POLICIES & PROCEDURES

Information Security Policy

Policy Owner:	Director of Corporate Services
Date Approved:	24 June 2026
Version:	V2.1
Equality Screening Date:	20 March 2026
Date of First Issue:	March 2022
Date of Next Review:	May 2029
Location:	Gateway

Contents

1. Introduction

1.1 Large organisations process substantial volumes of information from multiple sources. The information must be managed securely to protect personal and confidential data from unauthorised access, loss, or misuse.

1.2 Information Security is a key organisational priority. The College maintains appropriate technical, physical and organisational controls to comply with relevant legislation and recognised standards, supporting the secure storage, processing and exchange of information.

2. Policy Purpose

2.1 The Information Governance framework provides a structured approach to the effective management of information. This policy is a core component of that framework and outlines how the College upholds the fundamental principles of Information Security:

- **Confidentiality**: Ensuring that access to information is restricted to authorised individuals.
- **Integrity:** Maintaining accuracy, consistency, and completeness of information.
- **Accessibility:** Ensuring that information is accessible to authorised users when required.

2.2 The College is committed to ensuring that:

- Information is protected against unauthorised access, loss, misuse damage or corruption throughout its lifecycle.
- Staff receive suitable training and awareness to understand their information security responsibilities and incident reporting obligations.
- Third-party service providers handling College information are appropriately monitored and managed.
- All payment card transactions are processed exclusively by approved third-party service providers external to all College systems. The College does not store, process or transmit cardholder data and maintains oversight to ensure

continued compliance with PCI DSS.

- Information is processed securely, supporting operational and business objectives.
- Risk of financial loss, regulatory non-compliance, and reputational damage are minimised through proportionate and effective controls.
- Adequate financial and organisational resources are available to maintain and continually improve information security controls.

3. Policy Scope

3.1 This policy applies to all individuals with authorised access to College information or systems including;

- Staff
- Students
- Governing Body
- External Organisations/Contractors/Visitors
- Third Parties

3.2 This policy applies to all information in all formats and locations, including on-site, remote working environments and third-party systems where College information is processed or stored.

3.3 All individuals within the scope are personally responsible for:

- Using College IT systems in accordance with acceptable use requirements.
- Complying with all relevant Information Security policies, procedures, and standards.
- Handling information in line with its classification (Public, Internal Use, Restricted or Confidential).
- Sharing information only with authorised recipients and exercising appropriate care when doing so.
- Remaining alert to security threats and completing mandatory security awareness training.
- Promptly reporting suspected or actual security incidents in accordance with the College IT Incident Response Plan.

4. Policy Objectives

4.1 The policy aims to:

- Establish an Information Security Framework aligned with confidentiality, integrity, and availability.
- Identify, assess and manage information security risks in line with the College's risk appetite.
- Ensure access to information and systems is role-appropriate and proportionate.
- Promote a strong culture of information security and data protection through appropriate training and awareness.
- Ensure no cardholder data is captured, stored or processed on College systems.
- Implement balanced physical, procedural, and technical controls that support effective operations.
- Use lessons learned from incidents to drive continuous improvement.

5. Implementation Measures

5.1 Training and Awareness

- Staff are vetted and informed of relevant policies during induction.
- Mandatory information security training is completed annually and available for reference.
- Ongoing awareness activities, including simulated phishing, address emerging threats.
- Data is retained in line with GDPR and the FE College Sector (NI) Retention and Disposal Schedule.

5.2 Access Controls

- Access is granted on the principle of least privilege.
- External or guest access is risk assessed and time limited.
- Line Manager approval and IT Services oversight are required for system specific access.
- Strong authentication controls are enforced, and accounts are promptly

revoked when no longer required.

- Access to sensitive systems is monitored.

5.3 Payment Card Processing Controls

- All card transactions are processed entirely outside College systems by approved third-party providers.
- The third-party provider operates secure, host payment environments, with payment details entered directly into their platform.
- All payment data is transmitted exclusively over encrypted connections.
- Cardholder data does not pass through College systems, and the College do not capture, process, store or transmit such data.
- Sensitive payment information remains solely within the external provider's secure infrastructure and is not retained by the College under any circumstances.
- Oversight arrangements ensure continued compliance with PCI DSS.

5.4 Operations Security

- Network protections include anti-virus software, vulnerability management, and Multi Factor Authentication (MFA), where required.
- Secure remote access solutions are enforced as appropriate, i.e. Virtual Private Networks (VPNs).
- Only approved and risk-assessed software may be used.

5.5 Physical and Environmental Security

- Physical access controls, CCTV and environmental safeguards protect facilities and assets.
- Contractor access is risk assessed and controlled.

5.6 Classification and Encryption

- Information is classified according to sensitivity.
- Encryption is applied where appropriate.

5.7 Backup

- All users are responsible for correctly and regularly saving their digital

information.

- Regular backups are performed which have defined recovery limits.

5.8 Information Disposal

- Information and equipment are disposed of securely in line with the FE College Sector (NI) Retention and Disposal Schedule.

5.9 Business Continuity Management

- Incident Response and Business Continuity Plans support recovery from disruptions and incidents.

5.10 Policy Framework

This policy is supported by related policies and standards, which include but is not limited to;

- Information Governance Policy
- Acceptable Use Policy
- IT Security and Auditing Policy
- User Account Management Policy
- IT Backup and Disaster Recovery Policies
- JANET Security Policy (JISC)
- Records Management and Data Protection Policies
- CCTV Policy

5.11 External Relationships

- Third-party access is authorised, limited, and monitored against agreed security requirements.

5.12 Asset Management

- Hardware and software inventories are maintained.
- Secure data cleansing and disposal procedures are applied.
- Asset recovery processes are in place for leaving Staff.

5.13 Information Security Events

- All incidents, near-misses or breaches must be reported promptly.

- Incidents are managed in line with the College procedures and Information Commissioner's Office (ICO) guidance, where required.
- Outcomes inform improvements to controls and practices.

5.14 Audits and Compliance

- Internal and external audits provide assurance of compliance.
- Gap Analysis and compliance checks support continuous improvement.
- Recognised standards such as Cyber Essentials and Cyber Essentials+ are maintained.

6. Roles and Responsibilities

6.1 All users share responsibilities for protecting College information. Additional responsibilities include:

- **Governing Body:** Ensure effective information governance arrangements are in place.
- **Chief Executive:** Accountable Officer, with overall responsibility for Information Governance.
- **Director of Corporate Services:** Senior Information Risk Owner (SIRO). Ensure effective governance and policy compliance.
- **Senior Leadership Team / Management Operations Team:** Promote and support policy implementation in their areas.
- **Information Asset Owners:** Are usually Managers and protect the confidentiality, integrity and availability of their assigned information assets.
- **Information Security Officer:** Supported by Service Delivery Managers, ensure appropriate technical measures are implemented and maintained.
- **College Users:** Comply with policies and promptly report security incidents or concerns to the Data Protection Officer or Information Security Officer.

7. Policy Review

7.1 This policy will undergo an annual review at departmental level to ensure it remains effective, compliant, and aligns with organisational requirements and all applicable

regulations. Where annual review confirms that no amendments are required, the policy will be deemed current and will not require resubmission for higher level approval. Should the review identify substantive changes, the updated policy will be submitted for approval in accordance with the College's established policy review cycle.

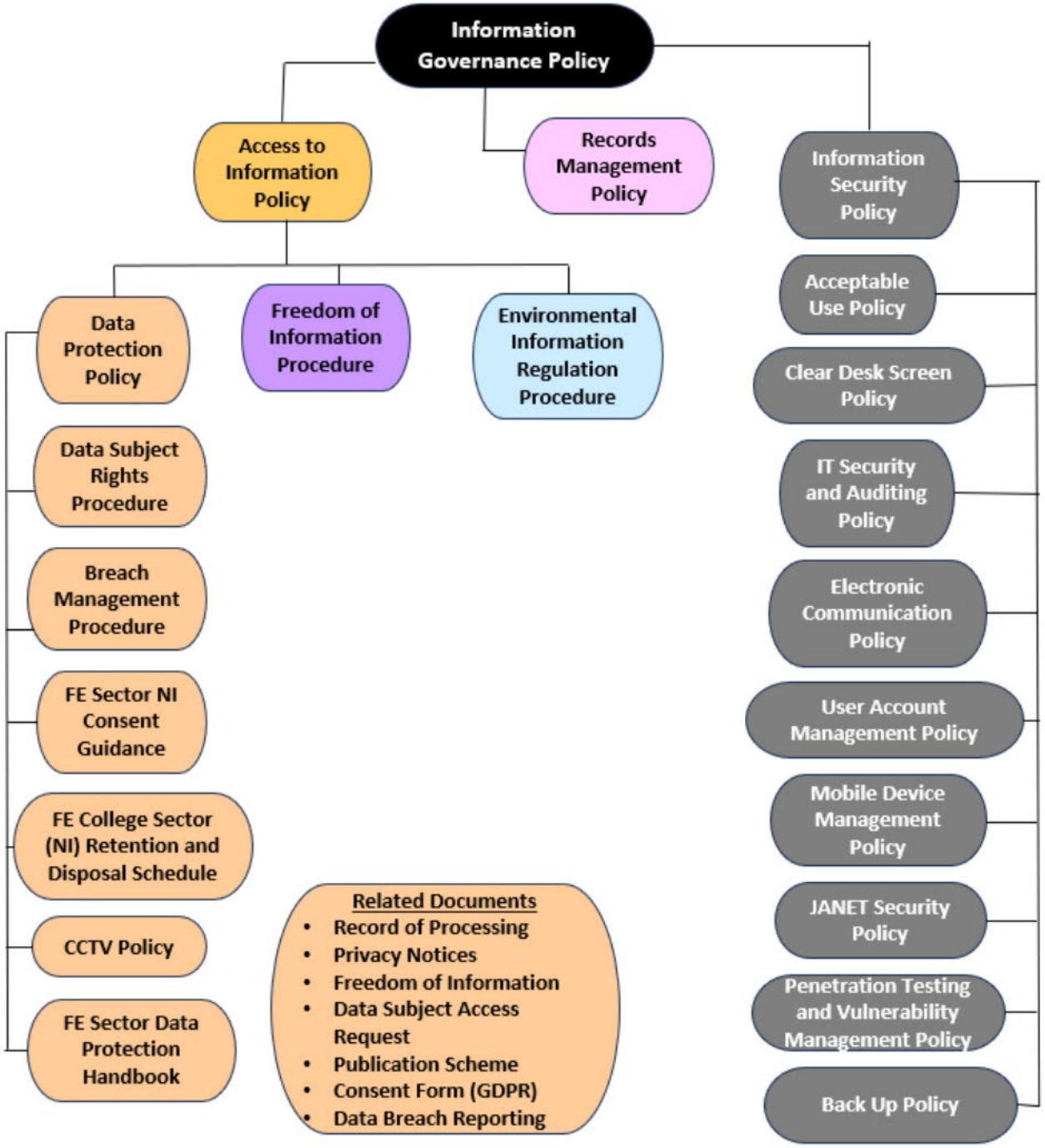
Signed Principal and Chief Executive: _____

Date: _____

Signed Chair of the Governing Body: _____

Date: _____

Appendix 1: Information Governance Framework Schematic



Related Documentation

Title	Location	Owner
Information Governance Policy	Gateway	Director of Corporate Services
Acceptable Use Policy	Gateway	Director of Corporate Services
Clear Desk Screen Policy	Gateway	Director of Corporate Services
Electronic Communications Policy	Gateway	Director of Corporate Services
User Account Management Policy	Gateway	Director of Corporate Services
IT Security and Auditing Policy	Gateway	Director of Corporate Services
Penetration Testing and Vulnerability Assessment Policy	Gateway	Director of Corporate Services
Joint Academic Network (JANET) Security Policy	IT Services	JISC
Access to Information Policy	Gateway	Data Protection Officer
Records Management Policy	Gateway	Data Protection Officer
Data Protection Policy	Gateway	Data Protection Officer
Further Education (FE) College Sector (NI) Retention and Disposal Schedule	Gateway	FE College Sector
Closed Circuit Television (CCTV) Policy	Gateway	Director of Corporate Services

Change Log

Location	Change from deletion/addition	Change to
Original policy rewritten/updated to reflect current practices		
Document header / governance	Version 2.0 with earlier approval, review dates and screening.	Updated to **V2.1** with refreshed approval dates, equality screening, and next review date.
Overall document structure	Largely static policy with limited emphasis on lifecycle controls.	Policy refreshed and streamlined to reflect **current operational practices and governance expectations.**
Introduction	General description of information security importance.	Clearer articulation of **organisational priority**, lifecycle protection, and alignment with legislation and standards.
Policy Purpose	Focused on CIA principles and compliance.	Expanded purpose covering **third-party oversight, PCI DSS arrangements, and organisational risk reduction.**
Policy Scope	Covered staff, students, and third parties.	Explicit inclusion of **all information formats, locations, remote working, and third-party systems.**
Policy Objectives	High-level objectives	Strengthened objectives including **risk appetite, culture of security, and assurance of no cardholder data processing.**
Information Security Framework	Framework described at high level	Expanded framework with clearer, structured control domains (training, access, operations, physical, encryption, backup, disposal, BCM).
Payment Card	Not explicitly defined.	**New explicit statement** confirming all

Processing		card processing is external, no storage or handling of cardholder data, and PCI DSS oversight.
Access Controls	Least privilege and guest access described.	Strengthened controls with **time-limited access, enhanced oversight, monitoring, and revocation expectations.**
Operations Security	Anti-virus, MFA, VPN referenced.	Reinforced operational controls with clearer expectations around **approved software and secure remote access.**
Information Disposal & Retention	Referenced FE retention schedule.	Clearer linkage to **GDPR and FE College Sector (NI) Retention and Disposal Schedule.**
External Relationships	High-level reference to suppliers.	Clearer expectations that **third-party access is authorised, limited, and monitored**
Roles & Responsibilities	Defined but more technically framed.	Clarified and updated responsibilities, including **SIRO role, leadership accountability, and user obligations.**
Policy Review	Biennial review cycle.	**Annual departmental review** with proportionate re-approval approach where no material changes occur.
Equality & Assurance	Screening referenced historically.	Equality screening explicitly completed and recorded for this version.
Change Log	Single generic statement	Retained high-level statement confirming **policy rewritten/updated to reflect current practices.**

Communication

Who needs to know (for action)	Director of Corporate Services
Who needs to be aware	All Staff, Students, Governing Body, Stakeholders

Communication Plan

Action	By Whom	By When
Upload to Gateway	Executive Support Officer	On approval
Circulation to key staff	Executive Support Officer	On approval

Document Development

Details of staff who were involved in the development of this policy:

Name	Role
Sharon McGrath	Director of Corporate Services
Paul Wade	Head of IT Services
Pamela Corrigan	Information Security Officer

Details of staff, external groups or external organisations who were consulted in the development of this policy:

Name	Organisation	Date
N/A	N/A	N/A

Approval Dates

Approved by	Date
Governing Body	24 June 2026

Document History

Issue no. under review	Date of review:	Persons involved in review	Changes made after review? Yes/No If Yes refer to change log	New Issue No.	If changes made was consultation required?	If changes made was Equality Screening required?
V1.0	27.02.2024	PC/PW/JL/SMcG	Yes	V2.0	No	V1.0 not screened-screening V2.0
V2.0	21.01.2026	PC/PW/SMcG	Yes	V2.1	No	Screening updated.