NIPEC/20/15

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Records Management Policy

December 2020

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:	July 2018 December 2020
Approved by / date:	**BTM:** 8th December 2020 **Council:** 31st December 2020
Date of next Review:	April 2023
Equality Screened by / date:	December 2020

CONTENTS

1. Introduction and Policy Statement

All Health and Social Care (HSC) records are public records under the terms of the Public Records Act (NI) 1923 and in the Disposal of Documents (Northern Ireland) Order (1925). The Act sets out the broad responsibilities for everyone who works with such records, and as such, NIPEC has a statutory duty to make arrangements for the management and safekeeping of its records, and for their retention, storage, and eventual disposal.

Furthermore, information is a corporate asset and NIPEC records are vital to the organisation in its current and future work, for the purposes of accountability, and for an awareness and understanding of its history. They are the corporate memory of the organisation.

This policy should be read in conjunction with the following NIPEC policies and other guidance:

- Information Governance Strategy
- Data Protection Policy
- Clear Desk and Screen Policy
- FOI Request Procedures
- ICT Security Policy
- IT Ethical Code and Computer Usage Guidelines
- Operational Procedure for NIPEC's filing system
- Relevant legislation, to include those referred to within section 1.1, The Data Protection Act (2018), The General Data Protection Regulation (2016) and the Freedom of Information Act (2000)
- Relevant guidance, to include The Department of Health's (DoH) 'Good Management, Good Records (2020) (GMGR).'

2. Purpose and Aims of Records Management

The purpose of this policy is to ensure that NIPEC adopts best practices in the management of its records so that authentic, reliable and useable records are created which are capable of supporting our functions and activities for as long as they are required. It aims to uphold the quality of NIPEC's records; to maintain, retain or dispose of these records in accordance with NIPEC's need and legislative requirements and to ensure the permanent preservation of appropriately identified records. The policy will ensure that:

- records are present, accurate and complete;
- the record provides a reliable and accountable representation of business activity and, if relevant, provides the rationale behind the decision-making process;
- effective filing systems are maintained that support improved information retrieval methods;

- records are made accessible to enable well-informed and appropriate judgements to be made;
- records are kept securely and protected from accidental loss, destruction and unauthorised access;
- records are kept for no longer than is necessary, in accordance with legal and professional obligations and with due regard to the regionally agreed retention and disposal schedule;
- staff are made aware of and trained in the management of records within their sphere of work or responsibility.

Compliance with this policy will ensure that NIPEC can provide evidence of performance and demonstrate accountability, as well as providing information about its decisions and activities.

3. Scope

The international standard of managing records, ISO 15489 defines a record as *"information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".*

In the context of this policy a record is any recorded information that contains information, in any media which is created, collected, processed, used stored and/or disposed of by NIPEC employees, as well as those acting as its agents in the course of NIPEC business. It also includes emails, and additional guidance on the use of emails can be found in Appendix 1.

This policy applies to **all staff**. In this document, the term 'all staff' refers to regular full-time, regular part-time, contractors, consultants, agency staff and temporary employees.

4. Accountability

The **Council** has overall responsibility to ensure compliance in all areas of information governance, including records management.

The **Chief Executive** and **Senior Team** have a duty to ensure that NIPEC complies with the requirements of legislation affecting management of the records. They will oversee the effective record management within NIPEC, and with **designated NIPEC staff**, have a duty to ensure that NIPEC complies with the requirements of legislation affecting the management of records and with supporting regulations and codes.

The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

The **Senior Information Risk Officer (SIRO)** is a senior manager who has responsibility to ensure compliance with legislation through the development and monitoring of policy and codes of practice. The SIRO is supported in this role by Information Asset Owners

(IAOs) who must provide assurance to the SIRO that information risk is managed effectively for the information assets that they own.

The Data Protection Officer on behalf of the SIRO will work closely with all staff to ensure that there is consistency in the management of records and that advice and guidance on good records management practice is provided throughout the organisation.

The **Information Governance Group** are responsible for maintaining the accuracy and relevance of this policy and providing assurance to NIPEC's Business Team and Council as to its implementation and effectiveness. They will work closely with all staff to ensure that there is consistency in the management of records and that advice and guidance on good records management practice is provided throughout the organisation.

All members of NIPEC staff are responsible for documenting their actions and decisions in the records and for maintaining records in accordance with section 5 of this policy. They have a duty to protect and ensure that any information they add to the record is necessary, accurate and complete. The confidentiality of client and staff records must always be of primary concern to NIPEC staff.

All staff are responsible for:

- ensuring they have a clear understanding of records management and demonstrate commitment to duties relating to record keeping;
- creating records which are consistent, reliable, accurate and complete;
- capturing records which authentically document activities in the course of which they were produced;
- accessibility of a record: filing records correctly in the appropriate area of NIPEC's filing system on the server;
- applying security and access controls to records where appropriate;
- identifying and applying appropriate disposal and retention periods to records.

5. Records Filing Structure

NIPEC's records are stored electronically on a central server. In the past NIPEC maintained a dual manual and electronic filing system, however, in April 2017, it was agreed NIPEC would move to a paper-lite system and as a first step, cease creating paper based/manual folders in which to store records. Historical manual folders have been retained and will be managed and disposed of as per NIPEC's Disposal Schedule.

The **Corporate IT and Information Officer** will monitor the storage and retention of NIPEC's records and, through the **Information Governance Group,** ensure NIPEC's Operational Procedure for its filing system and guidance within GMGR is being followed by all staff.

6. Retention and Disposal of Records

All records should be retained and disposed of in accordance with the Department of Health's Good Management, Good Records (GMGR).

A regular quality check of NIPEC's filing system, at least once every two years, will be undertaken by the Corporate IT and Information Officer. In liaison with NIPEC's Business Team and approval of the Chief Executive, relevant manual and electronic files will be archived, disposed of, and, where relevant, forwarded to PRONI for permanent preservation.

7. Monitoring Compliance

Monitoring of compliance with this policy will be undertaken by NIPEC's Information Governance Group, reporting any issues to NIPEC's Business Team in order to agree any changes required or action to be taken.

A failure to adhere to this policy and any associated procedures may result in disciplinary action.

8. Equality

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 specific equality impacts and outlines the way that 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 here
http://www.hscbusiness.hscni.net/services/2166.htm

Appendix 1

NIPEC guidance on the use of emails

NIPEC staff are reminded of their responsibility to protect NIPEC records and treat all sensitive and personal information as confidential. This applies to information held in all formats, including emails.

The following guidance should be followed:

- Be aware that all work emails are organisational records;
- Remember that an email is not a secure form of communication;
- Remember that all emails may be open to scrutiny and are discoverable under the Freedom of Information Act 2000 and the Data Protection Act 2018;
- Only send information to those who need to receive that information;
- Only copy (cc) or 'forward' emails when it is necessary;
- Always check you have the correct recipient / email address before sending the email;
- When sending emails to a number of individuals, consider using the 'BCC' function especially where personal email addresses are included;
- Avoid sending excessive amounts of confidential information by email;
- Do not include names in the subject line of an email;
- When attaching sensitive or personal information, use passwords and encryption for an extra level of protection;
- Personal or sensitive information should not be emailed either to or from any staff member's personal computer or personal email account;
- Exercise the same degree of care and professionalism in regard to the content of email messages as you would with a letter - think of an email as an open 'post card'
- Delete unwanted emails as soon as they are no longer required, ensuring these items are deleted permanently from your system.