NIPEC 2024/04
Replacing NIPEC/20/13

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Data Protection Policy

August 2024

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

James House
2-4 Cromac Avenue
Belfast
BT7 2JD
Tel: 0300 300 0066
https://nipec.hscni.net

Developed by:	Business Manager
Approved by / date:	**BTM:** 12th January 2021; 10th September 2024; **Council:** 8th February 2021; 18th September;
Date of next Review:	August 2027
Equality Screened by / date:	Business Manager -June 2024

CONTENTS

1. Introduction and Purpose

NIPEC is fully committed to complying with Data Protection Legislation. The UK General Data Protection Regulation ('UK GDPR') is a UK law which came into effect on 1st January 2021, following the UK's withdrawal from the EU. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The Data Protection Act 2018 ('DPA 2018') sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25th May 2018. It was amended on 1st January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

It sits alongside and supplements the UK GDPR, for example by

- providing exemptions;
- setting out separate data protection rules for law enforcement authorities;
- extending data protection to some other areas such as national security and defence;
- setting out the Information Commissioner's functions and powers.

As a public body, NIPEC has a statutory duty to safeguard the information it holds, from whatever source. The purpose of this policy is to support the protection, control and management of personal data. The policy has been developed to support all staff, and where applicable contractors and third-party suppliers, to comply with legislation, policy and best practice relating to the protection of personal data.

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
- Adverse Incident Reporting Policy
- Data Protection Impact Assessment Policy
- Operational Procedure for Filing System
- Social Media Policy / Guidance
- ICT Security Policy.

2. Scope and Definitions

The scope of this policy is to support the protection, control and management of personal information.

The following definitions are as defined within Articles 4 and 9 of the UK GDPR:

- **Personal Data**: means any information relating to an identified or identifiable natural person (data subject);
- **Special Categories**: of personal data is data relating to one or more of 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;
- **Data Controller**: is 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 data;
- **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;
- **Processing:** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Pseudonymisation:** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **Restriction of Processing:** means the marking of stored personal data with the aim of limiting their processing in the future;
- **Profiling:** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- **Consent**: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **Personal data breach:** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Genetic data:** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology

or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- Biometric data: means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;
- **Data concerning health**: means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

3. Data Protection Principles

NIPEC, its staff and others who process personal information on its behalf must ensure that they follow the principles set out within Article 5 of the UK GDPR. In summary, this means personal data shall be:

(i) processed fairly, lawfully and in a transparent manner ('Lawfulness, Fairness and Transparency');
(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes ('Purpose Limitation');
(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('Data Minimisation');
(iv) accurate and where necessary, kept up to date ('Accuracy');
(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 ('Storage Limitation');
(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 (Integrity and Confidentiality').

In addition, the UK GDPR requires NIPEC to implement appropriate technical and organisational measures to implement the above principles and safeguard individual rights. This is known as 'privacy by design and by default.'

Together, both the UK GDPR and DPA 2018 set out the minimum standards we must adhere to, in order to protect personal data, and to ensure that we are only using it for specific and limited purposes. There are 7 principles set out within UK GDPR which are summarised in the following paragraphs.

4. Lawfulness, Fairness and Transparency

NIPEC will only process personal data if doing so satisfies one or more of the criteria as set out within Article 6, and where applicable, Article 9 and Article 10 of the UK GDPR and associated provisions of the Data Protection Act 2018.

The lawful basis for the processing of personal data as set out in Article 6 are as follows:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal/statutory obligation to which the controller is subject to;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (although 'legitimate interest cannot generally be used by public bodies as a basis for processing, it is included here in the interest of completeness).

We must identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data, and ensure that anything we do with this data does not breach any other laws. We must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned, and we must be clear, open and honest from the start about how we will use their personal data.

5. Purpose Limitation

NIPEC must only process personal data for specified, explicit and legitimate purposes, as set out in privacy information within Section 4. These purposes must be documented and we must not use personal data for a new purpose unless the new purpose is compatible with the original purpose, specific consent is obtained for the new purpose or we have a clear function set out in law.

Any new purpose must be fully documented prior to this new purpose commencing.

6. Data Minimisation

Personal data should be limited to what is necessary, and not processed unless it is relevant for the purposes intended. Staff must only process personal data as part of the discharge of their role and never for any reason unrelated to their job duties.

Personal data must be periodically reviewed to ensure it remains adequate, relevant and limited.

7. Accuracy

NIPEC staff must take all reasonable steps to ensure the personal data processed is not incorrect or misleading. All reasonable steps must be taken to amend inaccurate data as soon as possible after an inaccuracy is noticed.

Personal data must be held in as few places as necessary. NIPEC must comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

8. Storage Limitation

NIPEC must not keep personal data for longer than is needed. Where personal data is no longer needed for specified purposes, all reasonable steps must be taken to delete it. The length of time to keep data should be justified in accordance with the regional retention schedule 'Good Management Good Records' (GMGR) and NIPEC's Retention Disposal Schedule.

NIPEC must consider and document any requests for erasure under the 'right to be forgotten.'

Personal data should be periodically reviewed to comply with the above.

9. Integrity and Confidentiality

NIPEC must ensure that we have appropriate security measures in place to protect the personal data we are processing and keep it secure from unauthorised or unlawful processing, accidental loss, destruction or damage.

Safeguarding will include the use of encryption, restricting access so that only those with authorisation can access personal data, access restriction in premises, staff training and adherence to policies.

Staff must familiarise themselves with all the requirements as set out in the following policies:

- Information Governance
- Clear Desk and Screen
- ICT Security Policy
- Adverse Incident Reporting Policy

- Hybrid Working Policy
- Records Management
- Data Protection Impact Assessment

10. Accountability

Accountability is central to UK GDPR. NIPEC must know what data we have and why it is used, for the purposes of demonstrating accountability.

Further, we must have additional measures in place, including:

- Contracts / formal agreements with those who we share data with, process on behalf of (or vice versa);
- Documenting all our data processing activities;
- Employment of a Data Protection Officer; and
- Registration with the Information Commissioner's Office (ICO).

11. 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 **Senior Information Risk Owner (SIRO)** is a senior manager (Head of Corporate Services) 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 Business Manager is the delegated NIPEC officer responsible for monitoring compliance of UK 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;
    - Ensure all mandatory and additional training are completed in order to help safeguard information.

12. Policy Awareness and Compliance

A copy of this policy will be given to all members of staff and it will be posted on the NIPEC website. All staff and relevant third parties must be familiar with and comply with this policy at all times. Compliance with this policy will be monitored regularly and reports passed to the appropriate management for consideration.

13. Non-Compliance

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

Serious breaches of this policy may be reported to the PSNI, ICO or another public authority for further investigation.

14. Equality Statement

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

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: https://bso.hscni.net/directorates/people-and-place/655-2/equality-and-human-rights-screening/equality-screening/

15. Review

This policy will be reviewed in August 2027, or sooner, in the event of new legislation, guidance or best practice.