NORTHERN
Regional College

Information Governance Policy

CBD 6

Issue	Date of 1st Issue	Last Reviewed	Date of Next Review	Responsibility of
01	March 2019		March 2020	Chief Information Officer

This document can also be produced in alternative formats upon request.

Contents

Information Governance Policy

1. Introduction

The Northern Regional College (the College) is heavily dependent on the information and records it holds. It recognises that its records and information must be appropriately managed, handled and protected to serve its business needs and act openly while at the same time ensuring that personal and sensitive data is protected. 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 and performance management.

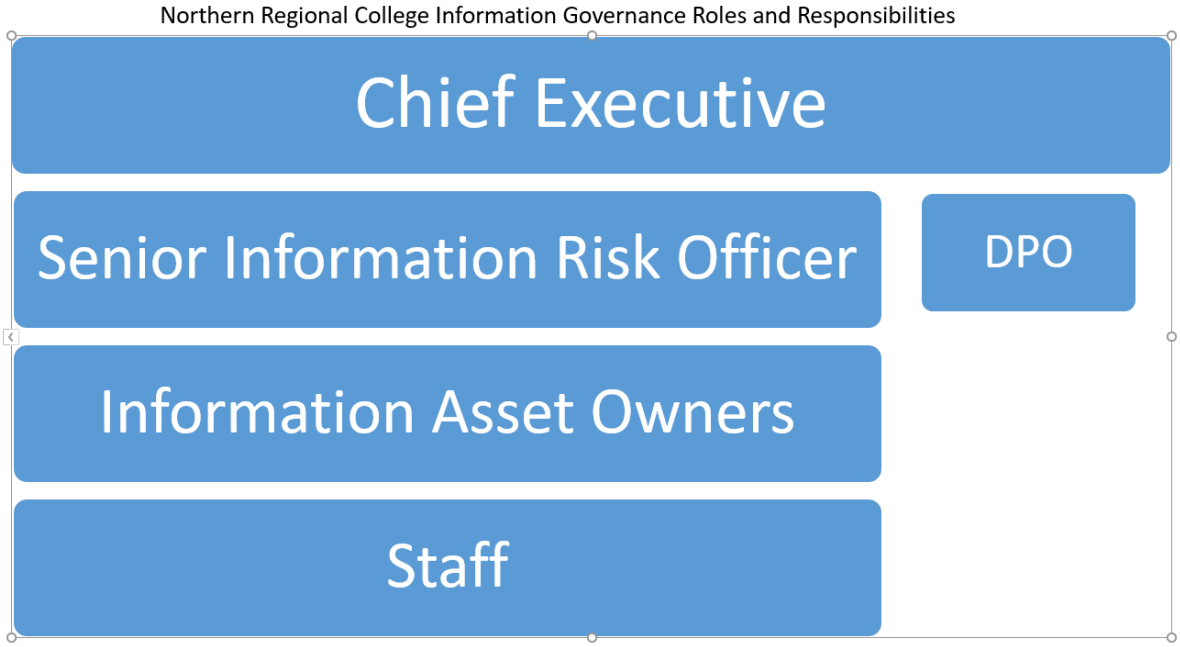
In recognising its public accountability the College will make every effort to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management. The framework will ensure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

2. Scope & Purpose of Information Governance Policy

The Information Governance Policy sets out the framework to ensure that the College meets its obligations in respect of information governance; it will also be the vehicle for improving information governance in the College. It will be supported by annual Action Plans setting out how it will be implemented. The action plan will be monitored by the Information Governance Team, chaired by the Senior Information Risk Owner (Chief Information Officer). Reports will be submitted to the Audit and Risk Committee on a regular basis.

The general purpose of the Information Governance Strategy is to provide clear direction to the College in delivering the requirements of information governance and associated policies. The strategy will assist in establishing and maintaining a robust and effective Information Governance Framework that allows the College to fully discharge its strategic duties ensuring that overall corporate compliance is met both in relation to legal and statutory obligations.

The Information Governance Strategy 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. Further information on the roles and responsibilities within the Information Governance Framework are detailed in Appendix 1.



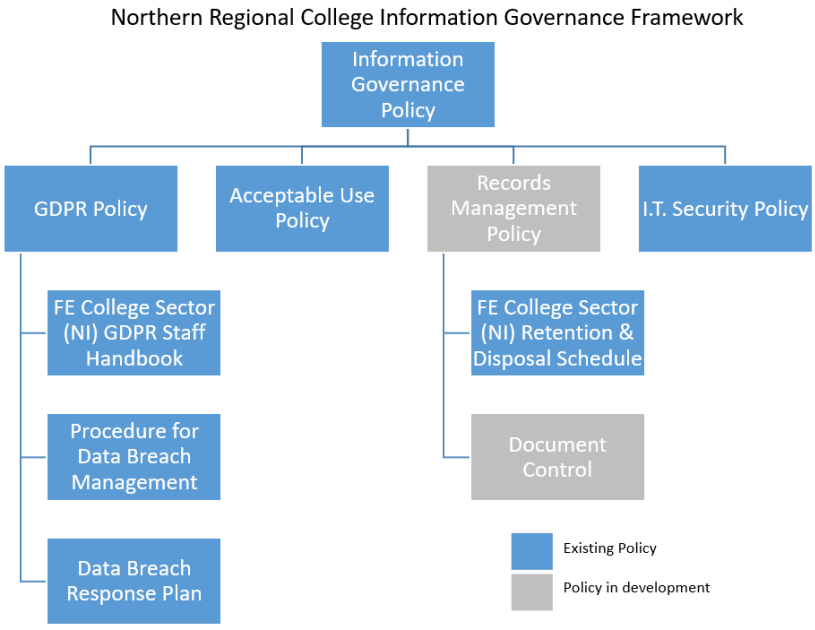
3. Information Governance Policy Statement

A clear policy framework is critical to ensuring a coherent approach to Information Governance across all College functions and locations. This strategy is supported by a suite of Information Governance policies. All Information Governance related policies will be reviewed and updated as necessary on a regular basis.

4. Information Governance Framework

The Information Governance Framework is intended to pull together the various strands of policy and activity covered by 'Information Governance'. This is important as there are several policies which impinge on Information Governance. It will enable the College to set out and promote a culture of good practice around the processing of information and use of information systems throughout the organisation. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The College requires all employees to comply with the extant

policies, procedures and guidelines which are in place to implement this framework.



5. Objectives

The objectives and subsequent benefits of a robust and fully implemented Information Governance strategy can be summarised as follows:

- Ensures that decisions are based on readily accessible high quality information
- Ensure that information is held and handled securely, and that personal and sensitive information is safeguarded
- Reduce risks associated with poor and unregulated systems and processes
- Reduce data losses and the negative impact such losses have on corporate image
- Ensures that legal and statutory obligations are met
- Supports corporate governance and corporate risk register
- Ensures that information and information assets are managed in a coherent manner reducing duplication of effort and increasing availability
- Complying with all legislation
- Establishing, implementing and maintaining policies for the effective management of information
- Recognising the need for an appropriate balance between openness and confidentiality in the management and use of information
- Providing assurance that all information risks are identified, managed and where possible mitigated
- Minimising the risk of breaches and inappropriate use of personal data

- Ensuring that the public are effectively informed and know how to access their information and exercise their right of choice
- Ensuring all staff are sufficiently trained and enabled to follow and promote best practice, in regard to the management of information.

6. Legislative Compliance, Relevant Policies, procedures and Guidance

Information Governance provides a consistent way for employees to deal with the many different information handling requirements.

The College, as the "legal person" and Data Controller for the purposes of the Data Protection Act 2018 will ensure that all personal data it holds is controlled and managed in accordance with the principles of the Data Protection Act 2018, European Convention of Human Rights (Article 8), Human Rights Act 1998 and common law Duty of Confidentiality. This is set out in the College's Data Protection Policy and Records Management Policy.

7. Information Governance Data Incidents

The Data Protection Officer must be notified immediately of all information security incidents involving the unauthorised disclosure of personal identifiable data/information (for consideration of any necessary actions refer to the College's Data Breach Response Procedure).

A key function of the Information Governance Team is to monitor and review untoward occurrences and incidents relating to Information Governance and to ensure that effective remedial and preventative action is taken.

Information incident reporting is in line with the College's overall incident reporting processes.

8. Data Protection Impact Assessments (DPIA)

All new projects or policies that involve processing of personal or sensitive personal data and any subsequent changes to projects or policies must have a DPIA

completed. All new software systems introduced to the College or restructuring of personal data must also have a DPIA completed. The DPIA must be completed prior to processing commencing. The DPO must be informed of a DPIA, they will monitor compliance, give advice and remain independent and they cannot complete the DPIA.

9. Implementation and Performance Monitoring

The implementation of this Policy is evidenced and monitored through the agenda of the Information Governance Team. It will also be monitored through regular audits performed jointly by IAOs and the DPO.

10. Dissemination

It is the responsibility of all Managers to ensure that staff have access to this policy and to ensure through team meetings that staff are aware of their obligations.

11. Resources Training and Education

All staff should receive basic Information Governance Training appropriate to their role through either face to face training or the training package on the College's Digital Learning Environment.

Information Governance Training is incorporated into the College's Mandatory Training programme. It is a **mandatory** requirement for all staff in the College, without exception to undertake Data Protection training which is appropriate to their role. This includes staff on temporary contracts, secondments, agency staff and students.

Different levels of training will be delivered:

- All staff to receive Information Governance awareness training as part of their corporate induction programme
- Departmental induction must ensure that staff are made fully aware of all Information Governance policies and procedure.

12. Quality Assurance

12.1. Comments and complaints regarding this document will be handled through the College's comments and complaints mechanisms. If you have a comment or complaint, or require further information regarding the process, please e-mail quality.improvement@nrc.ac.uk .

12.2. The following processes must be followed to monitor and review this document:

a. It will be monitored on an ongoing basis and subject to a full review at least every two years.
b. It may also be updated if changes or improvements in processes or procedures are identified.
c. In monitoring and reviewing the document, the following will be taken into consideration:
   - feedback regarding the content and format of the document;
   - uptake and usage;
   - comments or complaints regarding the document;
   - Equality information and monitoring data.

13. Links to other Documents

Internal Documents:

- IT Security Policy
- Records Management Policy (in development)
- Acceptable Use Policy
- FOI Procedure
- GDPR Policy

External Documents:

- FE Sector Retention and Disposal Policy

Appendix 1: Roles and Responsibilities

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

The College 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. An Information Governance annual report will be presented to the Governing Body at least annually.

College Senior Leadership Team SLT - will receive updates on Information Governance matters on both a formal and informal basis via the Chief Information Officer who fulfils the role of Senior Information Risk Owner (SIRO) and Chair of the Information Governance Team. -

The Senior Information Risk Owner - The Chief Information Officer is the Senior Information Risk Owner (SIRO). The SIRO has overall responsibility for managing information risk across the College and is the owner of the Information Asset Register. The SIRO is a member of the Senior Leadership Team and provides advice to the Accounting Officer in regard to information risk.

The SIRO is responsible to the SLT and Governing Body for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with the College's Information Governance and Records Management Policies.

Information Governance Lead/Data Protection Officer - The Head of Performance and Planning leads on the Information Governance Programme and provides assurance to the SIRO and also acts as the College's Data Protection Officer. The Head of Performance and Planning responsibilities include:

- ❖ to review and update Information Governance policy in line with local and national requirements;

- ensure that line managers are aware of the requirements of Information Governance and associated policies;
- monitor and report on compliance with Freedom of Information Act and Data Protection Act 2018;
- assess risk and advise on information incidents and data breaches to ensure consistent reporting to regulatory bodies;
- Provide advice and guidance on Information Governance issues with targeted training as appropriate.

Information Governance Team - has responsibility for overseeing the implementation of the Information Governance Strategy incorporating Framework, and the Information Governance Policy.

Information Asset Owners (IAOs) - are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.

The IAO role is to understand and assess risks to the information assets they 'own' and to provide assurance to the SIRO (via Head of Performance and Planning) on the security and use of those assets. They will ensure that all threats, vulnerabilities and impacts are properly assessed and included in their Directorate Risk Register and where necessary that these are escalated to the Corporate Risk Register by the Vice Principal.

All Staff - it is the responsibility of each employee to adhere to this policy and all supporting Information Governance policies, procedures and guidance.

All staff members are required to undertake mandatory information governance e-learning modules. Information governance training is required to be undertaken on a three yearly basis. All staff must ensure that they use the College's Information Technology systems appropriately, and adhere to the Acceptable Use Policy.

Appendix 2: Legislation and Guidance

Public Records Act (NI) 1923

It is a legislative requirement for Northern Regional College to implement records management as set out in this Act. The legislation lays down the procedures both for the destruction of records/information deemed to have no long-term value, and for the preservation and transfer of it.

Freedom of Information Act 2000 (FOI)

The FOI Act provides a statutory right of access to information held by public authorities (subject to exemptions). Public authorities are obliged to comply with The Lord Chancellor's Code of Practice on Information Management which is intended to support the objectives of the FOI legislation by outlining the management practices that should be followed by public authorities in relation to the creating, keeping, managing and disposal of their records.

The Data Protection Act 2018 (DPA)

The DPA entitles individuals to access their personal information, which is being processed by another on request. Records therefore need to be managed effectively to enable Northern Regional College to respond to requests for access to information.

Environmental Information Regulations 2004 (EIR)

The EIR provides the public with a statutory right of access to environmental information held by public authorities.

Appendix 3: Northern Regional College Information Governance Team Terms of Reference

- Provide Quality Assurance, including advice and support, to Projects and Groups to ensure best practice in information governance in line with appropriate legislation
- Develop Strategic solutions to Common Information Governance problems
- Provide a forum to raise awareness and share experience and best practice in Information Governance
- Act as Directorate point of contact for Information Governance related issues such as Freedom of Information, Information Security and Data Protection etc.
- Ensure that the actions identified in the information governance action plan are taken forward.
- Share knowledge/experience.

Working Arrangements

- The Group will meet on a Monthly basis.
- The Group may from time to time call upon advisors
- The group will be chaired by the SIRO
- The SIRO's department will provide the secretariat for the meeting
- The content and the agenda will be agreed with the Chair of the meeting prior to issue.
- Minutes of meeting will be produced and agreed with the chair prior to issue. These will be circulated as soon as possible after the meeting listing topics discussed, actions agreed and individuals responsible for undertaking those actions.
- The Group will review its TOR on an annual basis.

Reporting Arrangements

The Group will report to:

- SLT
- Audit and Risk Committee

Membership

- Steve Brankin Chief Information Officer/ SIRO – Chair
- Helen Dixon Head of Digital Learning
- Glenn Millen Head of Process & System Transformation
- John Ross Head of IT
- Julie Kerr Head of MIS
- Deborah Kerr Head of Performance and Planning/DPO
- As required other IAOs may attend

Document Development

Please complete with details regarding the development of this Policy.

D1. Working Group

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

Name	Position
Steve Brankin	Chief Information Officer/ SIRO
Helen Dixon	Head of Digital Learning
Glenn Millen	Head of Process & System Transformation
John Ross	Head of IT
Julie Kerr	Head of MIS
Deborah Kerr	Head of Performance and Planning/DPO

D2. Consultation

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

Please refer to Equality Screening Consultation Guidance.

Name	Organisation	Date
	FE Sector DPO Group	December 2018

D3. Approval Dates:

Details	Date Approved
Equality Screening *(please refer to Equality Screening Guidance)*	11.3.19
Quality Checked *(please refer to Quality Checklist)*	11.3.19
SLT	
Governing Body *(SLT to decide if PPS needs to go to Governing Body)*	21.2.19

D4. Communication Plan:

Please provide details and dates as to how this policy will be communicated, implemented and disseminated:

Action:	Action by:	Date:
All staff email to be issued	DK/BM	13.3.19
Upload to the Staff Intranet	QM	13.3.19

D5. Document History

Issue no. under review (Please see the front page)	Date of review: (Date)	Who was involved in reviewing the document? (Name/s)	Were changes made to the document after reviewing? (Yes or No)	If changes have been made, please provide brief details:	New Issue No.	If Yes, did the document need to go through consultation again? (Yes*/No)	If Yes, did the document need to be Equality Screened again? (Yes*/No)	If Yes, date those affected by document will be alerted of updated document: (Date)

***** If you answered 'Yes' in columns E or F, you must forward details of additional consultation and/or screening to the Equality Officer.