NIPEC/20/21
(replacing NIPEC/19/13)

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Information Governance Policy

(incorporating the Information Governance Framework)

January 2021

Any request for the document in another format or language will be considered

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

https://nipec.hscni.net

Developed by:	Janet Hall
Reviewed:	November 2019 January 2021
Approved by / date:	**BTM:** 12th January 2021 **Council:** 8th February 2021
Date of next Review:	December 2023
Equality Screened by / date:	2019

Contents

1.0 INTRODUCTION

Information Governance (IG) is about how we look after our information and describes necessary safeguards for, and appropriate use of, all information including personal and sensitive information to ensure we process it carefully, confidentially and in line with current legislation. A robust IG framework is essential to ensure that information is efficiently managed and that appropriate policies, procedures and accountability arrangements are in place.

IG helps us manage and control our information by:

- supporting our work activities;
- helping us understand our performance relating to the management of information and data;
- identifying improvement and ensuring compliance with our statutory and legislative duties.

It is the responsibility of all organisations and staff to comply with the law and we can achieve this by ensuring that our staff are supported in and made aware of their individual and collective responsibilities and of any penalties for non-compliance.

2.0 LEGISLATION AND STANDARDS

IG is an overarching term used to describe all aspects of information management. This policy outlines our approach and intentions to fulfilling our statutory and organisational responsibilities in relation to the management of information. It will enable managers and staff to make correct decisions, work effectively and comply with relevant legislation and our own organisational aims and objectives.

A robust IG Framework provides a consistent way for NIPEC staff to deal with the many different pieces of legislation and standards that apply to effective management of information, i.e. how we source, hold, use, transfer, store, support access to and dispose of information. These include:

- General Data Protection Regulation (GDPR) 2016 / Data Protection Act 2018
- Freedom of Information (FOI) Act 2000
- Public Records Act (NI) 1923
- Disposal of Documents Order 1925
- Computer Misuse Act 1990
- Re-Use of Public Sector Information Regulation 2005
- Human Rights Act 1998
- Environmental Information Regulations 2004
- Public Interest Disclosure Act 1998
- Guidance from the Information Commissioners Office
- Good Management Good Records (GMGR) (February 2020)
- Code of Practice on Protecting the Confidentiality of Service User Information.

- Information Management Assurance Checklist (IMAC) 2018

This Policy should be considered alongside NIPEC's supporting set of policies and procedures covering key aspects of Information management including:

- Freedom of Information Policy
- Records Management Policy
- Data Protection Policy
- Incident Reporting Policy
- Data Protection Impact Assessment Policy
- Clear Desk and Screen Policy
- Accessible Formats Policy for the Provision of Information
- Publication Scheme
- Operational Procedure for Filing System
- Security of NIPEC Property and Personal Property
- Information Technology Ethical Code and Computer Usage Guidelines
- Business Continuity Plan
- Social Media Policy / Guidance
- ICT Security Policy

In addition, this policy should be considered alongside professional / organisational Codes of Conduct such as the Codes for the NMC and HSC Employees.

3.0 PURPOSE

The overall purpose of this Policy is to provide clear direction and guidance for staff in delivering the requirements of good IG practice. It acts as an overarching policy for all of NIPEC's IG related policies and aims to:

- Outline the approach to fulfilling our IG responsibilities;
- Ensure compliance with legal and regulatory frameworks is maintained;
- Provide a robust framework for preserving the confidentiality, integrity, security and accessibility of data, systems and information;
- Provide assurance that information is processed legally, securely, efficiently and effectively.

The policy sets out the approach to be adopted for managing NIPEC's information and informs our staff of the best practice for holding, using and transferring information both internally and externally. It seeks to ensure that our information and data is of the highest quality, accurate, easily accessible, relevant, understandable and complete.

4.0 SCOPE

The Policy supports the protection, control and management of information assets and covers all information held by NIPEC in all information systems, electronic and non-

electronic. It applies to all staff employed by NIPEC, Agency staff, third party contractors/service providers and any other individual or organisation processing information for or on our behalf.

IG covers all information held, and all information systems used to hold that information. This includes, but is not necessarily limited to, information:

- Stored on computers;
- Transmitted across internal and public networks such as email or the internet;
- Stored within databases;
- Printed or handwritten on paper, whiteboards etc.
- Stored on removable media such as iron keys etc.
- Stored on fixed media such as hard drives etc.
- Paper and electronic structure record systems
- Information recording and processing systems whether paper, electronic, video or audio records;
- Presented on visual and audio media, such as PowerPoint slides;
- Spoken during telephone calls and meetings or conveyed by any other method.

This Policy also covers all forms of information held and systems purchases, developed and managed by / or on behalf of NIPEC, and any individual directly employed or otherwise used by NIPEC, including, but not limited to:

- Information about members of the public;
- Non-employees on NIPEC premises;
- Staff and personal information;
- Organisational, business and operational information.

5.0 OBJECTIVES

The key objectives of this Policy are to assure that all organisational and corporate information handled or held by NIPEC:

- Exists within a policy and procedure framework compliant with best practice;
- Complies with all legislation, standards and guidance;
- Appropriately balances openness and confidentiality in the management and use of information;
- Has risks identified, managed and where possible mitigated;
- Is handled by NIPEC staff who are sufficiently trained and enabled to follow and promote best practice in regard to the management of information;
- Is used within a culture of continuous improvement through action planning, increasing awareness and providing training on the key issues.

6.0 BENEFITS

The benefits of a robust and fully implemented IG Policy include:

- Assurance that decisions are based on readily accessible high quality information;

- Assurance that information is held and managed securely by NIPEC;
- Reduction of risks associated with poor and unregulated systems and processes;
- Reduction of data losses and the negative impact such losses have on corporate image;
- Assurance that legislation, standards, guidance and all other Department of Health requirements are met;
- Support of corporate governance and underpinning of the assurance framework and corporate risk register;
- Assurance that information and information assets are managed in a coherent manner reducing duplication of effort and increasing availability;
- Construction of annual improvement plans, supported by appropriately prepared and knowledgeable staff members.

7.0 INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

Adherence to IG principles is a corporate responsibility across the whole organisation, for all staff whether employed on either a NIPEC permanent, bank, temporary or agency contract, and should focus on the ability of the organisation to capture, manage, preserve, store and deliver the right information to the right people at the right time.

The Department of Health seeks an annual assurance from HSC organisations in relation to their compliance with IG. This annual assurance, Information Governance Management Framework (2018), is shown at Appendix 1. It provides a high level summary of the key IG roles, policies, reporting and oversight arrangements, training and incident management processes in place within NIPEC. This framework is also used by BSO internal audit to assess our IG compliance on a periodic basis.

7.1 Roles, Responsibilities and Reporting Arrangements

The information governance roles and responsibilities within NIPEC are as follows:

- **NIPEC Council**
  The Council has overall responsibility to ensure compliance in all areas of IG and should receive an annual performance report from the SIRO highlighting any issues or concerns that may arise in relation to information governance including adverse incidents.

- **The Chief Executive**

  As NIPEC's Accounting Officer, the Chief Executive has ultimate responsibility for the delivery of this policy and subsequent policies and procedures.

- **Personal Data Guardian (PDG)**

  The PDG is responsible for protecting the confidentiality of patient and service-user information and facilitating appropriate information sharing including the

authorisation of data sharing agreements between NIPEC and other organisations.

- **Senior Information Risk Owner (SIRO)**

  The SIRO is a senior manager who has responsibility to ensure compliance with legislation through the development and monitoring of policies. They are supported in their role by the appointment of Information Asset Owners (IAOs).

  The SIRO annually reviews information risk and is responsible for ensuring that identified information security risks are followed up and incidents managed effectively. The SIRO will document any and all security breaches, information loss or unauthorised disclosure, and other risks associated with information management will be documented and managed in line with NIPEC's overall adverse incident reporting processes.

- **Information Governance Lead**

  The Head of Corporate Services is the NIPEC Information Governance Lead. Key responsibilities include:

  - Ensuring there is senior level awareness of and support for Information Governance arrangements;
  - Ensuring the implementation of necessary governance improvements within NIPEC with the support of the senior team;
  - Providing direction and guidance when formulating, revising and implementing relevant policies and promoting IG in the organisation;
  - Monitoring and reporting on performance in information handling;
  - Ensuring that the annual Department of Health IMAC and improvement action plans are prepared for approval;
  - Ensure appropriate training is made available to staff and completed as necessary to support their duties;
  - Liaising with other organisations including the NIPEC Data Protection Officer (DPO) (service provided by BSO) in relation to their Information Governance arrangements to support best practice
  - Provide a focal point for the discussion and resolution of any Information Governance issues that may arise in NIPEC;
  - Supported by the DPO, reporting to NIPEC Council all data breaches and serious incidents relating to information governance, and the Information Commissioner's Office (ICO) when required.

  Note: *NIPEC's Head of Corporate Services (HCS) acts as the PDG and SIRO, as well as the organisation's Information Governance Lead. NIPEC's small structure requires that one individual is responsible for these roles to maximise efficiency however independent advice and guidance is available from the DPO service provided by BSO)*

- **Information Governance Group**

  The Information Governance Group exists to ensure that NIPEC adheres to all legislation, policies, procedures and guidance relating to the handling and management of information within the organisation. Key duties include:
  - Develop policies and procedures to support the effective use of information in NIPEC;
  - Review IG related policies on a regular basis;
  - Maintain and review a comprehensive Information Asset Register;
  - Ensure compliance with IG policies;
  - Identify training and development for all staff to ensure they discharge their IG responsibilities appropriately;
  - Develop and monitor action plans for the management of IG;

- **Information Asset Owners (IAOs)**

  There are a number of staff in NIPEC trained as IAOs and each is responsible for certain information assets. IAOs manage and address associated risks to the information assets they 'own' and provide assurance to the SIRO on the security and management of those assets. The IAO should:

  - Know who has access to the asset and why;
  - Ensure access is monitored and auditable;
  - Understand and address risks to the asset and provide assurance to the SIRO.

- **Information Asset Administrators (IAAs)**

  IAAs ensure that policies and procedures are followed, recognise any security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. In NIPEC there are nominated staff that maintain certain information assets, such as the procurement records.

- **All Staff**

  All staff must undertake mandatory e-learning programmes to update their knowledge on policies, procedures and legislation relevant to NIPEC and information management and governance. In the event of an issue relating to Information Governance arising, it is the responsibility of all staff involved to ensure that appropriate information management policies are followed.

7.2 Supporting Staff

All staff have responsibility for the information and data held and used by them. Clear accountability arrangements will ensure that our information assets are processed and managed accordingly and corporate policies, processes and

controls are monitored for compliance under a defined Information Governance Management Framework.

This approach ensures that staff adhere to best practice guidance, meet their role and responsibilities and follow the appropriate legislation. The information provided within this Policy, along with any related policies and procedures, will inform staff of any changes that need to be made and how they should carry out their duties adhering to such.

We are committed to maintaining an open and supportive environment in which any arising issues or concerns relating to information governance can be immediately addressed, with corrective measures implemented swiftly and processes changed accordingly. This culture within NIPEC further mitigates the risks associated with the handling and processing of information.

7.3 Communication

The Department of Health has developed and communicated clear requirements for information handling to ensure that it is:

- **Held** securely and confidentially
- **Obtained** fairly and efficiently
- **Recorded** accurately and reliably
- **Used** effectively and ethically
- **Shared** appropriately and lawfully.

These above requirements are followed accordingly in terms of the use, storage and sharing of information throughout our organisation. These standards have been communicated to all staff via relevant policies and training to ensure compliance and that all staff are aware of Information Governance processes and procedures. This is an essential action to ensure we effectively meet the aims and objectives set out in this strategy.

7.4 Mandatory Training

We will ensure that all staff have the knowledge and skills needed relevant to their role and level of responsibility within the organisation, and make sure that appropriate training and information is available to up-skill existing staff and train new members of staff.

Completion of the regionally agreed Information Governance e-learning training programme is mandatory for all NIPEC staff and must be renewed every 3 years. This training covers areas such as Data Protection, Freedom of Information and Records Management.

In addition, staff are required to complete and renew the following HSCNI e-learning training programmes:

- IT Security *(every 3 years)*
- Cyber Security (every *2* years)
- Risk Management Awareness *(every 2 years)*
- Fraud Awareness *(every 2 years)*

Specific training for SIROs and IAOs is also undertaken by relevant staff. This covers:

- The role of the SIRO and IAO;
- Understanding what information assets are;
- Maintaining an information asset register;
- Developing an information security policy and supporting systems;
- Managing Information Governance incidents;
- Understanding data flow mapping;
- Understanding forensic readiness;
- Understanding privacy impact assessments and the annual SIRO report.

It is the responsibility of Line Managers to support training and provide assurance that staff are aware of and appropriately prepared for their responsibilities under Information Governance.

7.5 Implementation and Performance Monitoring

NIPEC's Information Governance Group will oversee, on behalf of the organisation, the effective implementation of this and any related policies and procedures, and that these are relevant, understandable, and available and complied with by all staff.

Performance will be monitored annually against a set of standards and targets in the form of the Department of Health's Information Governance Management Framework (2018) and any learning resulting from audits of NIPEC's information governance arrangements undertaken by BSO's Internal Audit. Staff compliance will also be monitored by existing appraisal mechanisms to ensure that staff are performing to the required standards.

Where a member of staff is failing to comply with IG requirements, every effort will be made to ensure they are supported to improve his/her practice. Where a staff member continues to fail to comply with this or any NIPEC policy or procedure, relevant disciplinary action will be taken.

8.0 SUMMARY AND CONCLUSION

IG is a vital and integral part of our overall work programme helping the organisation and our staff to manage and control our information, ensuring compliance with our statutory and legislative duties and that accountability, standards, policies and procedures are developed, implemented and maintained.

Implementation of this Policy, and related policies and procedures, will ensure that we have the appropriate framework in place to meet legislative and organisational requirements.

9.0 EQUALITY STATEMENT

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998.

The screening has identified some minor equality impacts and outlines the way these will be addressed. No significant equality implications have been identified therefore the policy will not be subject to an equality impact assessment.

The equality screening has been published and can be accessed at http://www.hscbusiness.hscni.net/services/2166.htm

10.0 REVIEW

We are committed to ensuring that all policies and procedures are kept under review to ensure they remain compliant with relevant legislation and guidance.

This policy is based on a regional HSC policy. It will be monitored and reviewed in December 2023 or sooner if a revised HSC policy is issued.

Appendix 1

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	• IG Lead • Senior Information Risk Owner (SIRO) • Personal Data Guardian	Due to the size of NIPEC as a small ALB a number of roles are amalgamated within the Head of Corporate Services (HCS) duties. In regard to Information Governance, IG Lead, SIRO and Personal Data Guardian are part of the HCS post holder's duties. NIPEC's DPO service is provided under SLA, by BSO.
Key Policies	• Over-arching IG Policy • Data Protection Act / Confidentiality Policy • Organisation Security Policy • Information Lifecycle Management (Records Management) Policy • Corporate Governance Policy • Freedom of Information policy • Risk Management • Information Quality	NIPEC has an Information Governance Policy (*incorporating its Information Management Governance Framework*) in place. NIPEC has access to a regionally agreed Shared Data Agreement which can be used as and when required for the sharing of service user / employee information. Also, the following policies are in place: • Data Protection Policy • Provision, usage and security of NIPEC smart phones Policy • ICT Security Policy • Social Media Guidance • Information Technology Ethical Code and Computer Usage Guidelines • Whistle Blowing Policy • Freedom of Information (FOI) Policy • Publication Scheme • Records Management • Risk Management Strategy and Action Plan • Performance Management Framework • Accessible Formats Policy on the Provision of Information • Business Continuity Plan • Security of NIPEC Property and Personal Property

		• Staff Code of Conduct Policy • Information Asset Register.
Key Governance Bodies	IG Board/Forum/Steering Group	NIPEC has in place an Information Governance Group with agreed Terms of Reference. This group's membership is drawn from across the organisation. Also, NIPEC is a member of the regional HSC Information Governance Group. NIPEC has in place a Council and an Audit and Risk (A&R) Committee, both of which meet at least four times per year. All Internal Audit Risk reports are taken to the A&R Committee for consideration.
Resources	Details of key staff roles and dedicated budgets	NIPEC has in place named staff responsible for the following positions: • Senior Information Risk Owner (SIRO) • Personal data Guardian (PDG) • Information Asset Owners (IAOs) • Information Asset Administrators (IAAs).
Governance Framework	Details of how responsibility and accountability for IG is cascaded through the organisation	The NIPEC Information Governance Policy articulates: • Role of Council • Role of the Chief Executive • Role of the SIRO and PDG • Role of the Information Governance Lead • Staff roles and responsibilities • Information Asset Register • Annual Information Governance Management Assurance.
Training & Guidance	• Training for all staff • Training for specialist IG roles	NIPEC uses regionally developed e-learning packages, via the HSC Leadership Centre website, including: • Information Governance • IT Security • Cyber Security • Display Screen Equipment (DSE)

		• Confidentiality of Service User Information • Fraud Awareness. The SIRO and IAOs have all received formal training on their roles and responsibilities. A review of staff training is part of the annual staff Appraisals system. A number of information leaflets and guidance have been developed and issued to staff, including: • Information Governance leaflet • Privacy Statement • Information Security – top tips
Incident Management	Documented procedures and staff awareness	NIPEC has in place the following policies/procedures: • Complaints Policy • Serious Adverse Incident Policy • Health and Safety Policy • Risk Management and Action Plan Policy • Disciplinary Policy and Procedures • Fraud Response Policy and Plan. The above policies and procedures are reviewed and updated on a rolling programme of review basis.