Policy Statements and Procedures

CYBER SECURITY POLICY

(To Include JCQ regulations 2025 to 2026)

SEPTEMBER 2025

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a college, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cyber Security Policy outlines Hewens College's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of Policy

This policy applies to all Hewens College staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the College.

Risk Management

Hewens College will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors.

Physical Security

Hewens College will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Hewens College will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform IT Support as soon as possible. Personal accounts should not be used for work purposes. Hewens College will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all Hewens College issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to IT Support
- Change all account passwords at once when a device is lost or stolen (and report immediately to AIT (help@advanceditservices.co.uk)
- Report a suspected threat or security weakness in Hewens College's systems to [Risk Register Owner]

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

Data Security

Hewens College will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Hewens College defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology:

- 3 versions of data
- 2 different types of media
- 1 copy offsite/offline

Sharing Files

Hewens College recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keep Hewens College's files on school systems
- Not send school files to personal accounts
- Verify the recipient of data prior to sending
- Use file encryption where possible, sending passwords/keys via alternative communication channels
- Alert IT Support to any breaches, malicious activity or suspected scams

Training

Hewens College recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

System Security

IT Support will build security principles into the design of IT services for Hewens College.

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

Major Incident Response Plan

Hewens College will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e., which backups need to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g., IT support company)

Maintaining Security

Hewens College understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Hewens College will budget appropriately to keep cyber related risk to a minimum.

Cyber Security (JCQ Regulations 2025–26)

In accordance with the **JCQ General Regulations for Approved Centres 2025–26**, this centre is committed to maintaining the highest standards of cyber security to protect candidate data, assessment materials, and all examination systems.

1. Responsibilities

- The **Head of Centre** is responsible for ensuring compliance with JCQ cyber-security requirements.
- All staff with access to awarding-body systems must complete **annual cyber-security training**, covering:
    - password management and the use of **strong, unique passwords**
    - **multi-factor authentication (MFA)** procedures
    - identifying and reporting **phishing attempts** or suspicious activity
    - secure handling of candidate information and assessment data

Training completion records must be retained for audit and inspection.

2. System Access and Controls

- Access to online systems and confidential materials is strictly **role-based** and provided only on a **need-to-know** basis.
- Accounts must be monitored regularly, and access revoked immediately when no longer required.
- **MFA is mandatory** for all staff accounts used to access awarding body platforms.
- Connected applications and integrations must be reviewed to ensure they do not compromise security.

3. Data and Material Protection

- All digital and physical assessment materials must be **securely stored** and transmitted only through approved, encrypted channels.
- Candidate data must be handled in line with **JCQ requirements**, the **UK GDPR**, and the **Data Protection Act 2018**.
- Back-up and recovery systems must be in place to protect against data loss, cyber-attacks, or system failures.

4. Incident Management

- Any **suspected or actual cyber breach** must be reported immediately to the Head of Centre and the relevant awarding body.
- A clear record of the incident, response, and follow-up action must be maintained.
- The centre will cooperate fully with awarding bodies and regulators in investigating and addressing security incidents.

5. Policy Review

- This cyber-security policy will be **reviewed annually** or following any significant change in JCQ requirements, awarding body systems, or internal IT provision.

Created	September 2025
Next Review Date	September 2026