NIPEC/24/16
(replacing NIPEC/20/21)

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Information Governance Policy

(incorporating the Information Governance Assurance Framework)

October 2024

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

James House
2-4 Cromac Avenue
BELFAST
BT7 3EA

Tel: 0300 300 0066

https://nipec.hscni.net

Developed by:	Business Manager
Approved by / date:	**BTM:** 12th January 2021; 12th November 2024; **Council:** 4th December 2024
Date of next Review:	October 2029
Equality Screened by / date:	August 2024

Contents

Section		Page
1.0	Introduction	**3**
2.0	Purpose	**3**
3.0	Scope	**4**
4.0	Policy Statement	**4**
5.0	Roles and Responsibilities	**6**
6.0	Monitoring Compliance	**6**
7.0	Non-Compliance	**6**
8.0	Review	**7**
9.0	Equality Statement	**7**
Appendix 1	Information Governance Assurance Framework	**8**

1.0 INTRODUCTION

Information Governance (IG) describes the approach within which accountability standards, policies and procedures are developed, implemented and maintained to ensure that all types of information are processed appropriately, securely and in line with current legislation. It has five fundamental aims:

- To support the provision of a high-quality service by promoting the effective and appropriate use of information;
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- To provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards;
- To help NIPEC to understand our own performance and manage improvement in a systematic and effective way; and
- To ensure compliance with our statutory and legislative duties.

Information held by NIPEC is one of our most valuable assets. It is the responsibility of all 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.

It is therefore essential that all information is managed effectively within a robust framework, in accordance with best practice and legislative/policy requirements, as set out in NIPEC's Information Governance Assurance Framework (Appendix 1).

2.0 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 aims to:

- Outline the approach to fulfilling our IG responsibilities;
- Ensure compliance with legal and regulatory frameworks is maintained;
- Establish 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 IG requirements set out within this policy and other policies and procedures are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used and ensuring that information is available where and when it is needed.

3.0 SCOPE

The Policy supports the protection, control and management of information and information assets. The policy will cover all information held by, or on behalf of, NIPEC, in all information systems, electronic and non-electronic, as well as records whether held electronically or manually. It applies to all staff employed by NIPEC, Agency staff, third party contractors/service providers and any other individual or organisation acting on our behalf.

IG covers all information held, and all information systems purchased, developed and managed by/or on behalf of NIPEC, and any individual directly employed or otherwise used by NIPEC to hold that information on any media, and in any format.

This Policy covers all forms of information held, including personal identifiable data as defined in data protection legislation, as well as non-personal identifiable data (such as organisational, business and operational information).

4.0 POLICY STATEMENT

NIPEC will ensure:

- **Openness:**

  - Establish procedures for handling requests under provisions of Freedom of Information (FOI) and Subject Access Requests;
  - Undertake regular assessments of IG policies and arrangements;
  - Ensure that publicly disclosable information about the organisation and its services is readily available, in line with relevant legislation and the Information Commissioner's Office (ICO) model publication scheme;
  - Ensure that Privacy Notices are published to advise the public according to its obligations under the UK GDPR;

- **Legal Compliance:**

  - NIPEC will establish and maintain policies to ensure compliance with relevant legislation including but not restricted to data protection, FOI and Environmental Information legislation and guidance;

- **Information Security:**

  - NIPEC will ensure that information security is embedded into relevant policies and procedures;

- Establish and maintain appropriate incident reporting procedures for the reporting, monitoring and investigation of all actual and/or potential breaches of confidentiality and security;
- promote effective confidentiality and security practice to ensure all staff and third-party associates adhere to this policy, and associated policies and procedures;

- **Information Quality Assurance:**

  - NIPEC will ensure that the information they hold is of the highest quality;
  - Establish and maintain procedures for information quality assurance;
  - Undertake regular audits of information quality and records' management arrangements;
  - Promote information quality and effective records management through policies, staff awareness and training;

- **Information Risk Management:**

  - That risks are identified, managed and where possible mitigated;
  - All appropriate risks will be recorded in NIPEC's Corporate Risk Register as documented in NIPEC's Risk Management Strategy;
  - Risk assess all information assets and information flows to determine that appropriate, effective and affordable IG controls are in place;
  - The SIRO will be made aware of all information risk assessments and approve any identified risk mitigation plans.

- **Records Management:**

  - That a record is managed through its life cycle from creation or receipt, through maintenance and use to disposal;
  - Adhere to the regional retention schedule, Good Management Good Records (GMGR);
  - Is handled by NIPEC staff who are sufficiently trained and enabled to follow and promote best practice in regard to the management of information;
  - To promote records' management through policies/procedures and training;

- **Training:**

  - That training is delivered for different roles as appropriate;
  - All staff complete mandatory training at induction and on a 3-yearly cycle thereafter;
  - All staff have access to relevant IG policies and procedures.

5.0 ROLES AND RESPONSIBILITIES

Responsibilities are as set out within NIPEC'S Information Governance Assurance Framework in Appendix 1.

NIPEC operate an internal Information Governance Group with representatives from both the professional and corporate teams. The role of this Group is set out within Appendix 1.

6.0 MONITORING COMPLIANCE

Monitoring of performance is set out within subsequent policies, namely:

- Data Protection Policy
- Freedom of Information Policy
- Records Management Policy
- Adverse Incident Reporting Policy

7.0 NON-COMPLIANCE

A failure by staff to adhere to the relevant legislation, this policy and any associated procedures may result in disciplinary action against the staff member, in line with management structures.

Staff should be aware that they may be personally liable for prosecution for non-compliance with this policy and any associated procedures (in relation to the use of ICT equipment including the use of the internet and email), and open to claims for damages if their actions are found to be in breach of legislation.

Where appropriate, breaches of this policy may be reported to the PSNI, ICO or other public authority for further investigation.

8.0 REVIEW

This policy (and framework) shall be reviewed regularly, and as a minimum:

- every 5 years; or
- following receipt of new information; or
- following updates to applicable legislation, guidance or best practice; or
- upon implementation of new agreements which may affect the policy/framework.

9.0 EQUALITY STATEMENT

This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

APPENDIX 1

NIPEC INFORMATION GOVERNANCE ASSURANCE FRAMEWORK

Contents

Section		Page
1.0	Introduction	**9**
2.0	General Principles	**9**
3.0	Annual IG Assurance	**10**
4.0	Information Governance Training	**10**
5.0	Roles, Responsibilities and Reporting Arrangements	**10**
6.0	Information Security Incident Management	**12**
7.0	Data Protection Impact Assessments	**13**
8.0	Information Asset Register	**13**
9.0	Freedom of Information	**13**
10.0	Confidentiality of Personal Data	**13**
11.0	Records Management	**13**
12.0	Third Party Contracts (including within HSC)	**14**
13.0	Information Governance Improvement Plan	**14**

1.0 INTRODUCTION

NIPEC's Information Governance Assurance Framework (IGAF) brings together all statutory, mandatory and best practice requirements concerning information management. The requirements are set out in the Department of Health (DoH) Information Management Assurance Checklist (IMAC) as a roadmap to enable NIPEC to plan and implement standards of practice, to measure and report compliance on an annual basis.

NIPEC's performance against the IMAC is mandated by and reported to DoH annually and forms part of NIPEC's assurance processes.

The Framework sets out an overarching summary for the IG agenda in NIPEC. In particular, this document looks at the operational and management structures, roles, responsibilities, systems, policies and audit controls that are used to ensure such issues are addressed within NIPEC. This structured approach relies on the identification of information assets and assigning 'ownership' of assets to senior staff.

2.0 GENERAL PRINCIPLES

Information Governance relates to how NIPEC handles its information, particularly personal information. It is important for staff to understand their own responsibility for recoding information to a consistently high standard and for keeping it secure and confidential when required to.

Listed below are some of the legislation, policies, standards, guidelines and best practice guidance applicable to this Framework:

- The Data Protection Act 2018
- UK General Data Protection Regulation
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Common Law Duty of Confidentiality
- The Caldicott Guardian Manual
- The Human Rights Act 1998
- The Public Records Act (NI) 1923
- The Disposal of Documents Order 1925
- The Re-use of Public Sector Information Regulations 2015
- The Electronic Communications Act 2000
- The Equality Act 2010

- The Public Interest Disclosure Act 1998
- The Computer Misuse Act 1990
- The Crime and Disorder Act 1998
- The Investigatory Powers Act 2016
- DoH Good Management Good Records (GMGR)
- Health and Social Care (HSC) Code of Conduct
- DoH Code of Practice on Protecting the Confidentiality of Service User Information
- DoH Information Management Assurance Checklist (IMAC)
- Guidance from the Information Commissioner's Office

NIPEC will maintain a suite of policies, in line with the above, including:

- Information Governance Policy
- Freedom of Information Policy
- Data Protection Policy
- Records Management Policy
- ICT Security Policy

3.0 ANNUAL IG ASSURANCE

NIPEC's compliance against the IMAC is completed by its SIRO (Head of Corporate Services), with assurance thereafter signed off by the Chief Executive.

NIPEC seeks to maintain compliance with the IMAC on an annual basis.

4.0 INFORMATION GOVERNANCE TRAINING

The development of an IG culture within NIPEC is fundamental to the success of delivering the Framework. Basic IG training is available to all staff and NIPEC Council members via the regional e-learning package.

IG training is incorporated into NIPEC's mandatory training programme. It is mandatory for all staff to complete the e-learning training every 3 years. NIPEC's Business Team monitor compliance with this requirement.

Additional training is provided when required, for example, Information Asset Owner training, which is offered to all staff. Training is also undertaken to those in more specialist roles such as SIRO (Senior Information Risk Owner) and Personal Data Guardian training.

5.0 ROLES, RESPONSIBILITIES AND REPORTING ARRANGEMENTS

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

- **The Audit & Risk Committee**

  Supports NIPEC Council with regard to their responsibilities for issues of risk, control, governance and associated assurances. Specifically, the Committee are tasked with oversight of the establishment and maintenance of an effective system of integrated governance, risk management and internal control, across the whole of the organisation's activities that supports the achievement of the organisation's objectives.

- **The Chief Executive**

  As NIPEC's Accounting Officer, the Chief Executive has responsibility for maintaining a sound system of internal governance that supports the achievement of the organisation's policies, aims and objectives, including for the delivery of this policy and subsequent policies and procedures.

- **Personal Data Guardian (PDG)**

  The PDG is a senior person within NIPEC who is responsible for ensuring that the personal data about those who use the organisation's services is used legally, ethically and appropriately, and that confidentiality is maintained.

- **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 NIPEC's 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 Asset Owners (IAOs)**

  Are senior individuals involved in running the business of the organisation. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good, and provide written input to the SIRO on the security and use of their asset.

- **Data Protection Officer (DPO)**

  NIPEC'S DPO service is provided by the Business Services Organisation via an annual SLA. In line with Article 39 of the UK GDPR, the DPO should carry out the following tasks:

  - Inform and advise NIPEC and its staff of their obligations pursuant to data protection legislation;
  - Monitor compliance with data protection legislation and this framework in relation to the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in processing operations;
  - Provide advice where requested as regards the data protection impact assessment;
  - Support NIPEC to co-operate with the ICO; and
  - Act as the point of contact for the ICO on issues relating to processing.

- **Managers**

  Managers are responsible for implementing this framework within their team structure.

- **All Staff**

  Are responsible for familiarising themselves with, and adhering to, all parts of this framework.

- **Information Governance Group**

  NIPEC operates an internal Information Governance Group with representatives from both the corporate and professional teams. As per its terms of reference, the role of IG Group is:

  - To advise the Chief Executive regarding how NIPEC can maximize the Information Governance and Communications/ IT contribution to the operational and strategic roles and functions of the organisation;
  - To provide assurance to the Chief Executive that NIPEC has adequate processes in place to manage its information;
  - To ensure that NIPEC fulfils its statutory obligations under UK GDPR, Data Protection Act and other relevant legislation;
  - To provide oversight of data protection and GDPR for all website, social media and communication activity on behalf of NIPEC;
  - To ensure that the needs of staff are identified and met in regards to training.

6.0 INFORMATION SECURITY INCIDENT MANAGEMENT

The SIRO must be informed immediately of all information security incidents involving the unauthorised disclosure of person identifiable data/information.

The SIRO will report such incidents to the DPO for consideration and to agree any necessary actions. In the absence of the SIRO, such an incident should be reported directly to the DPO by email, dpo.bso@hscni.net by a senior member of NIPEC staff.

A key function of the IG Group is to monitor and review incidents, actual and potential, and ensure that remedial and preventative action is taken. Information incident reporting will be in line with NIPEC's Adverse Incident Reporting Policy.

7.0 DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The impact of any proposed changes to the processes and/or information assets need to be assessed to ensure that the confidentiality, integrity and accessibility of personal data are maintained.

The DPO should be consulted during the completion of any DPIA in order that they can provide independent advice.

Please refer to the Data Protection Impact Assessment Policy for more detailed guidance on completion of DPIAs.

8.0 INFORMATION ASSET REGISTER (IAR)

Each Information Asset Owner is responsible for identifying what information assets are held within their area of responsibility and to ensure that this is documented in NIPEC's IAR.

The IAR should include type of asset, format, location, backup information and license details. Ownership should be agreed and documented for each of the assets along with a risk assessment.

The IAR should be reviewed regularly to ensure it remains fit for purpose.

9.0 FREEDOM OF INFORMATION

NIPEC will ensure compliance with the Freedom of Information Act 2000 and ICO guidance. This is set out in NIPEC's Freedom of Information Policy.

10.0 CONFIDENTIALITY OF PERSONAL DATA

NIPEC will ensure that all personal data it holds is managed in accordance with data protection legislation. This is set out in NIPEC's Data Protection Policy.

11.0 RECORDS MANAGEMENT

NIPEC is committed to a systematic and planned approach to the management of records from their creation to their disposal. NIPEC will ensure that it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner and can dispose of the information efficiently when it is no longer required. This process is set out in NIPEC's Records' Management Policy.

12.0 THIRD PARTY CONTRACTS (INCLUDING WITHIN HSC)

For business purposes, third parties will have access to NIPEC's information assets, e.g. payment of salaries and expenses via regional systems. This can result in third party staff having significant access to personal/sensitive personal data.

Suitable clauses must be included in contracts and service level agreements (SLAs) with third parties who have access or process data on behalf of NIPEC. These should be in line with data protection requirements and any other applicable legislation. When sharing information within HSC, an agreed template (e.g. a data access agreement) should be used to ensure that the requirements of law, policy and guidance are being met.

The SIRO and IAOs must take all reasonable steps to ensure third parties to whom personal data is disclosed comply with their contractual obligations to keep personal data secure and confidential. Risk assessments should be carried out prior to any agreement being made with a third party to evaluate any threats from third party operatives, proportionate to the potential risk.

IAOs should ensure that all existing contracts are monitored and are included on NIPEC's contracts' register.

13.0 INFORMATION GOVERNANCE IMPROVEMENT PLAN

An essential element of the IMAC is that NIPEC continues to monitor, and where appropriate, improve performance in relation to IG. This is achieved via completion of the annual self-assessment against the IMAC.

To support this further, NIPEC carries out an annual self-assessment against the IG assurance map and any gaps in the process or potential improvements are included

in an Annual Assurance Maps action plan. The plan is presented to NIPEC's Audit & Risk Committee for approval, along with mid-year and yearend updates.