STRANMILLIS UNIVERSITY COLLEGE
A College of Queen's University Belfast

INFORMATION SECURITY POLICY

Version No:	Reason for Update	Date of Update	Updated By
1	New Policy Developed	Approved by Governing Body on 13 June 2017	Senior Management
2			
3			
4			

1. Introduction

The confidentiality, integrity and availability of information, in all its forms is critical to the on-going functioning and good governance of the University College (the College). Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for the College to recover.

This Information Security Policy outlines the College's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the College's information systems. Supporting policies and procedures provide further details on the implementation of this Policy. The College is committed to a robust implementation of Information Security Management; providing clear guidelines to staff, students and other users of the College's information assets of their responsibilities for appropriate use and safety of these assets, and their legal obligations to comply with related statutory requirements.

The principles defined in this Policy will be applied to all of the physical and electronic information assets for which the College is responsible. The College is specifically committed to preserving the confidentiality, integrity and availability of documentation and data created by it and supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract.

1.1 Purpose

The primary purposes of this policy are to:

- make certain that users are aware of and comply with all current and relevant UK and EU legislation.

- ensure the protection of all College information (including but not limited to all documents, computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

- provide a safe and secure information systems working environment for staff, students and any other authorised users.

- ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

- protect the College from liability or damage through the misuse of its IT facilities.

- respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This Policy is applicable to, and will be communicated to, all staff, students, and third parties who interact with information held by the College and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to the College data or telephone networks, systems managed by the College, mobile devices used to connect to College networks or hold College data, data over which the College holds the intellectual property rights, data over which the College is the data owner or data custodian, communications sent to or from the College.

2. Policy

2.1 Principles

The following information security principles provide overarching governance for the security and management of information in the College.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Section 2.5. Information Classification*) and in accordance with relevant legislative, regulatory and contractual requirements (see *Section 2.3 Compliance*).

2. Staff with particular responsibilities for information (see *Section 2.6 Responsibilities*) are responsible for ensuring the classification of that information; for handling that information in accordance with its classification level; and for any Policies, Procedures or Systems for meeting those responsibilities.

3. All users covered by the scope of this Policy (see *Section 1.2 Scope*) must handle information appropriately and in accordance with its classification level.

4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.

5. Information will be protected against unauthorized access and processing in accordance with its classification level.

6. Breaches of this policy must be reported and investigated (*see Section 2.14).*

7. The College will endeavour to adhere to ISO 27001 Information Security Management Standard as a framework for its Information Security Strategy along with other supporting good practices, and will ensure continuous assessment, development and maturity of the strategy.

8. The College will adopt an information security risk management approach in line with the Institution's Risk Management Policy *(see Section 2.11)* to ensure information security risk mitigation efforts reflect the College's risk appetite.

9. The College will establish and promote an information security awareness culture amongst its information asset users through induction, user awareness and training, publications on

information security risks and incidents, and guidelines for managing them.

10. User access to the College's information assets will be based on job requirements rather than job titles. Access rights will be reviewed at regular intervals and revoked if or where necessary.

11. The College believes that information security is the responsibility of its Information Asset Owners and Users, and will set out the responsibilities for the strategic leadership, management and coordination of the information security strategy, and use of its information assets via relevant policies, job descriptions and terms and conditions of employments.

12. Disaster recovery plans for mission critical information assets and related services will be established, tested and maintained.

13. The College will enforce and monitor compliance with the Information Security Policy, supplementary policies, processes, standards, procedures and guidelines.

2.2 Objectives

The objectives of the Information Security Policy are:

1. To ensure that College information assets are available when required to authorised users.

2. To ensure that College information assets are adequately protected against unauthorised access, malicious or accidental loss, misuse or damage.

3. To ensure that all users of College information assets are aware of and fully comply with this policy and supplementary policies, processes, standards, procedures and guidelines.

4. To ensure that all users of College information assets understand their responsibilities for protecting the confidentiality and integrity of the College's information assets.

5. To ensure that the risks to College information assets are appropriately managed.

6. To ensure that information security incidents are reported and resolved promptly and appropriately.

7. To ensure that the College meets relevant audit and statutory requirements.

8. To ensure there is an efficient disaster recovery plan in place.

9. To protect the College from any legal liability resulting from information security incidents.

2.3 Compliance

The College has an obligation to comply with relevant legal and statutory requirements. The Information Security Policy and supplementary policies, processes, standards, procedures and guidelines are to promote and enforce compliance with applicable laws by providing directions and guidelines on good information security practices to underpin the College's compliance with these laws.

The applicable laws include but are not limited to:

a) Data Protection Act (1998)
b) Copyright, Designs and Patents Act (1988)
c) Computer Misuse Act (1990)
d) Public Interest Disclosure Act
Other relevant legislations that may influence this policy can be accessed through the following link:

Legal and Professional Obligations that Limit, Prohibit or Set Conditions in respect of the Management, Use and Disclosure of Information and the Range of Statutes that Permit or Require Information to be Used or Disclosed.

2.4 Relationship with other College Policies

This Information Security Policy is related to the College's:

a) Data Protection Policy
b) Data Privacy Policy
c) IT Security Policies
d) Records Management Policy and Information and Records Management Best Practice Guidance
e) Risk Management Policy
f) Research Data Management Policy
g) Business Continuity Plan

All users of College information assets must comply with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines and must also keep abreast of updates to these policies.

Failure to adhere to the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be addressed in accordance with the College's Disciplinary Procedures, Student Disciplinary Regulations and Procedures and relevant contractor and third party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

2.5 Information Classification

The following table provides a summary of the information classification levels that have been adopted by the College and which underpin the 13 principles of information security defined in this policy. These classification levels explicitly incorporate the Data Protection Act's (DPA) definitions of Personal Data and Sensitive Personal Data, as laid out in the College's Data Protection Policy, and are designed to cover both primary and secondary research data.

Security Level	**Level of Access**	**Examples**	**FOIA2000 / DPA1998 status**

1. Confidential	Normally accessible to specified members of College staff	DPA-defined *Sensitive personal data* (racial/ethnic origin, political opinion, religious physical/mental health condition, sexual life, criminal record) including as used as part of primary or secondary research data as appropriate;
		individuals' bank details;
		Passwords;
		Large aggregates of personally identifying data (>1000 records) including elements such as name, address, telephone number.
			Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.

2. Restricted	Normally accessible only to specified members of College staff or the student body	DPA-defined *Personal Data* (information that identifies living individuals including home / work address, age, telephone number, schools attended, photographs); Draft reports, papers and minutes; Staff monitoring information; Student Results and Classifications; Student Support	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.

		information;
		Governing Body and Committee Papers, including Reserved Business;
		Systems.	

3. Internal Use	Normally accessible only to members of College staff and the student body	Internal correspondence, final working group papers and minutes, committee papers; Information held under license; Governing Body Brief to Staff; Internal College and other Papers held on SharePoint.	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
4. Public	Accessible to all members of the public	Annual Accounts, Annual Report Governance arrangements; Minutes of Governing Body meetings (excluding Reserved Business); Information available on the College website or through the College’s Publications Scheme.	Freely available on the website or through the LSE’s Publication Scheme.

2.6 Responsibilities for Information Security

Senior Management Team

The Senior Management Team is ultimately responsible for information security management and compliance with related statutory laws in the College. The Senior Management Team is responsible for the strategic direction of information security within the College including:

a) Ensuring the information security strategy aligns with College objectives.

b) Endorsing the implementation of approved policies, processes, standards and procedures.

c) Resourcing and supporting information security initiatives.

d) Ensuring risks are mitigated to acceptable levels.

2.7 Corporate Planning Team

The Corporate Planning Team will be responsible for:

a) facilitating the establishment, implementation and evolvement of the Information security strategy; ensuring that information security is properly managed across the College.

b) driving the allocation of resources and supporting the implementation of information security initiatives.

c) facilitating an information security awareness culture in the College.

d) reviewing and approval of relevant policies, procedures, standards and processes.

e) ensuring compliance with relevant policies, audit and statutory requirements.

f) facilitating the implementation of information security initiatives and providing governance oversight on progress and outcomes.

g) reviewing information security requirements for IT and data sharing/migration projects and recommend best practices.

h) reviewing major information security incidents and lessons learned and making recommendations.

i) advising and recommending response plans to related internal and external audit findings.

j) advising the Governing Body and Audit and Risk Assurance Committee on matters relating to information security management and compliance assurance.

2.8 Information Security Management (Digital and Technical Services)

Information Security Management sits within the Digital and Technical Services Team and is responsible for:

a) coordinating the implementation of the Information Security Strategy and Policy, and supplementary policies, processes, standards, procedures and guidelines across the College.

b) communicating the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines to all users of its information assets.

c) coordinating the development and implementation of the Information Security Awareness and Training Plan.

d) monitoring compliance with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines.

e) updating the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines to ensure they remain fit for purpose.

f) managing the implementation of information security risk assessments and relevant mitigation controls; monitoring and reporting on risks to the Corporate Planning Team.

g) managing and monitoring incidents and reporting findings to the Corporate Planning Team.

h) monitoring the state of College information security and reporting on findings and key performance indicators to the Corporate Planning Team to inform the College's governance Statement.

i) monitoring and analysing external information security attack trends and advising the Corporate Planning Team of related risks to the College.

2.9 Information Asset Owners (IAOs)

The College will appoint Information Asset Owners (IAOs) from across the different areas of the College. The IAOs will be accountable to their line manager who is in turn responsible to the Principal as Senior Information Risk Owner (SIRO) for the College. The Principal in turn provides assurance to the Departmental Accounting Officer on the management of Information assets in the College. Detailed guidance on the IAO role and responsibilities is set out in the Information Asset Owner's Handbook.

In brief, the role of the IAO is to understand what information is held, what is added, what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information, and ensure that it is fully used within the law for the public good. IAOs need to manage information assets to comply with statutory obligations (such as the Freedom of Information Act, the Data Protection Act and the Public Records Act 1923).

2.10 All Users (staff, students, contractors and third party agents)

All individuals who access, use, handle and manage the College's information assets are responsible for:

a) familiarising themselves with the Information Security Policy, related policies, processes, standards, procedures and guidelines.

b) familiarising themselves and agreeing to comply with their legal responsibilities for appropriate use and safety of University information assets.

c) completing relevant information security awareness and training courses.

d) ensuring that all Contracts and Service level Agreements entered into by the College, include, where appropriate, clauses in relation to Information Security.

e) reporting information security incidents via the appropriate procedure promptly.

2.11 Risk Management

The College Risk Management Policy is a high level document that sets out the College's approach to managing and reducing risks to an acceptable level.

In line with the Risk Management Policy, the Information Asset Management Handbook contains the necessary guidance and processes which will support College staff in identifying internal and external risks to the security of the College's information assets they are responsible for. Relevant, appropriate and cost effective controls along with necessary training where applicable will be implemented in a timely manner to mitigate identified risks.

In addition, the information security risk management system will be a tool for evaluating the effectiveness of risk mitigation controls, and will inform the recommendation and implementation of new or additional controls where necessary, and ensure continuous monitoring of risks.

2.12 Awareness and Training

Information Security Awareness and Training will be a key component of the College's Information Security Strategy designed to strengthen users' compliance with College Information Security Policies and the College's compliance with audit and statutory requirements.

Through information security awareness and training, the College aims to establish an information security conscious culture, providing basic knowledge and relevant skills that will enable users to carry out their information security responsibilities, and promoting good security practices amongst users of its information assets.

College staff and students must complete relevant awareness and training courses made available by the College. Contractors and third parties will be responsible for providing necessary awareness and training to their staff.

2.13 Incident Management

The management of information security incidents in a prompt and appropriate manner will enable the College to efficiently mitigate the risks and any legal implications that may be associated with information security incidents.

The College's Information Security Incident Reporting Procedure sets out the procedure and guidelines for reporting information security and data breach incidents. The Procedures are available to all users via the College's internet and intranet. All users are responsible for complying with the statements and steps detailed in the Procedures.

2.14 Policy Review and Maintenance

This Policy will be reviewed and updated every three years, or sooner if necessary to ensure that it remains appropriate in light of changes to statutory laws, business requirements or contractual obligations.

3. Definitions

Authorised Users (in the context of this policy and related documents)

All users who access, handle, process, store, share or manage the University College's information assets. These are University College staff, students, contractors and third party agents.

Availability

Information assets are accessible only to authorised users when required.

Business Impact Analysis

A process for determining the impact of a loss or unavailability of an information asset or service to an organisation.

Confidentiality

Access to and sharing of sensitive or personal information is restricted only to authorised individuals.

Information Assets (in the context of this policy and related documents)

A collection of information (paper or digital format), hardware, software, infrastructure and services that support the implementation of University strategic and operational activities.

Research Data

The recorded information (regardless of the form or the media in which they may exist) necessary to support or validate a research project's observations, findings and outputs.

Information Systems

Information processing computers or data communication systems.

Integrity

The preservation of the complete, accurate and validate state of information assets.

Key information assets	Information assets that are highly **essential** to the University College’s **critical** activities and services.
Risk	The probability of an exploited weakness and its resulting consequence leading to an adverse event.
Risk Assessment	A process for identifying and evaluating risks.

Failure to comply with this Policy may give rise to disciplinary action.

4. Review Arrangements

This Policy, which was agreed by the Governing Body on 13 June 2017, will be formally reviewed in three years.

Dr Anne Heaslett	Date	June 2017
Principal	Review Date:	June 2020

For distribution to: All Staff