NIPEC/20/13
Replacing NIPEC/18/10

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Data Protection Policy

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:	Jill Jackson
Reviewed:	July 2018 January 2021
Approved by / date:	**BTM:** 12th January 2021 **Council:** 8th February 2021
Date of next Review:	January 2024
Equality Screened by / date:	Corporate Services Manager, February 2021

CONTENTS

1. Introduction and Purpose

NIPEC is fully committed to complying with the General Data Protection Regulation (GDPR) 2016 / Data Protection Act 2018 (GDPR) which came into force on 25 May 2018. The new law expands the rights of individuals to control how their personal data is collected and processed and places a range of obligations on organisations to be more accountable for data protection.

As a public body, NIPEC has a statutory duty to safeguard the information it holds, from whatever source, which is not in the public domain. The purpose of this policy is to set out the principles that must be followed by anyone who works for NIPEC and has access to personal information including all employees, contractors, agents, consultants and other parties, ensuring that they are fully aware of and abide by their duties and responsibilities under the Act. The policy also aims to clarify how and when personal information may be shared and the requirement to inform individuals of the ways in which their information may be used.

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
- Information Governance Policy
- Clear Desk and Screen Policy
- Incident Reporting Policy
- Data Protection Impact Assessment 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
- Social Media Policy / Guidance
- ICT Security Policy.

2. Policy Scope

The scope of this policy is to support the protection, control and management of personal information. NIPEC needs to collect and use personal information about people with whom we work in order to carry out our business and provide our services. 'People' may include members of the public; current, past and prospective employees; clients; customers; and suppliers. In addition, we may be required by law to collect, use and share personal information.

All personal information, whether in paper, electronic or any other format, must be handled and managed in accordance with GDPR.

3. Data Protection Principles

NIPEC, its staff and others who process personal information on its behalf must fully support and comply with the six principles of the Act. In summary, this means personal information shall be:

(i) processed fairly, lawfully and in a transparent manner;
(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes;
(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(iv) accurate and kept up to date;
(v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
(vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Our purpose for holding personal information, along with a general description of the categories of people and organisations to which we may disclose it, is listed in the Information Commissioner's Data Protection Register.

4. Definitions

4.1 Personal Information

The term 'personal information' applies to any information relating to an identified or identifiable natural person. It relates to both electronic and manual information held in any format.

4.2 Special categories of personal information

Article 9 of GDPR defines 'special categories' of personal information as information relating to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data for the purpose of uniquely identifying a natural person
- health (mental or physical)
- sexual life or sexual orientation.

4.3 Data Controller

The 'data controller' is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal information.

4.4 Data Processor

A ‘data processor’ is a natural or legal person, public authority, agency or any other body which processes personal information on behalf of the data controller.

5. Policy Objectives

NIPEC will apply the above principles to the management of all personal information by adopting the following objectives:

5.1 Privacy by Design

NIPEC will apply ‘privacy by design’ when developing and managing information systems containing personal information by:

- Adopting data minimisation: collecting, disclosing and retaining minimum personal information for the minimum time necessary for the purpose that it is being processed;
- Anonymising personal information wherever necessary and appropriate;
- Where appropriate, using proportionate privacy impact assessment to identify and mitigate data protection risks at an early stage of any project.

5.2 Lawful Processing

NIPEC will:

- Only collect and use personal information that is needed to fulfil operational or legal requirements, and in accordance with the conditions set down under GDPR, namely:
  - Consent of the Data subject;
  - To perform in terms of a contract;
  - To comply with a legal obligation;
  - To protect a data subject’s vital interests;
  - If it is in the public interest;
  - If it is in the controller’s legitimate interests.
- Provide transparent information on how personal information will be processed which will detail:
  - What information is needed;
  - Why this information is needed;
  - The purpose that the information will be used for;
  - How long this information will be kept for.
- Ensure that personal information is collected for specific purposes and is not reused for a different purpose than stated or that the individual did not agree to or expect;
- Ensure the quality of personal information processed.

5.3 Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. NIPEC will not disclose personal information to any third party unless it

believes it is lawful to do so. Respect to confidentiality will be given where appropriate. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- NIPEC has the statutory power or is required by law to do so;
- the information is clearly not intrusive in nature;
- the member of staff has consented to the disclosure;
- the information is in a form that does not identify individual employees.

5.4 Processing of Personal Sensitive Data

Sensitive personal data should normally only be processed if the data subjects have given their explicit and written consent to this processing. Explicit consent is consent that refers to specific and identifiable processing of personal data. Such consent should where possible be obtained in writing as this can be used for future reference, whilst explicit verbal consent cannot. NIPEC may process sensitive personal data without the subjects' explicit consent if the processing is necessary:

- because of any right or obligation imposed by employment law;
- for medical purposes, including medical research, and is undertaken by a health professional or equivalent person;
- for equal opportunities monitoring and in compliance with Section 75 of the Northern Ireland Act 1998.

5.5 Right of Access

GDPR gives any individual who has personal information kept about them by NIPEC the right to request, in writing, a copy of the information held relating to them. NIPEC will ensure that an applicant receives access within a calendar month, unless there is a valid reason for delay or an exemption is applicable.

5.6 Third Party Users of Personal Information

Any third parties who are users of personal information supplied by NIPEC will be required to confirm and demonstrate that they will abide by the requirements of GDPR and will provide assurances to NIPEC in this respect.

5.7 Disposal and Retention of Personal Data

GDPR places an obligation on NIPEC not to hold personal data for longer than is necessary. The Department of Health (DoH) Good Management, Good Records (GMGR) (February 2020), advises on the procedures for disposing of records and length of time records should be retained by NIPEC.

NIPEC will apply retention policies to all personal information, destroying all information no longer required and where deemed appropriate, transferring information to the Public Records Office of Northern Ireland.

6. Roles and Responsibilities

- **NIPEC Council** has overall responsibility to ensure compliance in all areas of information governance;
- The **Chief Executive** has ultimate responsibility for the delivery of this policy;
- The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of patient and service-user information;
- The **Senior Information Risk Owner (SIRO)** is a senior manager who has responsibility to ensure compliance with legislation through the development and monitoring of policies;
- The **Data Protection Officer** (DPO) function is provided via a service level agreement by the Business Services Organisation (BSO). The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements;
- The **Corporate Services Manager** is the delegated NIPEC officer responsible for monitoring compliance of GDPR throughout NIPEC and providing advice and guidance to staff;
- All **NIPEC Staff,** whether permanent, temporary, bank or agency, have a responsibility to ensure that they are aware of the requirements to protect personal information held by NIPEC. They will take steps to ensure that:
    - They familiarise themselves with and abide by the principles of this policy;
    - They understand how to safeguard personal information;
    - They regularly review personal information held by them and update it if it is found to be out of date;
    - If the information is no longer required, it should disposed of in line with GMGR;
    - They never use personal data held about others for their own purposes.

7. Policy Awareness and Monitoring Compliance

A copy of this policy will be given to all new members of staff and interested third parties. Existing staff and any relevant third parties will be advised of the policy which will be posted on our NIPEC website, as will any subsequent revisions. All staff and relevant third parties must be familiar with and comply with this policy at all times.

NIPEC will assess effectiveness of this policy by:

- Ensuring that all staff are appropriately trained to process and manage personal information and monitoring completion of such training;
- Assessing and reporting performance on the management of compliance to access requests, FOIs and data breaches including near misses;
- Carrying out regular audits to ensure that the retention and disposal of records is in line with GMGR;
- Seeking advice and guidance from the DPO on changes in legislation and performance improvements.

8. Non-Compliance

Compliance with this policy will be monitored regularly and reports passed to the appropriate management for consideration. A failure to adhere to this policy and any associated procedures may result in disciplinary action.

9. 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 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

10. Review

This policy is based on a regional HSC policy. It will be monitored and reviewed in January 2024, or sooner, if a revised HSC policy is issued.