NIPEC/18/10
Replacing NIPEC/17/07

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Data Protection Policy

(Including GDPR)

May 2018

Review date: June 2020

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

www.nipec.hscni.net

Introduction

1. NIPEC is fully committed to complying with the Data Protection Act 2018 (DPA 18) which superseded the 1998 Act and came into force on 25 May 2018. The DPA 18 incorporates the GDPR (General Data Protection Regulations) addressing areas in which flexibility and derogations are permitted.

2. Significant and wide-reaching in scope, the new law expands the rights of individuals to control how their personal data is collected and processed and places a range of new obligations on organisations to be more accountable for data protection.

3. We will follow procedures to ensure that all employees, contractors, agents, consultants and other parties who have access to any personal information held by or on behalf of us are fully aware of and abide by their duties and responsibilities under the Act.

Statement of Policy

3. We need to collect and use 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 and use information. All personal information, whether in paper, electronic or any other format, must be handled and managed in accordance with DPA.

Data Protection Principles

4. We 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
   (iii) adequate, relevant and limited to what is necessary
   (iv) accurate and kept up to date
   (v) kept in a form which permits identification of data subjects for no longer than is necessary
   (vi) processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

   Further details of the above are shown in Appendix A.

5. 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.

Disclosure of Personal Information

6. Strict conditions apply to the disclosure of personal information both internally and externally. We will not disclose personal information to any third party unless we believe 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:

- we have the statutory power or are 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.

Handling of Personal Information

7. All staff will, through appropriate training and responsible management:

- fully observe conditions regarding the fair collection and use of personal information
- meet our legal obligations to specify the purposes for which personal information is gathered and used
- collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of personal information used
- apply strict checks to determine the length of time personal information is held
- ensure that the rights of people about whom information is held can be fully exercised under the Act
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without adequate safeguards.
- advise the Head of Corporate Services (HCS), or in his absence the Corporate Services Manager (CSM), at the earliest opportunity if either a data breach has occurred or is suspected. Data breaches that are likely to result in risk to the organisation, should be reported to the HCS / CSM, **within 72 hours** of awareness to enable the ICO and, in some cases, the effected data subjects to be informed – see Appendix B. The HCS / CSM will advise BSO's DPO of all data breaches, using the dedicated email address – databreach@bso.hscni.net

Compliance with Data Protection Principles

8. We will ensure that:

- each year staff are reminded of their obligations under DPA
- everyone managing and handling personal information understands that they are directly and personally responsible for following good Data Protection practice
- only staff who need access to personal information as part of their duties are authorised to do so
- everyone managing and handling personal information is appropriately trained to do so and supervised
- anyone wanting to make enquiries about handling personal information knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are clearly described
- the way personal information is managed is regularly reviewed

- methods of handling personal information are regularly assessed and evaluated
- performance on handling personal information is regularly assessed
- all Subject Access Requests (SARs), which are received in writing, will be dealt with in accordance with DPA and within 30 calendar days of receipt.

9. To assist in achieving compliance, we have:

- designated the HCS as the officer with overall responsibility for Data Protection within NIPEC
- nominated the HCS as the Personal Data Guardian (PDG) and Senior Risk Owner (SIRO) within NIPEC
- signed an enhanced SLA with the BSO, Human Resources, to enable expert advice on DPA to be available to NIPEC from their Data Protection Officer
- appointed the CSM as NIPEC officer responsible for monitoring compliance of the Act throughout NIPEC; providing advice and guidance; dealing with escalated complaints from data subjects; and liaising with the ICO and HSC solicitors on data protection issues
- nominated the CSM and Corporate IT & Information Officer as Information Asset Owners within NIPEC
- nominated the PA to the Chief Executive and Chair, Corporate Services Officer and Events and IT Support Officer as Information Asset Administrators (IAA) within NIPEC
- created a 'NIPEC Data Protection Manual', providing staff with detailed guidance on data protection procedures.

A data protection reporting structure (Appendix C) has been developed to reflect the above roles and responsibilities.

Staff Responsibilities

10. All staff have a responsibility to protect the personal information held by NIPEC. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- they are appropriately trained in the handling of personal information
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment
- personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically
- individual passwords should be strong and not disclosed to ensure that they are not compromised.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted or disposed of.

11. If and when, as part of their responsibilities, staff collect information about other people, they must comply with the guidance set out in our Data Protection Manual. No one should disclose personal information outside this guidance or use personal data held about others for their own purposes.

Disposal and Retention of Personal Data

12. DPA places an obligation on NIPEC to exercise care in the disposal of personal data, including protecting its security and confidentiality during storage, transportation, handling and destruction. All staff have a responsibility to consider safety and security when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved, i.e. how sensitive is it, and the format in which it is held.

13. DPA also places an obligation on NIPEC not to hold personal data for longer than is necessary. NIPEC's Disposal Schedule advises on the procedures for disposing of records and length of time records should be retained by NIPEC.

Sensitive Personal Data

14. DPA 18, like its predecessor the 1998 DPA Act, includes a category for sensitive personal data, which was subject to additional safeguards.

15. Sensitive personal data is any personal data which includes information on:

    - racial or ethnic origin
    - political opinions, religious or similar beliefs
    - trade union membership
    - physical or mental health
    - sexual life
    - the (alleged) commission of any offence, subsequent proceedings or sentence.

16. 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. If this is not possible, the data may still be processed if one of a number of other conditions is met. 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.

Third Party Users of Personal Information

17. 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 the Act. There will be an expectation that these parties will audit their compliance with the DPA and will provide assurances to NIPEC in this respect.

    As stated in Section 7, any data breach or suspected data breach must be notified to the HSC, copied to the CSM, **within 72 hours** of awareness.

Policy Awareness and Review

18. A copy of this policy statement 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.

19. This policy will be monitored during its time period and reviewed and/or updated, as appropriate.

Signed: _____ Date: _____
Chief Executive

Data Protection Principles

The DPA 18 builds on the fundamental six principles of:

- Fairness
- Transparency
- Accuracy
- Security
- Minimisation
- Rights of individuals

by adding the following additional principles through **'Privacy by Design'** i.e.

- Lawful Processing
  - 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

- Data Subject Increased rights
  - To receive information within a month, free of charge
  - Correction of data which is wrong
  - Restrict processing in certain circumstances
  - Transfer to another data controller
  - The Right To Erasure
  - Right to compensation

- Processing conditions
  - Precisely why the information is required
  - The period for which the data will be stored
  - Their rights (such as the ability to withdraw consent and the right to complain to the ICO)

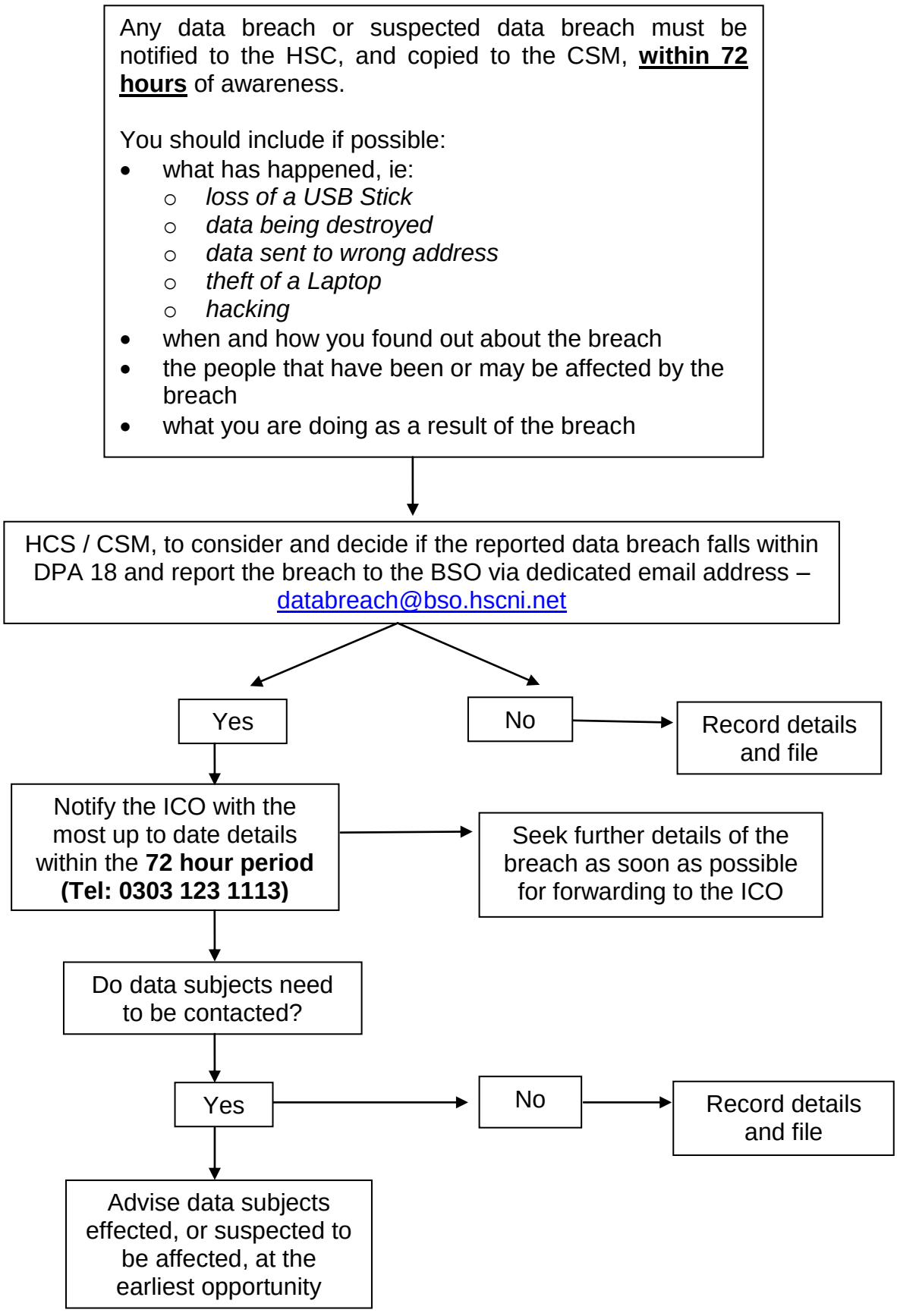
- Rapid notification of breach(s)
  - Data controllers must notify data breaches that are likely to result in risk *for the rights and freedoms of individuals* to the ICO within 72 hours of awareness.
  - In some cases, the data controller must also notify the affected data subjects without undue delay

- Significant fines
  - The GDPR allows the ICO to take a range of actions:
    - Issue warnings
    - Issue reprimands
    - Impose fines that will in each case be effective, proportionate, and dissuasive
    - Tier 1: Up to £10,000,000 or 2% of turnover
    - Tier 2: Up to £20,000,000 or 4% of turnover
  - Fines will be based on circumstance as well as actions to be taken to mitigate the breach

- Direct accountability for data processors
  - **Data Controllers:**
    - obligation to ensure contracts with data processors comply with GDPR
  - **Data processors have direct obligations**:
    - maintain a written record of processing activities carried out on behalf of each controller
    - notify the controller on becoming aware of a data breach without undue delay

Appendix B

Data Breach Notification/Decision Flow Chart



Appendix C

Data Protection Flow Chart – Reporting Structure Corporate Services