POLICY TITLE

INFORMATION GOVERNANCE POLICY

Academic Year: 2021/2022 onwards

Target Audience:

Governing Body
All Staff and Students
Stakeholders

Approval by:

CMT - 7 June 2019

Governing Body – 24 June 2019

Policy Number: 057-2019

First Created: May 2019
Reviewed: May 2020
May 2022
Next Review: May 2024

Related Documents:

SERC Publication Scheme
SERC Retention Schedule
Freedom of Information Policy
Data Protection Policy
Freedom of Information (FOI) SOP
ICT Security Policy
Acceptable Use Policy
ICT Security SOP
Freedom of Information Act 2000
Data Protection Act (2018)
General Data Protection Regulations
Environmental Information Regulations 2004

Summary of Contents:

Good Information Governance allows the College to satisfy the needs of corporate accountability, statutory obligations and audit requirements.
This policy sets out in broad terms how College information is managed effectively.

Superseded Documents (if applicable):

02-2013
017-2014 Records management Policy

Enquiries: Any enquiries about the contents of this document should be addressed to:-

Title: Records Manager

Campus Address: Bangor Campus, Castle Park Road, Bangor, BT20 4TD

Tele: 028 9127 6600
Fax: 028 9127 6601
E-mail: informationrights@serc.ac.uk

Equality of Opportunity and Good Relations Screening Information (Section 75):

Date Policy Screened – 27 June 2019

Information Governance Policy
Version History

Version	Description of Changes	Date
1.0	Created	May 2019
1.1	No changes made	June 2020
1.2	No changes made	June 2022

1.0 Background

1.1 South Eastern Regional College's (SERC) compliance with the Data Protection Act (2018) (DPA), UK GDPR and the Freedom of Information Act (2000) (FOI) can only be efficient if there is an investment of time and resources in creating an organised and agreed Information Governance system.

1.2 Information is a vital asset, both in terms of the delivery of teaching and learning and the efficient management of services and resources. It plays a key part in corporate governance, curriculum planning, service delivery and performance management.

1.3 In recognising its public accountability, the College will make every effort to ensure that information is efficiently managed, and that appropriate policies, procedures, training and management accountability and structures provide a robust Information Governance framework. The framework will ensure that information is accessible while also ensuring the confidentiality of personal data and commercially sensitive information, through adopting robust security measures to protect that information from accidental loss, accidental disclosure or deliberate unauthorised disclosure

1.4 Good Information Governance allows the College to satisfy the needs of corporate accountability, statutory obligations and audit requirements by appropriately managing and preserving the records which serve these aims. An approved Information Governance system reduces the risk of records being lost, damaged or accessed by unauthorised personnel.

1.5 In addition, effective Information Governance is an efficient management of resources, helping to reduce costs, avoid wastage and improve retrieval rates in response to Subject Access and Freedom of Information requests.

1.6 SERC is committed to ensuring that the records it produces are managed effectively from the point of creation to their ultimate destruction or transfer to permanent preservation. This policy statement sets out in broad terms how that commitment will be put into practice.

1.7 The term 'Information Governance' describes the structures, policies and practices used to ensure the confidentiality and security of student records, employment records relating to staff and SERC corporate business.

1.8 In terms of SERC, records are documents which evidence College's actions and decisions.

1.9 A record is any information created or received and maintained as evidence of business by a person or organisation. These records can be paper-based or electronic. Some records are essential for on-going work, such as a student Electronic Individual Learning Plan (E-ILP) or Electronic Personal Training Plan (e-PTP). Some records are required to be archived for a statutory period, such as financial records. As a public authority, the College also has a duty to keep some records simply as evidence of what was done and why.

2.0 Scope

2.1 This policy applies to all records created and received by the College. These records will include all student and staff files, invoices, correspondence, policies, minutes of

meetings etc. Its provisions extend to all staff and any students conducting business on behalf of the college.

3.0 Purpose

3.1 The implementation of this policy will:

- Provide clear direction to the College in delivering the requirements of Information Governance and associated policies
- Assist in establishing and maintaining a robust and effective Information Governance Framework that allows The College to fully discharge it legal and statutory obligations.
- Recognise the need for an appropriate balance between openness and confidentiality in the management and use of information
- Minimise the risk of breaches and inappropriate use of personal data and the appropriate management of Information Governance incidents.
- Ensure all staff are sufficiently trained and enabled to follow and promote best practice in regard to the management of information
- Support the embedding of an Information Governance culture in the Trust through increasing awareness and providing training on the key issues
- Maintain a clear reporting structure and ensure that through management action and training all staff understand the IG requirements

4.0 Information Governance Framework

4.1 This Information Governance Framework is intended to pull together the various strands of policy, activity and accountability covered by 'Information Governance'. This is important as there are several policies which impinge on Information Governance.

4.2 The Framework cannot be seen in isolation as information is central to all areas of work in the College. Information Governance is also a key element of Corporate Governance. This policy is, therefore, closely linked with other strategies to ensure integration with all aspects of the College's business activities.

4.3 The Framework will enable the College to set out and promote a culture of good practice around the processing of information, the use of information systems throughout the organisation and the quality of our records to comply with our statutory and legislative requirements. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner.

4.4 The College requires all employees to comply with the extant policies, procedures and guidelines which are in place to implement this framework

5.0 Roles and Responsibilities for Information Governance and Organisational Responsibility

5.1 Principal and Chief Executive

The Principal and Chief Executive is the Accounting Officer with overall accountability and responsibility for Information Governance in the College and required to provide assurance to the Department of Economy that all risks, including those relating to information, are effectively managed and mitigated.

5.2 College Governing Body

The Governing Body is responsible for ensuring appropriate systems are in place to ensure effective Information Governance across all the services for which the College is responsible. The Governing Body will have an agreed method of Information Governance assurance with the College Management Team.

5.3 College Management Team

The College Management Team will receive updates on Information Governance matters on both a formal and informal basis via the Director of Curriculum and Information Services who fulfils the role of Senior Information Risk Owner (SIRO) and Chair of the Information and Cyber Security Committee.

5.4 Information and Cyber Security Committee

The purpose of the Information and Cyber Security Committee is to provide strategic direction & to ensure the implementation of best practice in regard to risk management, the security of college IT systems & the security/privacy/retention of information relating to staff, students & other business activity.

5.5 Chief Technology Officer

The Chief Technology Officer is responsible for IT security within the College by:

- Providing advice on the design and implementation of IT security aspects of IT solutions;
- Providing technical leadership on all aspects of the College's IT security infrastructure
- Ensuring Best Practice standards are adhered to
- Pro-actively monitor key systems to ensure the security of College information and information systems
- Investigating IT security breaches and incidents
- Ensuring IT security services operational documentation is up to date.

5.6 Records Manager

The Records Manager has responsibility on behalf of the above to:

- Ensure the College is aware of changes in legislation which impact on how we manage our records and update relevant policies and SOPs to reflect such.
- Establish, monitor and review a College Information Governance system to ensure compliance with legislation which impact on College records.
- Develop, co-ordinate and deliver a College wide training and awareness programme on DPA, FOI and Information Governance and communicate staff responsibilities applicable to regarding compliance.
- Act as point of contact for all FOI and Data Protection Requests, liaise with all responsible owners and issue a response in compliance with the relevant Act(s) of legislation.

5.7 All Budget Holders

Budget Holders are responsible for:

- The compliant management of records within the scope of their responsibility
- Reporting concerns to the Records Manager.

- Adherence to data protection legislation, associated policies and SOPs, the FE Sector Retention and Disposal Schedule and ensuring all staff within their units have completed mandatory training.

5.8 **All Staff**

All employees, workers, contractors, agency workers, consultants, directors (collectively referred to as Staff) are responsible for:

- Adhering to this Policy and other supporting policies, procedures and training.
- Reporting incidents regarding College information to managers or Data Protection Officer immediately upon discovery

6.0 Legal Obligations

6.1 As a public authority SERC must manage its records in accordance with Acts of legislation. The Information Commissioners Office (ICO) regulates the application of these Acts and will take action where a breach occurs.

6.2 In addition, the Northern Ireland Public Services Ombudsman (NIPSO) has the regulatory power to request SERC records in response to any allegation of maladministration. The College must be able to evidence records of its business affairs and decision-making rationale.

6.3 Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act (2000)
Section 46 of the Freedom of Information Act (2000) states that the Lord Chancellor will issue "a Code of Practice providing guidance to relevant authorities as to the practice which it would, in his opinion, be desirable for them to follow in connection with the keeping, management and destruction of their records."

6.4 The Public Records Act (NI), 1923

The Public Records Act (1923) established The Public Record Office of Northern Ireland (PRONI) as the place of deposit for public records, created the roles of Keeper and Deputy Keeper of the records as well as defining what public records actually are.

6.5 Freedom of Information Act (2000)

The Freedom of Information (FOI) Act 2000 covers any recorded information i.e. printed documents, computer files, letters, emails, photographs, sound and video recordings held by the College. The main principle behind the FOI legislation is that the general public have a right to know about the activities of public authorities unless there is a good reason for them not to. Information may only be withheld if there is an absolute exemption or the public interest test considers that the public interest in maintaining a qualified exemption outweighs disclosure.

The College has a legal obligation to provide information through an approved publication scheme and in response to requests. The College must respond to a request within **20** working days.

6.6 Publication Scheme

The College must also produce a “Publication Scheme” which should list classes of information about activities which are in the public domain and which the College has published or intends to publish. In this context, "publish" means to make information routinely available. It must also make clear how the information described can be accessed, the medium in which it is available and whether or not charges will apply.

These descriptions are called "classes of information". The scheme is not a list of the actual publications, because this will change as new material is published or existing material revised. It is, however, SERC’s commitment to make available the information described.

The Publication Scheme is available on the SERC website.

6.7 Disposal of Records Order (1925)

The Disposal of Records Order (1925) sets out how PRONI and government departments should deal with the disposal of public records once their business need comes to an end. Records management is ultimately a matter of risk management, and the College must control the risks associated with the retention and disposal of records. The ICO and PRONI require the College to develop an NI Assembly approved Retention Schedule which identifies the classes of information held, how long the record should be archived and retained and what the final action will be e.g. destroy, transfer to permanent archive. A Retention Schedule is a list of record types or ‘classes’ with the following information:

- **Functionality**: The general category of information
- **Record Type:** What the record contains information on and how it is used
- **Retention Period:** How long to keep the records for
- **Statutory authority or guidelines:** Is there a legal or departmental requirement to retain the information
- **Final Action:** What we do when the record reaches its ‘disposal date’

The majority of records created by the College do not have sufficient importance to warrant permanent retention and should be destroyed at specified times according to the agreed Retention Schedule. The destruction of any record produced by the College in the course of its activities should only be carried out after it is has been assessed for legal, administration or archival retention requirements. Confidential records must be disposed of securely and safely and an audit trail must be kept of such actions.

6.8 Data Protection Act (2018) UK GDPR

Under DPA/GDPR the College is a registered data controller, registration number Z6477199. The College is required to process and safeguard all personal data in accordance with the 6 principles set out in UK GDPR.
The College recognises the importance of protecting its information assets and, in particular, the information relating to its staff, students and other individuals in whatever form that information is held.

6.9 Environmental Information Regulations (2004)

The Environmental Information Regulations (2004) EIR require public authorities to take reasonable steps to organise and keep up to date the environmental information which it holds, and which is relevant to the public authorities' function. It gives members of the public the right to access 'environmental information' held by public authorities. The College must respond to a request within 20 working days.

7.0 Classification of types of records – format, confidential and non-confidential

7.1 There are three stages of the life of every record: it is created as a current/active record; it is maintained as a semi-current record with continued value for the College e.g. reference purposes or audit requirements; and it is destroyed or transferred to permanent preservation when it becomes a non-current record.

8.0 Information Audit

8.1 The Records Manager will conduct biennial audit of SERC records. The audit will identify new records created and held by SERC, storage arrangements and permissions for electronic access. Significant changes to records held by SERC will be considered for inclusion on the Retention and Disposal Schedule.

9.0 Information Asset Register/Record of Processing Activities

9.1 The College has an Information Asset Register which also serves as the Record of Processing Activities as required by UK GDPR. This document records the detail of both personal and no personal data. It will be appraised on a biennially. See 8.1 above.

10.0 Version control

10.1 As part of efficient management of information and audit requirements it is vital that the administrative journey of a policy is recorded. The final approval should indicate the level at which final approval of the policy rests and the date when the policy receives final approval. Policy Review should document any changes and whether it requires re-approval.

11.0 Communication Plan

11.1 This Policy will be communicated via staff development training and the intranet and will be made available, on request, in alternative formats including large print, braille, audio, and in minority languages to meet the requirements of those who are not fluent in English

12.0 Review

12.1 This Policy will be reviewed (and amended if necessary) every two years, or sooner if required to reflect changes in legislation or circumstances.