Cyber Security Policy (Public)

Responsible Senior Manager:	Director of IT Services
Effective Date:	November 2026
Related Policies:	
Approved By:	College Leadership Team
Next Review Date:	November 2027

HSDC COLLEGE GROUP

Contents

1.	Scope	4
2.	Governance, Compliance and Audit	4
3.	Roles and Responsibilities	4
4.	Risk Management	5
5.	Staff Awareness & Training	6
6.	Risk Management	6
7.	Technical Security Controls / Safeguards	6
8.	Account Management	7
9.	Incident Management & Response	8
10.	Supply Chain Management	8
11.	Information and Data Protection	8
12.	Planning for a Secure Future	9

Purpose

HSDC recognises that cyber security is fundamental to the delivery of education, the protection of personal information and the continued operation of college services.

HSDC is committed to protecting the confidentiality, integrity and availability of its information, systems, and services. This policy outlines the College's approach to cyber security and demonstrates its commitment to protecting students, staff, partners, and other stakeholders from cyber threats.

1. Scope

This policy applies to:

- All College-owned information systems.
- Cloud-based services used by the College.
- All Staff, Students, Governors, Volunteers, and other stakeholders.
- Contractors and third parties accessing College information or systems.
- Suppliers providing services which process, store or transmit College information.

2. Governance, Compliance and Audit

In-line with the expectations of the UK Government and the guidance of the NCSC, Cyber Security is a board-level concern, and the current state of the college's security posture is regularly communicated and reported on to the college's Executive Team and the Board of Governors.

The college is committed to maintaining recognised cyber security assurance standards, including Cyber Essentials, and continually improves its security posture. Further, it continues to align with all applicable legislation, including UK GDPR and applicable DfE and SFA funding and compliance requirements.

Regular audits are conducted commensurate with risk. This includes policy review, commercial penetration testing of its systems, and compliance audits; both internally and provided by industry recognised compliance service providers across its information systems and services.

The College maintains governance policies and processes to:

- Identify, report on, and remediate cyber security risks.
- Assess threats and vulnerabilities.
- Implement appropriate security controls.
- Review security posture and adjust for real-world threats.
- Support continual reinforcement of good practice.
- Develop, deliver, and track user training.

3. Roles and Responsibilities

Board of Governors	• Providing oversight of cyber security risks. • Ensuring sufficient resources are available. • Reviewing significant cyber security incidents and risks.
Principal and Executive Team	• Supporting effective cyber security governance. • Embedding cyber security into organisational decision-making.

	• Ensuring compliance with this policy.
Director of IT Services (IT Services Team)	• Developing and maintaining the cyber security framework. • Implementing appropriate security controls. • Monitoring cyber risks. • Coordinating incident response activities. • Reporting significant risks and incidents to senior management.
Line Managers	• Ensuring staff complete required training. • Supporting compliance with security policies & procedures. • Reporting concerns and incidents promptly.
Staff	• Completing required training. • Following policies and associated procedures. • Supporting students and other stakeholders they are responsible for in continuing to use college system safely and responsibly and reporting any concerns to the IT Services Team immediately.
Students and other stakeholders.	• Use IT systems responsibly and report any concerns to the IT Services Team immediately.

4. Risk Management

The College adopts a risk-based approach to cyber security.

Risks are identified, assessed, and managed in accordance with college risk management processes.

Security controls are implemented proportionately based upon identified threats and organisational requirements

5. Staff Awareness & Training

All staff are required to complete mandatory training on Cyber Security, Data Protection, and Information Governance both at the start of their employment and regular refreshers at least once a year dependant on role. These courses cover but are not limited to:

- Password security.
- Authentication methods.
- Multi-Factor Authentication (MFA).
- Phishing awareness.
- Other Social engineering threats.
- Safe handling of information.
- Data protection obligations.
- Incident reporting procedures.
- Secure use of cloud services and mobile devices.
- Use of public networks.
- Separation of personal and professional accounts and data.

Completion of mandatory training is tracked and recorded centrally. Results are communicated with managers for compliance management.

6. Risk Management

The College adopts a risk-based approach to cyber security.

Risks are identified, assessed, and managed in accordance with college risk management processes.

Security controls are implemented proportionately based upon identified threats and organisational requirements

7. Technical Security Controls / Safeguards

The college operates a defence-in-depth approach and maintains technical and organisational measures designed to protect information and systems, including but not limited to:

- Dedicated hardware security appliances.
- Server and Endpoint protection against malicious software and unauthorised ingress.
- Email and cloud security.
- Appropriate physical security.

- Access control measures. Including MFA/2FA everywhere it is technically supported.
- Patch management and updates in-line with Cyber Essentials as a minimum.
- Zero trust and least privileged access policies.
- Authentication and account management policies and processes.
- Data protection policy and controls.
- Continually reviewed secure configurations across all software and systems the college administers.
- Data is encrypted in transit and at rest, everywhere this is supported.
- Operational security monitoring and vulnerability management.
- Change management processes.
- Tested and verified backup and recovery arrangements.
- Business continuity and disaster recovery policies and procedures.
- Regular and relevant security awareness training for all staff.

8. Account Management

The College acknowledges that user accounts are often the first and weakest point of attack and most security and data protection breaches happen because of social engineering and phishing attacks. In-line with this and other risk and compliance considerations, the college operates account management policies and procedures, including:

- HR aligned ‘Joiners, Movers, and Leavers’ process.
- Accounts are promptly disabled when users leave.
- Access to systems, services, and software are based on job roles and reviewed regularly.
- Privileged access is tightly controlled and regularly reviewed.
- Password requirements for all systems must at least follow NCSC Guidance and be in-line with Cyber Essentials as a minimum.
- Account activity is monitored and audited, and risks are investigated and remediated with all reasonable speed.

9. Incident Management & Response

The College maintains procedures for identifying, reporting, responding to and recovering from cyber security incidents.

Incidents are investigated promptly and reported to relevant stakeholders where required, either for legal or compliance reasons or to alert them out of courtesy where this is appropriate.

All stakeholders are encouraged to report a suspected incident or any concerns through appropriate means as soon as possible. Staff members have an obligation to report incidents to the IT Service Desk at the earliest opportunity.

While the college does employ information and cyber security staff, additionally, the college maintains relationships with external cyber security specialists to support incident response when required.

Individuals who believe they have identified a security concern involving College systems are encouraged to report it promptly through the College's published contact channels.

10. Supply Chain Management

Cyber security considerations form part of the college's procurement and supplier evaluation processes. Security risks are assessed before new systems, software or services are implemented. All software, systems, and services undergo review commensurate with the risk the use of the aforementioned present. The college keeps a record of all software, systems, and services it operates, including the purpose, rationale, internal leads, access rights and authentication mechanisms, the risk associated with its use, amongst other data to facilitate stakeholders safe use of these resources. This list is reviewed regularly.

Suppliers and partners handling College information are required to implement security controls appropriate to the services they provide, and security requirements may form part of contractual agreements and procurement processes. These must be at least in-line with the task being undertaken and the guidance set by the NCSC and the college’s Cyber Essentials compliance requirements.

Additionally, the college conducts DPIAs (Data Protection Impact Assessments) where data is being shared with third parties and is appropriate or no other agreement or contract covers the storage, processing, or other access to that data.

11. Information and Data Protection

The College is committed to protecting personal data and processing information fairly, lawfully, and securely. Appropriate technical and organisational measures are implemented to safeguard personal information in accordance with applicable legislation. Separate policies are maintained for Information and Data Protection.

12. Planning for a Secure Future

The College is committed to continual improvement and development of its security practises, policies, and procedures which are informed by relevant security standards and bodies including UK GDPR, ISO 27001, DfE and SFA standards, the NCSC, Jisc, and requirements from JCQ and other examinations and awarding bodies, as well as being an active participant in cyber security communities to keep pace with emerging threats.

This policy is reviewed – in line with associated internal policies, processes, and procedures – annually by the Senior Leadership Team in partnership with the IT Services and Information Security teams, with oversight from the Board of Governors.