding-related incidents
Communications Officer (CEO)	Managing internal and external communications

Incident Response Phases

Phase: Identification

Staff must immediately report suspicious emails, unauthorised access, or unusual system behaviour to IT or the Online Safety Lead.
IT logs the event and escalates if a potential breach is detected.
Incident Lead determines severity (low, medium, high) and activates the IRT if required.

Phase: Containment

Isolate affected systems or networks to limit spread (e.g. disconnect internet).
Disable compromised accounts or services.
Secure physical access if needed.
Record all actions taken with time stamps.

Phase: Assessment & Classification

Assess nature and scope of the breach (systems affected, data types, user impact).
Evaluate whether personal data is involved.
Determine if breach is notifiable under UK GDPR.

Phase: Notification

Inform key stakeholders: Headteacher, CEO, Chair of Trustees (as appropriate).
If personal data is compromised:

- Notify the DPO immediately.
- Notify the ICO within 72 hours, if required.
- Notify data subjects if there is a high risk to their rights and freedoms.

Inform the DfE for serious cyber incidents.

Phase: Eradication and Recovery
Remove malware, restore systems from backups.
Conduct vulnerability scans.
Reinstate services after validation and testing.
Change all compromised credentials.

Phase: Post-Incident Review
Convene a review meeting with IRT within 10 working days.
Evaluate root cause, effectiveness of response, lessons learned.
Produce a formal Incident Report for the Trust Board and maintain a secure log.

9. Policy Review

This policy will be reviewed and ratified annually by the Executive Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.