**Cyber Security Policy**

**(Aligned with JCQ and NCSC National Cyber Security Centre Guidance)**

**Policy Title:** Cyber Security Policy
**Effective From:**30 April 2025
**Next Review Date:** 29 April 2026
**Version:** 1.0
**Approved by:** Kandiah Kandeepan (Head of Centre)
Created by: Shandhya Parameswaran, Exams Officer
**Applies To:** All staff, students, contractors, and third-party service providers involved in assessment delivery.

**1. Introduction and Purpose**

Harrow Independent College is committed to ensuring that the security and integrity of its digital systems, particularly those used for assessment and examinations, are protected against the growing threat of cyber-attacks. Cyber security is an essential element in safeguarding not only sensitive personal data but also the fair and uninterrupted delivery of public examinations. This policy has been designed in accordance with the Joint Council for Qualifications (JCQ) publication *Guidance for Centres on Cyber Security* (November 2023) and incorporates best practices advised by the National Cyber Security Centre (NCSC). It aims to establish a robust framework of processes, roles, and technical controls to prevent, detect, and respond to cyber threats that could impact exam delivery and school operations.

**2. Key Objectives**

The primary objective of this policy is to minimise the risk of disruption or data loss caused by cyber incidents such as phishing attacks, malware, unauthorised access, or data breaches. The policy is intended to ensure that secure digital and procedural environments are in place for accessing, storing, and handling examination content and candidate data. This involves the implementation of technical safeguards, user awareness training, well-defined responsibilities, and responsive action plans. By clearly defining expectations and procedures, the college seeks to promote a culture of cyber awareness and proactive risk management.

**3. Governance and Responsibilities**

Responsibility for cyber security ultimately lies with the Head of Centre, who ensures the policy is resourced, supported, and implemented across all relevant departments. The Management Team is responsible for overseeing the day-to-day execution of this policy, coordinating training efforts, evaluating risks, and initiating improvements where necessary. The Business Support Manager is tasked with ensuring that all digital systems are protected through current security tools such as firewalls, anti-malware software, and access controls. They are also in charge of detecting suspicious activity and leading the response to any incident. The Examinations Officer ensures that digital exam materials are downloaded, stored, and handled according to JCQ timelines and security protocols. All staff members are required to follow the college's cyber safety practices and report any suspicious activity without delay. Students are expected to comply with acceptable use policies and are encouraged to engage with awareness initiatives where appropriate.

**4. Risk Management**

The college conducts a formal cyber risk assessment at least once a year and reviews it each term to reflect changes in technology, staffing, or emerging threats. This assessment identifies vulnerabilities in systems, applications, processes, and user behaviour. Each potential risk is evaluated for its likelihood and potential impact, and appropriate control measures are identified and prioritised for implementation. The assessment also includes consideration of physical risks, such as insecure workspaces or access to shared devices. The findings are documented and discussed within the SLT to support informed decision-making and resource allocation.

**5. Access Control and Authentication**

To protect access to sensitive systems, all staff and relevant users are required to use strong, unique passwords that follow recommended practices such as the use of three random words. Access to examination-related platforms, candidate records, and administrative systems is protected through multi-factor authentication (MFA) wherever possible. User access rights are based on the principle of least privilege and are reviewed at regular intervals. Any change in job role or departure from the organisation results in the immediate removal of access. Audit logs are maintained to track who accessed sensitive data and when, ensuring accountability and traceability.

**6. Device and Network Security**

All college-managed devices are configured with up-to-date antivirus software and are included in a central monitoring and patching regime to ensure software is updated in a timely fashion. Devices that are used to access or download examination materials are encrypted and are not used for any non-examination-related purposes. Personal devices are not permitted to access secure examination systems. Network firewalls are configured to protect the school’s internal systems from external threats, and alerts are generated when any unusual behaviour is detected. Any use of removable storage devices is strictly controlled, and only encrypted media is permitted under exceptional circumstances with the written approval of the Business Support Manager.

**7. Data Protection, Storage and Backup**

All candidate data and examination content are encrypted both during transmission and when stored. Data is securely backed up daily to encrypted cloud-based services as well as a secondary offline system to mitigate the risk of ransomware or system failure. These backups are tested regularly to ensure that data can be restored effectively and promptly. Access to examination materials is restricted to authorised users only and is logged appropriately. Retention of data complies with data protection legislation, and sensitive records are deleted securely in accordance with the college’s data retention schedule.

**8. Phishing and Threat Awareness**

Phishing emails and social engineering are among the most common threats to information security. Therefore, all staff are required to complete cyber security awareness training on an annual basis, with refresher briefings delivered termly. These sessions include training on how to identify malicious emails, links, or phone calls and how to report them to the IT department. Simulated phishing campaigns may be carried out periodically to test the responsiveness of staff. Staff are reminded that examination materials should never be downloaded or viewed on non-secure devices or in unsecured locations.

**9. Secure Handling of Examination Materials**

The college strictly adheres to JCQ requirements that examination materials may only be accessed within 60 minutes of the scheduled examination time. These materials are downloaded using a secure college-managed device, which is physically isolated from general use and configured to prevent any unauthorised access. Once downloaded, examination materials are stored in a locked digital folder that is only accessible to the Examinations Officer and Head of Centre. Where printed papers are required, printing is conducted in a secure room with limited access and records of each print job are retained. Any deviation from this procedure, such as an early download or system malfunction, is recorded and reported to the appropriate awarding body.

**10. Incident Response Plan**

A clear incident response plan is in place to guide staff in the event of a cyber security breach. This includes steps to identify the nature of the breach, isolate affected systems, preserve evidence, and notify the relevant awarding bodies and authorities, such as the Information Commissioner’s Office (ICO) if personal data is involved. The IT Manager leads the technical response, while the Head of Centre manages communication with stakeholders. After the incident is contained, a post-incident review is conducted to understand the root cause and to update defences to prevent recurrence. Lessons learned are documented and shared with relevant teams.

**11. Training and Staff Development**

Cyber security training is mandatory for all staff upon joining the college and is refreshed annually. Role-specific training is provided to individuals in high-risk roles, such as those with access to exam materials or IT systems. In addition to structured sessions, the college distributes quarterly cyber awareness bulletins that highlight emerging threats and share practical tips. Students are also invited to participate in digital safety workshops and are encouraged to report suspicious behaviour. The college promotes an open culture where reporting incidents is seen as a positive and necessary act.

**12. Monitoring and Policy Review**

The Management is responsible for monitoring system activity, including logins, file access, and network traffic, using automated tools where possible. Compliance with this policy is reviewed internally at least once a year, and following any significant incident or change in JCQ regulations. Findings from internal audits or reviews may result in updated procedures, retraining, or investment in new technologies. Any serious non-compliance with this policy is subject to disciplinary procedures and may be escalated to external bodies if necessary.

**13. Policy Approval and Endorsement**

This policy has been reviewed and approved by the Head of Centre and reflects Harrow Independent College’s commitment to ensuring a safe, secure, and compliant examination environment.