DOCUMENT DETAILS

Document Name:	**Information Security Policy**			
Approval body:	Board			
Approval date:	March 2025			
Review date:	December 2027			
Document author	Rich Williams, Vice Principal - Funding, MIS & IT			
Document owner	Andy Comyn, Deputy CEO / CFO			
Applicability	Students	x	Staff	x
	Governors	x	Other	
Summary	The purpose of this document is to set out the policy for information security			

DOCUMENT CONSULTATION & APPROVAL

Consultation person / body	**Date passed**
Audit Committee	March 26

Approval body	**Date approved**
Board	March 2026

IMPACT ASSESSMENT

A significant negative impact has been identified in the following area and a full impact assessment / risk assessment is available.

Equality & diversity	No
GDPR	No
Health & safety	No
Safeguarding	No

Friendly version of policy available	No

POLICY CHANGES

Key updates	**Impact**	**Section reference**
Section 5 - Responsibilities	Updating of roles and responsibilities to better reflect responsibility for information security and classification	5
Section 6 - Compliance	Updated to reflect achievement of Cyber Essentials	6
Sections 7-9 – Classification and security measures	Inserted to clarify levels of information classification and security of physical information storage	7-9

CONTENTS

Introduction 2

1. Purpose 2

2. Legislative framework/related policies 3

3. Scope 3

4. Information Security Incident Management 3

5. Responsibilities 4

6. Compliance 5

7. Information Classification 5

8. Access Control 5

9. Physical Security 5

10. Monitoring 5

11. Training and Support 6

12. Review 6

Introduction

This policy is regulated and updated by the information technology (IT) department. It is available to all users of Nottingham College IT services. It will be reviewed and updated on a regular basis to reflect changes in technology and the way in which systems are used, it may also reflect new developments within the IT infrastructure.

The key goal of the Nottingham College Information Security Policy is to present the standards and guidelines that will preserve the confidentiality, integrity, and availability of information and data within the college and with partner organisations. These are core principles within the field of information security and in line with legislation regarding the protection of individual rights. Further detail is provided below.

Lawful Basis for Processing – all data collected, processed and shared by the college should only relate to the performance of the business relationship.

Confidentiality - data is only accessed, processed and shared by authorised users and organisations.

Integrity - data will be accurate, authentic, complete and processed correctly. Where necessary personal data will be removed at the owner's request where this does not impact on the business of the college.

Availability - data can be accessed when required, by those who are authorised to access the data. Data subjects will have access to personal data upon request as stipulated by the UK General Data Protection Regulation (GDPR) under the section individual rights.

Data Breaches – any breach of data protection legislation should be reported to the designated Data Protection Officer in line with the Nottingham College data breach management procedure, who will assess the breach and advise on any appropriate action. Individuals whose data may have been compromised will be informed in a timely manner in line with the legislation. The policy will help the college to maintain the above principles and mitigate the threat of any potential security breaches.

1. Purpose

The purpose of this policy is to detail the standards and guidelines that users should adhere to when accessing the facilities of Nottingham College. It also defines procedures that will be taken to assist in providing a secure environment for information accessibility. Finally, it provides further information, clarification and advice in the form of an 'advisories' section at the end of the policy.

The purpose of the Nottingham College Information Security Policy is to:

- Promote, develop, and maintain a consistent and secure approach to the handling, storing and processing of information.
- Ensure all staff, students and relevant third parties understand their responsibilities with regards to information security.
- Ensure the college Information assets and IT infrastructure are not misused.
- Ensure the college adheres to relevant information security legislation

Failure to adequately secure information increases the risk of significant financial and reputational losses. This policy outlines the college's commitment and approach to information security as well as the roles and responsibilities required to support this.

2. Legislative framework / related policies

2.1 The legislative frameworks applying to this policy are:

- Data Protection Act 2018; UK GDPR; Data Use and Access Act 2025
- Computer Misuse Act 1990
- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

2.2 The related Nottingham College policies are.

- Data Protection Policy
- Data Breach Management Procedure
- Data Retention & Disposal Policy
- Data Subject Access Request Procedure
- Freedom of Information Policy
- IT Acceptable Use Policy
- IT Asset Management Policy
- Network Policy
- Business Continuity & Disaster Recovery Policy

2.3 External standards relevant to this policy are:

- Information Security ISO/IEC 27001
- Information Security ISO/IEC 27002
- JANET Acceptable Use Policy.
- National Cyber Security Centre: Cyber Essentials

3. Scope

3.1 The policy scope is to ensure that the following three key principles of information security are upheld:

Confidentiality:	Ensuring information assets are protected from unauthorised access or modification.
Integrity:	Ensuring information is accurate, complete, and is delivered by reliable systems.
Availability:	Ensuring information is accessible and useable when required for authorised use.

3.2 For the purpose of this policy, information includes data stored on computers (including mobile devices), transmitted across networks; printed out or written on paper; sent out by fax; stored on disk or tape; and, spoken in conversation or over the telephone, including voicemail recordings.

3.3 As such, all information that is created, processed, stored. or transmitted physically or electronically as part of Nottingham College's educational and related business activities is an asset of the organisation and, therefore, should be appropriately protected.

4. Information Security Incident Management

2.1 Any member of staff, student or contractor aware of any information security incident should report it immediately to the college's Data Protection Officer

(dataprotectionofficer@nottinghamcollege.ac.uk). The information security incident management procedure details how such events are addressed and learnt from.

5. Responsibilities

5.1 The Nottingham College board of governors is responsible for approval of the Information Security Policy and for ensuring that appropriate information security arrangements are in place.

5.2 The Nottingham College senior management team is responsible for:

- Providing leadership and commitment to the application of information security, including ongoing review of the Information Security Policy.
- Embedding information security into college operations.
- Ensuring adequate resources are provided for information security

5.3 The Vice Principal - Funding, MIS & is responsible for:

- Reviewing and maintaining the Information Security Policy and updating the documentation to address new threats, legislation and operational requirements of the college.
- Provision of specialist advice on matters of information security.
- Identifying and addressing risks to information systems.
- Ensuring that new systems or changes made to the college's IT do not compromise the security of the existing infrastructure.

5.4 The Head of Governance & Corporate Services is responsible for:

- The classification scheme for information based on its importance to the college.
- Ensuring the implementation and the ongoing maintenance of the records management system.
- Providing advice and guidance to staff regarding record keeping, storage and destruction of documents.
- Ensuring business processes associated with the collation, interpretation and reporting of information across the college are robust, auditable and implemented by all staff.
- Acting as the point of contact with the Information Commissioner's Office.

5.5 The Director Estates & Capital Projects is responsible for:

- Ensuring the physical and environmental security of the Nottingham College premises.

5.6 Information asset owners are responsible for:

- Determining and reviewing the level of access to be granted to staff, students and third parties to ensure the information they manage is appropriately accessible and secure.

5.7 All managers are responsible for:

- Ensuring their staff are aware of their security responsibilities.
- Ensuring their staff have appropriate training for the systems and information they are using or processing.

5.8 All staff:

Should be aware that information security is their responsibility and should be considered as part of everyday working practice. As such, they are responsible for are responsible for:

- Complying with this policy and related procedures Reporting actual or suspected information security incidents immediately and protecting information they access or handle

5.9 All students:
Must abide by the college's Acceptable Use Policy which documents how to use the college's IT appropriately

6. Compliance

6.1 This policy applies to all staff, students, contractors, third parties and partner organisations. Non-compliance should be raised as security incident to the Nottingham College IT Services Helpdesk.

6.2 The College is certified against the UK Government Cyber Essentials scheme and will maintain compliance with its requirements.

6.3 Compliance with this policy may be monitored through audits, reviews, vulnerability management, and technical controls.

6.4 Breaches of this policy may result in disciplinary action and, where appropriate, legal action.

7. Information Classification

Information will be classified to ensure appropriate protection. As a minimum, the college adopts the following classifications:

- Public – Information approved for public release.
- Internal – Information for internal college use only.
- Confidential – Sensitive information requiring protection, including personal data.
- Highly confidential – Information requiring the highest level of protection, such as safeguarding records.

Handling, storage, transmission, and disposal requirements will be defined for each classification.

8. Access Control

- Access to information and systems must be based on business need and least privilege.
- Users must have unique user IDs and must not share accounts.
- Strong passwords and, where appropriate, multi-factor authentication must be used.
- Access rights must be reviewed regularly and removed promptly when no longer required.

9. Physical Security

- Access to college premises and secure areas must be controlled.
- Servers, network equipment, and sensitive records must be protected from unauthorised access.
- Visitors must be supervised where they may have access to information or systems.

10. Monitoring

10.1 The effectiveness of the Information Security Policy and referenced policies requires periodic and event-based monitoring. Any organisational changes to Nottingham

College, legislative change or major IT changes may require review of this policy and others.

10.2 Each college policy will be monitored and its implementation evaluated. Appropriate procedures for monitoring and evaluation are the responsibility of the lead officer. These procedures will be subject to audit.

10.3 The number of information security incidents raised is recorded in a data breach log by the Data Protection Officer.

11. Training and Support

The college will provide mandatory cyber security training to staff and students; this will include and is not limited to software that simulates a cyber incident. Participation is mandatory for staff, and those that do not complete the training in the designated timeframe may be subject to enhanced network controls and restrictions.

12. Review

The Information Security Policy shall be reviewed annually by the Vice Principal - Funding, MIS & IT and presented for approval to the Board or other designated committee every 3 years