NIPEC/16/08

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Information Governance Strategy incorporating the Information Governance Framework

Date of Publication: April 2016

Ownership: NIPEC

Review Date: April 2020

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

www.nipec.hscni.net

1.0 Introduction

The provision of health and social care, to a large extent, is driven by the quality of data that is available at the point of care and that which is used to make decisions that impact upon people and society. As the information and communications technology (ICT) Management Controls Assurance Standards set out: '*Good quality data and information together with well-implemented and managed technologies, can greatly improve all aspects of organisational performance. Conversely, poor quality data and information and badly managed technologies can make existing problems more difficult*'[1].

Information Governance assures the necessary safeguards for and appropriate use of information, referring to the approach within which accountability, standards, policies and procedures are developed, implemented and maintained. This ensures that all types of information are sourced, held and used appropriately and legally. Implementation of a robust Information Governance Strategy will deliver improvements in information handling within NIPEC, and will follow the guidelines set out in the Information Management Controls Assurance Standards issued in July 2013 by the Department of Health, Social Services and Public Safety (DHSSPS)[2].

NIPEC adheres to *Good Management Good Records* (GMGR)[3] which incorporates the DHSSPS advice and guidance on records management. It includes a retention and disposal schedule, prepared in accordance with the Public Records Act (NI) 1923 and the Disposal of Documents Order 1925. These guidelines will be followed and incorporated in the production of the Information Governance Strategy within NIPEC.

This Information Governance Strategy should be considered alongside the supporting set of existing Information Management and ICT Management policies and guidance held within NIPEC:

Information Management

- Freedom of Information Request Procedures
- Records Management Policy Statement
- Retention and Disposal Schedule
- Data Protection Policy Statement
- Accessible Formats Policy for the Provision of Information
- Publication Scheme
- Public Involvement Strategy

[1] Department of Health, Social Services and Public Safety. (2009). *ICT Management Controls Assurance Standards.* Belfast, DHSSPS.
[2] Department of Health, Social Services and Public Safety. (2013). *Information Management Controls Assurance Standards.* Belfast, DHSSPS.
[3] Department of Health, Social Services and Public Safety. (2011). *Good Management Good Records.* Belfast, DHSSPS.

- Operational Procedure for Manual and Electronic Filing System
- Security of NIPEC Property and Personal Property
- Disciplinary Procedure

ICT Management

- Information Technology Ethical Code and Computer Usage Guidelines
- IT Contingency Policy
- Business Continuity Plan
- Social Media Policy / Guidance
- Website Information Procedure
- Information and Communication Technology (ICT) Strategy
- ICT Security Policy

Note: This list is not exhaustive. There are further policies outside of Information Management and ICT Management that include related Information Governance guidance.

2.0 Purpose

The overall purpose of the NIPEC Information Governance Strategy is to provide clear direction and guidance to the organisation in delivering the requirements of good Information Governance practice alongside associated policies. The strategy will assist in establishing and maintaining a robust and effective Information Governance Framework that allows NIPEC to fully meet its strategic duties ensuring that overall corporate compliance is met both in relation to legal and statutory obligations and all relevant codes of practice. The Information Governance Strategy and supporting policies ensure that NIPEC's information and data is of the highest quality in relation to being accurate and easily accessible, relevant, understandable and complete. This will essentially be of benefit to all staff by providing a document that will assist and inform them of the best practice for holding, using and transferring information both internally and externally[4].

3.0 Scope of Information Governance

The Information Governance Strategy applies to all staff employed within NIPEC, setting out a framework to meet organisational objectives and responsibilities. It will be used as the vehicle for improving Information Governance practice within NIPEC. This strategy has a timeframe of four years covering the period from April 2016 – April 2020.

4.0 Information Management within NIPEC – An Overview

Information Management is a corporate responsibility across senior management roles to front line staff and should focus on the ability of the organisation to capture,

[4] NHS Connecting for Health. (2010). *Health and social care staff members: What you should know about Information Governance.* London, The Stationery Office .

manage, preserve, store and deliver the right information to the right people at the right time[5].

A range of relevant legislation governs NIPEC in the production and implementation of an Information Governance Strategy. A list and explanation of the legislation can be found at Appendix 1, page 18. In addition to legislation, the Information Management Controls Assurance Standards (2013)[6] set the principles as to how information should be managed. Organisations are required to carry out self-assessments of compliance against the criteria, to determine whether their information is managed correctly. The ICT Controls Assurance Standards (2009)[7] require the organisation to have a consistent, comprehensive and systematic approach to the management of electronic information and systems.

NIPEC holds and uses different types of information; this information varies between electronic and manual format. A NIPEC information map can be found at Appendix 2, page 19. Note: This map is not exhaustive.

Much of NIPEC's information is used and shared internally for organisational purposes and for the benefit of informing staff of any changes to policies, procedures or legislative requirements. Under the Freedom of Information Act 2000, non-confidential public facing data and information can be accessed through NIPEC's websites. This data includes information on NIPEC's current work and projects, staff, and links to other related sites. NIPEC uses, publishes and presents data in a way that protects the rights of all those involved. NIPEC's Publication Scheme ensures information is available to the public as part of normal business activities.

The NIPEC computer and filing rooms have passcode keypads installed. Human Resources, Payroll, Travel and Subsistence (HRPTS), email accounts and records are also password protected. NIPEC stores minimal registrant information for purposes of contact and any that is held is with the consent of the individual. Effective arrangements are in place to protect the security and quality of all NIPEC's sensitive information, in line with legislative requirements.

NIPEC recognises the need to identify, monitor and mitigate any risks that arise within the organisation, based on the level of sensitivity of information.
A descriptor for categorising risks can be found at Appendix 3, pages 20-21. These definitions will enable staff to classify and group restricted data (high risk), confidential data (medium risk) and public data (low risk), to apply the appropriate

[5] *What is Information Management? Available at: http://www.aiim.org/What-is-Information-Management (Accessed: 01/10/15).*
[6] Department of Health, Social Services and Public Safety. (2013). *Information Management Controls Assurance Standards.* Belfast, DHSSPS.
[7] Department of Health, Social Services and Public Safety. (2009). *ICT Management Controls Assurance Standards.* Belfast DHSSPS

directions from supporting organisational policy. Also included at Appendix 3 are examples of how this is applied in practise.

5.0 Benefits

The benefits of a robust and fully implemented Information Governance Strategy within NIPEC are summarised below:

- 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[8]
- reduction of data losses and the negative impact such losses have on corporate image
- assurance that legislation, standards, guidance and all other DHSSPS 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 year on year improvement plans, supported by appropriately prepared and knowledgeable staff members.

6.0 Objectives

The key objectives of this Information Governance Strategy 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[9]
- 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 an Information Governance culture of continuous improvement through action planning, increasing awareness and providing training on the key issues.

[8] *5 Benefits of Creating an Information Governance Strategy. Available at: http://www.consultparagon.com/blog/5-benefits-of-creating-an-information-governance-strategy (Accessed: 23/11/15).*

[9] *What is Information Governance? Available at: http://systems.hscic.gov.uk/infogov (Accessed: 23/11/15).*

7.0 Information Governance Framework

The Information Governance Framework enables NIPEC to set out and promote a culture of good practice around the processing of information and use of information systems throughout the organisation. It ensures that information is handled to meet ethical and quality standards in a secure manner[10]. NIPEC requires all employees to comply with the legislation, policies, procedures and guidelines that are in place to implement this framework. The framework defines roles, responsibilities and mandatory training that all staff must undertake as part of their duty. It also provides assurance that appropriate safeguards are in place[11].

The structure and management arrangements of this framework can be found at Appendix 4, pages 22-24.

7.1 Information Governance Policy Statement

This strategy is supported by a group of Information Management and ICT Management policies, which have been identified. All policies and guidance relating to Information Governance are reviewed and updated to ensure they comply with legislative requirements.

7.2 Roles, Responsibilities and Reporting Arrangements

The information governance roles and responsibilities within NIPEC are distributed as follows;

- **The Chief Executive**

As NIPEC's Accounting Officer, the Chief Executive has a duty to ensure that NIPEC complies with its statutory obligations and directives from the DHSSPS. He/she holds the primary responsibility to ensure the identified Information Governance Strategy and Management Framework are effectively adhered to.

- **NIPEC Council**

The membership of the Council consists of the Chief Executive of NIPEC, nine professional members (including Chair), the Chief Nursing Officer, DHSSPS and six lay members. NIPEC Council monitor and oversee any issues or concerns that may arise in relation to information governance. The Chief Executive will update the Council members each quarter in relation to action plans and implementation of the strategy and framework.

[10] NHS Connecting for Health. (2010). *Health and social care staff members: What you should know about Information Governance.* London, The Stationery Office .

[11] Information Governance Framework. Available at: https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/info-gov-framework. (Accessed: 23/11/15).

- **Audit and Risk Committee**

The Audit and Risk Committee is comprised of NIPEC representatives, representatives from the NIAO, External Auditors and the Internal Auditors, a representative from the Business Services Organisation, and four non-executive members of Council. The responsibilities of this committee lie with the independent review of the systems of corporate governance, risk management, internal control and external audit processes. The Audit and Risk Committee report to NIPEC Council if an issue arises, with progress formally reviewed each quarter.

In NIPEC the Head of Corporate Services (HCS) occupies both the roles of the Personal Data Guardian (PDG) and Senior Information Risk Owner (SIRO). The HCS has also been identified as the overall Information Governance Lead. NIPEC's small structure requires that one individual is responsible for these roles to maximise efficiency.

- **Personal Data Guardian (PDG)**

The PDG holds the responsibility for ensuring that NIPEC adheres to the highest practical standards for handling personal data. The PDG protects the security and confidentiality of information and enables appropriate information sharing which includes authorising all data sharing agreements between NIPEC and other organisations.

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

The SIRO manages information risk at board level, advises the Accounting Officer on the information risk aspect of the Governance Statement and owns the overall information risk and risk assessment processes. The SIRO annually reviews information risk and is responsible for ensuring that identified information security risks are followed up and incidents managed effectively.

- **Information Governance Lead**

The role of the Information Governance Lead within NIPEC is to develop and maintain documentation that demonstrates commitment to and ownership of Information Governance responsibilities. This strategy with supporting policies and procedures ensures compliance with this.

Other responsibilities of the Information Governance Lead include to:

- ensure staff awareness of Information Governance arrangements
- ensure the implementation of necessary governance improvements within NIPEC
- provide direction and guidance when relevant policies are established and promoted

- form working groups to coordinate the Information Governance responsibilities required by staff members
- ensure appropriate training is made available to staff and completed as necessary to support their duties
- liaise with other organisations in relation to their Information Governance arrangements to support best practice
- monitor information handling
- provide a focal point for the discussion and resolution of any Information Governance issues that may arise in NIPEC.

- **ICT and Governance Group**

The ICT and 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.

- **Information Asset Owners (IAOs)**

There are nominated staff in NIPEC that have been trained as IAOs and are responsible for certain information assets. The main role of each IAO is to manage and address associated risks within their area and to provide assurance and support to the SIRO on the management of the identified information assets.

- **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 manage certain information assets such as the Freedom of Information Requests and Procurement.

- **All Staff**

As part of their training, 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 arising, relating to Information Governance, it is the responsibility of all staff involved to ensure that appropriate information management policies are followed including a relevant risk assessment.

7.3 Leadership

Leadership is essential in creating a successful and operative Information Governance culture within NIPEC. Robust leadership will ensure that the Information

Governance Strategy and Action Plan are implemented correctly by all staff across the organisation[12].

As mentioned above, The Head of Corporate Services (HCS) has been nominated as the overall Information Governance Lead. It is essential however that each member of staff takes ownership and responsibility of the information they hold and use in order to achieve effective compliance with all states and codes of practice.

7.4 Supporting Staff

As stated above, staff will have responsibility for the information and data held and used by them. Clear accountability arrangements will ensure that NIPEC's information assets are processed and managed accordingly. Within the organisation this means that corporate policies, processes and controls will be monitored for compliance under a defined Information Governance Management Framework[13]. This approach ensures that all NIPEC staff members adhere to best practice guidance and perform under the identified Information Governance Code of Conduct GMGR[14]. The information provided within this document, along with any related policies and procedures, will inform supporting staff of any changes that need to be made and how they should carry out their duties adhering to such.

NIPEC is committed to maintaining an open and supportive environment in which any arising issues or concerns relating to 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.

7.5 Communication

The DHSSPS 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.[15]

The above requirements are followed accordingly by NIPEC in terms of the use, storage and sharing of information throughout the organisation. These standards

[12] *Leadership, governance and strategy. Available at: http://systems.hscic.gov.uk/qipp/mobile/support/leadership/index_html#leadership-and-governance (Accessed: 23/11/15).*

[13] Hagmann, J. (2013). Information governance – beyond the buzz. *Records Management Journal*, 23(3), pp.228-240.

[14] Department of Health, Social Services and Public Safety. (2011). Good Management Good Records. Belfast, DHSSPS.

[15] NHS Connecting for Health. (2010). *Health and social care staff members: What you should know about Information Governance.* London, The Stationery Office.

have been communicated to all staff via policies and relevant training to ensure compliance. Communication will be on-going throughout NIPEC to ensure that all staff are aware of Information Governance processes and procedures. This is an essential action to ensure NIPEC effectively meets the aims and objectives set out in this strategy.

7.6 Mandatory Information Governance Training

NIPEC will ensure that all staff have the knowledge and skills needed relevant to their role and level of responsibility within the organisation. NIPEC will make sure that appropriate training and information is available to up-skill existing staff, and train new members of staff. Training required under the Information Management and ICT Controls Assurance Standards is incorporated within the e-learning platform and includes:

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

In addition within the suite of mandatory e-learning programmes in NIPEC; the following elements are linked:

- Risk Management Awareness
- Fraud Awareness

There is specific training that NIPEC's Information Asset Owners (IAOs) avail of which covers the following:

- the role of the IAO
- understanding what information assets are
- maintaining an 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 and are appropriately prepared.

7.7 Implementation and Performance Monitoring

The ICT and Governance Group will oversee on behalf of the organisation, the effective implementation of the Information Governance Strategy, and its Information Governance Action Plan (pages 14-15), and that related policies and procedures are relevant, understandable, available and complied with by all staff. The Information

Governance Action Plan sets out the necessary actions that are required to ensure the successful implementation of the Information Governance Strategy. It details the steps that NIPEC will take to make sure that all staff are aware and trained in Information Governance best practice, and that they carry out their duties adhering to this strategy and related policies at all times. The Action Plan will be distributed to all staff in NIPEC via email and will be readily available and accessible through the organisational server.

Examples of best practice for Information Governance will be identified and shared with relevant staff.[16]. Review of the Action Plan will be carried out via quarterly reports on progress brought to the ICT and Governance Group and Business Team.

Performance will be monitored annually against a set of standards and targets in the form of the Information Management and ICT Controls Assurance Standards, including maintenance of training requirements. Staff compliance with NIPEC's Information Governance arrangements will 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 Information Governance requirements, every effort should be made to ensure the staff member is supported to improve his/her practice. Where a staff member continues to fail to comply with any NIPEC policy or procedure the process relating to disciplinary procedures will be commenced.

8.0 Information Governance Action Plan

The table below sets out NIPEC's Information Governance Action Plan.

[16] NHS Connecting for Health. (2010). *Health and social care staff members: What you should know about Information Governance.* London, The Stationery Office.

Action	Start Date	Owner	Target Date	Completion Date	Notes
Develop and publish the following policies: • Data Protection and Confidentiality Policy • Records Management Policy • Web Content Standards • Clear Desk Policy • Review IT Contingency and Security Policy (draft)	February 2016 February 2016	• Head of Corporate Services • ICT and Governance group	March 2017		To ensure the ICT Security Policy covers the use of digital recorders, provision of encrypted USB.
Review Staff training to ensure compliance with CAS to include: • Mandatory e-learning programmes for Information Governance • Identification of development needs related to Information Governance for Council Members	April 2016 June 2016	• Head of Corporate Services • ICT and Governance group	March 2017 November 2016		• Data Protection Awareness • Freedom of Information • Records Management • ICT Security • Risk Management Awareness • Fraud Awareness

Develop an Information governance leaflet to raise awareness with Staff and Council Members	May 2016	• Head of Corporate Services • ICT and Governance group	February 2017		
Implement recommended steps to move towards a paper-lite system by developing a principles based approach to: • Cease maintaining current manual files • Create electronic files only	TBC 2016	• Head of Corporate Services • ICT and Governance group	March 2017		
Develop a protocol for serious adverse incidents related to information breaches or data losses	April 2016	• Head of Corporate Services • ICT and Governance group	September 2016		
Develop and implement Audit of ICT and Filing Procedures Self-assessment tool	April 2016	• Head of Corporate Services • ICT and Governance group	December 2017		
Determine requirements for and develop further quality assurance mechanisms for management of information and technology systems	April 2016	• Head of Corporate Services • ICT and Governance group	On-going/ rolling programme		

9.0 Summary and Conclusion

Information Governance is a vital and integral part of NIPEC's overall Governance programme. The implementation of the Information Governance Strategy and related Information Management and ICT Management policies and procedures will ensure that NIPEC has the appropriate framework in place to meet legislative and organisational requirements. The associated Action Plan will drive the development and implementation of year on year improvement plans, which will ensure that Information Governance arrangements in NIPEC are continually monitored.

10.0 Equality and Human Rights Considerations

As required by Section 75, Schedule 9, of the Northern Ireland Act, 1998, any equality implications of the Strategy have been considered. In addition, consideration has been given to the terms of the Human Rights Act 1998.

As a result of these considerations a screening of the Strategy has been undertaken and can be viewed at: http://www.hscbusiness.hscni.net/services/2166.htm.

Using the Equality Commission's screening criteria; no significant equality implications have been identified. The Strategy will therefore not be subject to an equality impact assessment.

11.0 Review of Strategy

NIPEC is committed to ensuring that all policies and procedures are kept under review to ensure that they remain compliant with relevant legislation and guidance. This Information Governance strategy will run from April 2016 until April 2020, therefore covering a four year period. The Head of Corporate Services along with the ICT and Governance Group are responsible and therefore will carry out the review of this strategy.

12.0 References

Department of Health, Social Services and Public Safety (DHSSPS) (2009) *ICT Management Controls Assurance Standards.* Belfast, DHSSPS.

Department of Health, Social Services and Public Safety (DHSSPS) (2013) *Information Management Controls Assurance Standards.* Belfast, DHSSPS.

Department of Health, Social Services and Public Safety (DHSSPS) (2011) *Good Management Good Records.* Belfast, DHSSPS.

Information Governance Framework. Available at: https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/info-gov-framework. (Accessed: 23/11/15).

NHS Connecting for Health. (2010). *Health and social care staff members: What you should know about Information Governance.* London, The Stationery Office .

What is Information Management? Available at: http://www.aiim.org/What-is-Information-Management (Accessed: 01/10/15).

5 Benefits of Creating an Information Governance Strategy. Available at: http://www.consultparagon.com/blog/5-benefits-of-creating-an-information-governance-strategy (Accessed: 23/11/15).

Hagmann, J. (2013). Information governance – beyond the buzz. *Records Management Journal*, 23(3), pp.228-240

Appendix 1: Legalisation and Guidance

Public Records Act (NI) 1923

It is a legislative requirement for NIPEC 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 1998 (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 NIPEC to respond to requests for access to information.

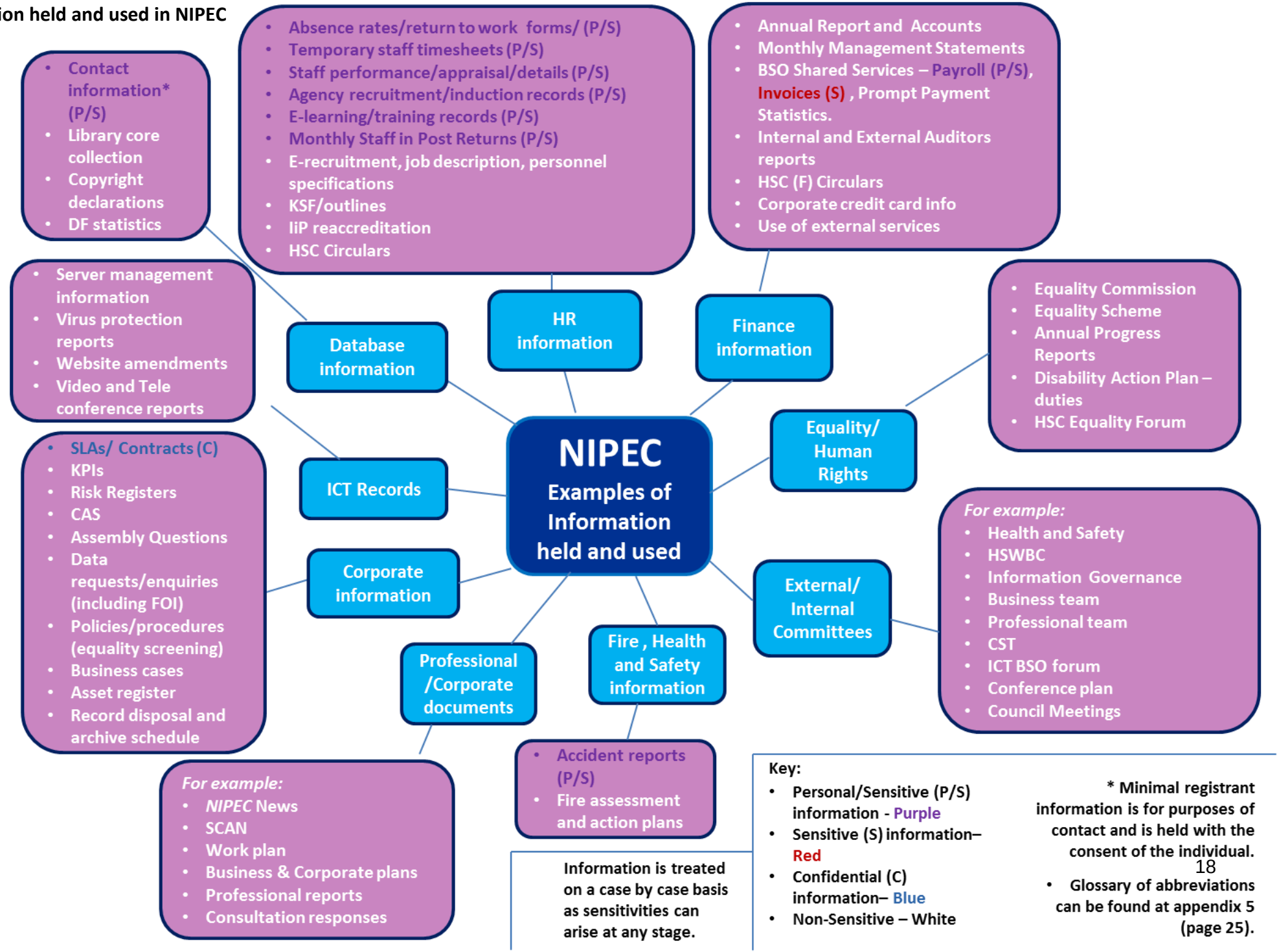
Environmental Information Regulations 2004 (EIR)

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

Good Management Good Records 2004 (GMGR)

GMGR incorporates the DHSSPS advice and guidance on records management. It includes a retention and disposal schedule, prepared in accordance with the Public Records Act (NI) 1923 and the Disposal of Documents Order 1925.

Appendix 2: Examples of information held and used in NIPEC



Appendix 3: Definitions of Access Categories

(1) Restricted Data (Authorised Access)

Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the organisation, staff members or stakeholders. The highest level of security controls should be applied to Restricted data.

(2) Confidential Data (Controlled Access)

Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the organisation, staff members or stakeholders. By default, all Data that is not explicitly classified as Restricted or Public should be treated as Confidential data. Moderate level of security controls should be applied to Confidential data.

(3) Public Data (Free Access)

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the organisation, staff members or stakeholders. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Examples of information safeguards for Access Categories

Information Format	**Restricted Data**	**Confidential Data**	**Public Data**
Manual Files or hard copy documents	*Refer to NIPEC policies; in particular the Records Management Policy*		
	Secured in a locked environment. Locked within safe or pass-coded room. Restricted data cannot be accessed unless it is by authorized personnel. e.g. Personal details of staff including human resources information and bank details.	Stored in a secure environment such as a filing cabinet or drawer. Controlled manual filing procedures are in place. e.g. Service Level Agreements (SLAs)/contracts.	Stored in an appropriate manner and accessible by staff. Appropriate manual filing procedures in place. e.g. Record disposal and archive schedule.
Electronic Information	*Refer to NIPEC policies; in particular the IT Ethical Code and ICT Security Policy, with specific reference to: computer usage guidelines, good password selection, data classification and encryption*		
	Stored securely and only accessed by authorized personnel. Personal/sensitive information is encrypted and password protected. Restricted data cannot be moved or transferred to a pen drive or hard drive of a personal computer Passwords are changed quarterly to ensure that private and sensitive files remain secure. e.g. Personal email addresses held with permission of stakeholders.	Electronic files and databases are stored in an appropriate and secure location, with controlled access. Passwords are changed quarterly to ensure that confidential files remain secure. e.g. Unverified accounts, Draft business plans.	Stored on NIPEC's server and accessible by staff. Appropriate electronic filing procedures in place. Accessible via NIPEC's websites. Passwords are changed quarterly to ensure that staff files remain secure. e.g. External/internal committee notes/agendas, information on NIPEC's current work and projects.

Appendix 4: Information Governance Management Framework

Framework Area	Requirement	NIPEC Structure	Quality Assurance Mechanisms of Information Management and Technology Systems
Senior Roles	• Information Governance Lead • Senior Information Risk Owner (SIRO) • Personal Data Guardian (PDG) • Information Asset Owners (IAOs)	Due to the small structure, the Head of Corporate Services acts as the Information Governance Lead, SIRO and PDG, and delegates appropriate responsibilities as required. The Corporate Services Manager is trained as an IAO to support the lead with these roles.	• Annual training outcomes • Annual appraisals
Key Policies	• Overarching Information Governance Strategy • Supporting Information Management Policies and Procedures • Supporting ICT Management Policies and Procedures	**Information Management** • Freedom of Information Request Procedures • Records Management Policy Statement • Retention and Disposal Schedule • Data Protection Policy Statement • Accessible Formats Policy for the Provision of Information • Publication Scheme • Public Involvement Strategy • Operational procedure for manual and electronic filing system • Security of NIPEC property and personal property • Disciplinary Procedure	• Rolling programme of review of policies and procedures • Annual CAS IM and ICT • Quarterly review by Audit and Risk Committee • Quarterly Council reports

		ICT Management • Information Technology Ethical Code and Computer Usage Guidelines • IT Contingency Policy • Business Continuity Plan • Social Media Policy / Guidance • Website Information Procedure • Information and Communication Technology (ICT) Strategy • ICT Security Policy Note: This list is not exhaustive. There are further policies outside of Information Management and ICT Management that include related Information Governance guidance.	
Key Governance Bodies	• Responsible Group for Information Governance	• NIPEC Council • Audit and Risk Committee • ICT and Governance Group	• Quarterly Audit and Risk reports • Quarterly Council reports • Annual CAS IM and ICT
Resources	• Key staff roles • Dedicated use of funding and budgets	• Information Governance Lead • SIRO • PDG • IAO • IAA • All staff • Information Asset Register	• Annual appraisals • Quarterly reports on the use of funding • 6 weekly monitoring by ICT and Governance Group
Governance Framework	• Details of how responsibility and accountability for Information Governance is communicated	Information Governance Strategy articulates: • Role of the Information Governance Lead	• CAS IM and ICT • Quarterly report to Council

	through NIPEC.	• Staff roles and responsibilities • Information Asset Register	
Training and Guidance	• Training for Information Governance roles • Training for all staff • Staff Code of Conduct	• Mandatory Information Governance e-learning training for all staff • SIRO, PDG and IAO training completed (for further details see page 12) • Staff Code of Conduct	• Annual review of staff training • Annual appraisals
Incident Management	• Policies and Procedures in place • Awareness and relevant training of all staff	• Risk Management policy, strategy and action plan • Disciplinary procedure	• Rolling programme of review of policies and procedures

Appendix 5: Glossary of abbreviations

BSO	Business Services Organisation
CAS	Controls Assurance Standards
CST	Corporate Services Team
DF	Development Framework
DHSSPS	Department of Health, Social Services and Public Safety
DPA	Data Protection Act
EIR	Environmental Information Regulations
FOI	Freedom of Information
GMGR	Good Management Good Records
HCS	Head of Corporate Services
HR	Human Resources
HRPTS	Human Resources, Payroll, Travel and Subsistence
HSC	Health and Social Care
HSC (F)	Health and Social Care (Finance)
HSWBC	Health and Social Wellbeing Committee
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICT	Information and Communications Technology
IiP	Investors in People
IT	Information Technology
KPI	Key Performance Indicator
KSF	Knowledge and Skills Framework
PDG	Personal Data Guardian
SCAN	Senior Nurse/Midwife Current Awareness from NIPEC
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement