**NIPEC/20/14**
(replacing NIPEC/18/16)

NIPEC

**NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY**

# Adverse Incident Policy

## For the reporting of Adverse Incidents, Near Misses, Accidents and Dangerous Occurrences

## 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:** | Janet Hall |
| **Approved by / date:** | **BTM:** 12th January 2021<br>**Council:** 8th February 2021 |
| **Date of next Review:** | December 2023 |
| **Equality Screened by / date:** | Corporate Services Manager, February 2021 |

# Contents

## 1. INTRODUCTION

1.1 This policy sets out the NIPEC process for the reporting of all Adverse Incidents, Near Misses, Accidents and Dangerous Occurrences (hereafter referred to as 'incidents') and gives guidance on what staff should do following an incident, how it should be managed and investigated. It encourages a reporting and learning culture with safety at its heart.

1.2 The policy has been developed in line with the Business Services Organisation (BSO) policy which involved consultation with representatives from the Health and Safety Committee, Human Resources, Trade Unions and the Equality Unit and took account of HSCB/DoH requirements.

1.3 Reporting all data breaches, adverse incidents, accidents, dangerous occurrences and near misses, however trivial they may appear, enables a profile to be built of the risks to staff, visitors and the business of NIPEC, from which a strong and factual basis for targeting resources effectively can be developed. By understanding the patterns and trends of incidents, NIPEC is better placed to manage the underlying risks.

1.4 NIPEC supports a culture of safety and openness. All staff are required to report incidents, and potential incidents, so that steps can be taken to improve the safety of visitors and staff. This awareness may serve to alert management and other staff to areas of potential risk at an early stage and enable avoiding action to be taken by improving work practice, and through feedback and learning provide a valuable source of learning and improvement.

1.5 Furthermore, the reporting of data breaches is mandatory under the General Data Protection Regulation (GDPR). Certain breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of their occurrence therefore it is essential that NIPEC have mechanisms in place to report and investigate data breaches, suspected or actual, in a timely manner.

1.6 This policy should be read in conjunction with other relevant health and safety and information governance policies, including NIPEC's Health and Safety Policy, Fire Safety Policy, Information Governance Policy, Data Protection Policy and Business Continuity Plan.

## 2. RESPONSIBILITIES

2.1 **NIPEC Council** has overall responsibility for effective risk management and this includes oversight of the management of adverse incidents within NIPEC for which the Chief Executive is accountable. The Head of Corporate Services has operational responsibility for this policy and is supported by the Corporate Services Manager in the day to day administration of the process.

2.2 The **Audit & Risk Committee** is responsible for seeking assurance and advising NIPEC Council on the management of all incidents;

2.3 The **Business Team** are responsible for ensuring that the policy is fully implemented in NIPEC;

2.3 **Managers** are responsible for:

- Ensuring that all staff are aware of the policy and reporting procedures, and understand the need to follow the process outlined for reporting incidents;
- Ensuring appropriate and timely reporting of incidents;
- Working with the Corporate Services Manager and other local staff who have responsibility for health and safety and/or information management;
- Supporting the process of reporting, reviewing and investigating local incidents;
- Taking local remedial and preventative action;
- Supporting and debriefing staff and ensuring appropriate access to learning and development in the managements of incidents.

2.4 The **Head of Corporate Services**, assisted by the **Corporate Services Manager**, will:

- Ensure accessibility of up to date reporting documentation and guidelines;
- Support the reporting process by reviewing incidents jointly with relevant managers;
- Support and facilitate investigations into incidents as appropriate;
- Ensure that incidents reports are sent to the appropriate persons and/or government agencies;
- Prepare reports for NIPEC's Audit & Risk Committee of all incidents on a regular basis or at least annually as appropriate including themes and trends where appropriate;
- Ensure records and databases are accurate and up to date and available for inspection by appropriate persons;

2.5 **All staff** (permanent, temporary and agency workers) are responsible for:

- Familiarising themselves and adhering to the requirements of this policy and all relevant legislation including through ongoing learning and development programmes;
- Reporting all relevant incidents in line with this policy;
- Provision of information and/or reports as requested as part of an investigation;
- Contributing to and learning lessons from investigations;
- Taking appropriate action to ensure incidents do not recur.

## 3. DEFINITIONS AND CRITERIA

3.1 **An accident: "**An unplanned event that causes injury to persons, damage to property or a combination of both and may be minor/ major/ fatal. Injury or harm to staff or other person, caused by an event."

3.2 **Adverse Incident** – “Any event or circumstances that could have been or did lead to harm, loss or damage to people, property, environment or reputation which includes an event that has, or may have, impacted upon the delivery of service or health improvement”.

Incidents include hazards (i.e. anything which has the potential under certain circumstances to cause injury, illness or harm), accidents (direct results of unsafe activities or conditions), dangerous occurrences and significant events.

Examples of incidents include:

- Any event that resulted in an adverse effect (however minor) on a service user / member of the public or member of staff;
- Failure of equipment, whether or not injury occurs;
- Serious damage to property to which NIPEC are tenants;
- Serious damage / loss / theft of NIPEC property;
- Damage, loss or theft to personal property whilst on NIPEC related business;
- Damage, loss or theft of personal property whilst on NIPEC property;
- Fire;
- Violence;
- Breaches of security;
- Lost records / Data Breaches;
- Illegal acts;
- Breach of Information Governance arrangements.

3.3 **A near miss:** An incident includes near misses. This is where any of the above may have happened had intervention or evasive action not been taken.

3.4 **Serious Adverse Incident (SAIs):** any incident which meets one or more of the following criteria should be reported as a SAI:

- Serious injury to, the unexpected / unexplained death of or unexpected risk to:
  - A service user
  - A staff member in the course of their work
  - A member of the public whilst visiting NIPEC offices.
- Unexpected or significant threat to provide service and/or maintain business continuity.

All Serious Adverse Incidents (SAIs) must be reported to NIPEC Council, Audit and Risk Committee and Sponsor Branch.

3.5. NIPEC’s IT service is managed by BSO ITS under a Service Level Agreement (SLA) and in the event of an IT incident, NIPEC staff will adhere to the BSO’s ICT Incident Management Procedure. Details of this are included in NIPEC’S Business Continuity Plan.

## 4. WHY REPORT AN INCIDENT?

4.1 The nature of NIPEC's business involves risks and things can go wrong. By analysing and tackling the root causes of incidents, these risks can be reduced and result in action being taken to reduce the risk of the same or similar incidents occurring.

4.2 There are obligations under legislation and Departmental Guidance to ensure effective management of incidents and accidents. These include but are not limited to:

- Circular HSC (SQSD) 08/2010 covers medical devices, serious equipment failings, fire, counter fraud and security management as well as serious incidents involving staff, service users or members of the public;
- The Social Security Act 1975 which requires a person who suffers personal injury by accident whilst at work to notify his employer or manager at the time of the accident;
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) Health and Safety legislation
- The Health and Safety at Work Act 1974 and NI Order 1978
- Management of Health and Safety at Work Regulations 1992
- Management of Health and Safety at Work Regulations (Northern Ireland) 2000
- Workplace (Health, Safety and Welfare) Regulations 1992
- Workplace (Health, Safety and Welfare) Regulations (Northern Ireland) 1993
- Manual Handling Operations Regulations 1992 (Amended 2004)
- Provision and Use of Work Equipment Regulations 1998 (PUWER 1998)
- General Data Protection Regulations (GDPR) 2016 / Data Protection Act 2018
- Provision and Use of Work Equipment Regulations (Northern Ireland) 1999
- Lifting Operations and Lifting Equipment Regulations 1998 (LOLER 1998)
- Lifting Operations and Lifting Equipment Regulations (Northern Ireland) 1999 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)
- Human Rights Act 1998
- Disability Discrimination Act 1995
- HSCB guidance on Serious Adverse Incidents as amended from time to time.

4.3 The process of reporting an incident aims to:

- Focus on service improvement for service users;
- Recognise the responsibilities of individual organisations and support them in ensuring compliance;
- Clarify the processes relating to the reporting, investigation, dissemination and implementation of learning arising from incidents which occur during the

course of the business of an HSC organisation /Special Agency or commissioned service;

- Keep the process for the reporting and review of SAIs under review to ensure it is fit for purpose and minimises unnecessary duplication. Where appropriate, the incident should be added to the Corporate Risk Register to ensure mitigation against a repeated incident is monitored;
- Ensure trends, best practice and learning is identified, disseminated and implemented in a timely manner, in order to prevent recurrence;
- Provide a mechanism to effectively share learning in a meaningful way across the HSC;
- Maintain a high quality of information and documentation within a time bound process.

## 5. REPORTING AND RECORDING OF INCIDENTS

All incidents should be reported as follows:

5.1 **All non-information related adverse incidents** (as described in Section 3) must be reported using the NIPEC's Incident Reporting Form (Appendix A). Completed forms should be forwarded by email to the Head of Corporate Services.

5.2 All **Serious Adverse Incidents** must be reported to the Health and Social Care Board (HSCB) as soon as possible via the Chief Executive's Office. NIPEC Council and Sponsor Branch, DoH, should also be informed as soon as possible via the Chief Executive's office or Head of Corporate Services.

5.3 All **Data breaches**, actual and suspected, must be reported to the Data Protection Officer via databreach@bso.hscni.net using the Data Breach Notification Form (Appendix B). These should be reported at the earliest opportunity and within 24 hours of a breach happening and copied to the Head of Corporate Services (HoCS) as NIPEC'S Senior Information Reporting Officer (SIRO).

The Head of Corporate Services will liaise with the Data Protection Officer to agree remedial action to mitigate the breach and where appropriate, whether the effected data subjects and Information Commissioner Office need to be informed.

In addition, data breaches that have originated in another organisation and have inadvertently led to the sharing of sensitive/personal information with a member of NIPEC staff, should also be reported to databreach@bso.hscni.net and copied to the HoCS. Those in receipt of such information should notify the sender of their error and destroy / delete the information and/or email(s) received.

5.3 **IT incidents** should be reported via BSO ITS vFire system. The BSO ITS Assistant Director or other relevant Senior Manager will manage ICT incidents in conjunction with BSO's ICT Incident Management Process.

5.4 Monitoring reports will be provided to NIPEC's Council / Audit and Risk Committee, Business Team, Information Governance Group, Health and Safety Committee by the relevant senior officer/manager as outlined within Section 2 above.

## 6. RIDDOR REQUIREMENT

6.1 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) require NIPEC to notify the Health and Safety Executive NI (HSENI) of accidents or dangerous occurrences at work. These reports enable the enforcing authorities to identify where and how risks arise and to investigate serious accidents.

6.2 Line managers have a duty to inform the Head of Corporate Services if an incident or accident has occurred to a member of staff which has resulted in 3 days or over sickness absence, i.e. it is RIDDOR reportable.

6.3 It is the responsibility of the Head of Corporate Services to inform HSENI of the details of the incident without delay (i.e. by telephone). This must be followed up within ten days with a completed RIDDOR report form (NI2508).

Further information can be found on the HSENI website www.hseni.gov.uk.

## 7. IMMEDIATE MANAGEMENT OF AN INCIDENT

7.1 The immediate responsibility for managing an incident falls to the most senior person on duty at the time the incident occurs. If the event is regarded as a Serious Adverse Incident, the Chief Executive and Head of Corporate Services must be informed immediately and they will decide whether to initiate Business Continuity Plan if required.

7.2 It is the responsibility of the most senior person on duty to:

- Make the situation safe;
- Provide or arrange any first aid or medical care as needed;
- Decide in conjunction with either the Chief Executive or Head of Corporate Services what other parties require to be informed;
- Ensure appropriate person(s) are informed;
- Ensure that an Incident Report Form (Appendix A) has been correctly and fully completed at the earliest opportunity and no later than two working days after the incident;
- If the incident relates to a Data Breach, the process outlined in 5.3 must be followed. Every reasonable effort must be made to locate and retrieve documents lost, altered and disclosed, and all communications concerning the data breach must be cleared by the Data Protection Officer / Head of Corporate Services.

## 8. INVESTIGATING AN INCIDENT

8.1 Investigations will be led by someone with the relevant expertise and any reports / recommendations approved by the Senior Management Team. The

lead investigator will be determined by the nature of the incident, who was involved and where it occurred. A risk adviser, health and safety adviser, information governance, technical staff, or equipment suppliers may need to be involved depending on the nature and seriousness of the incident.

8.2 Incident investigations should, if appropriate to the circumstances:

- Identify what happened by obtaining statements/interviewing relevant staff;
- Identify how and why it happened;
- Satisfy mandatory and reporting requirements;
- Provide a detailed report of the investigation, which identify the cause and outline actions necessary to either eliminate or significantly reduce the risk of the incident reoccurring;
- Identify areas of learning from incidents and make recommendations;
- Implement improvement strategies to help prevent, or minimise recurrences, thus reducing future risk of harm.

## 9. REFLECTION / LEARNING LESSONS

9.1 Incident reporting an investigation is a method of identifying problems and addressing these to reduce risk and improve safety. One method of achieving this is to use the lessons learned from incidents to review the systems and processes in place to assess whether modifications are required to prevent the same incident occurring in the future.

9.2 Dissemination of these lessons learned is essential to maximise the benefits of investigating incidents and will form part of the reporting process outlined in Section 5 above.

## 10. NIPEC PERFORMANCE AND CONDUCT PROCEDURES

10.1 Whilst the emphasis within NIPEC will be on treating all incidents as a learning experience, a failure to report an incident or an investigation or review of an incident may highlight issues that also need to be dealt with separately under the relevant performance and disciplinary procedures.

10.2 If such issues arise at any stage with the relevant manager they will be referred to BSO's Human Resource Directorate which will decide whether and when to take any separate action having considered all appropriate options. The investigation of the incident will continue even if a referral to the Human Resource Directorate has been made.

## 11. EQUALITY SCREENING

11.1 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 for … *[specify the groupings]* and outlines the way these will be addressed
or

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.

## 12. REVIEW

12.1 We are committed to ensuring that all policies and procedures are kept under review to ensure they remain compliant with relevant legislation and guidance.

12.2 This policy is based on a regional HSC policy. It will be monitored and reviewed in December 2023, or sooner if a revised HSC policy is issued.

**Signed:** _____ **Date:** _____

**Chief Executive**

**Appendix A**

# NIPEC INCIDENT REPORT FORM

**N.B. All incidents should be reported as soon as possible and within 24 hours of occurring**

This form should be completed electronically wherever possible. To do so, first save the form to your desktop and once completed, email this to the Head of Corporate Services.

| | |
|---|---|
| **Name:** | |
| **Incident date and time:** | |
| **Date reported:** | |
| **Line Manager:** | |

| **Description of Incident:** |
|---|
| |

| **Immediate Action Taken:** |
|---|
| |

| **Was any person injured or affected in the incident?** | **Yes / No** |
|---|---|
| If yes, please provide details | |

| **Were there any witnesses to the incident?** | **Yes / No** |
|---|---|
| If yes, please provide details | |

| **Was any other person involved in the incident?** | **Yes / No** |
|---|---|
| If yes, please provide details | |

| **Was there any equipment involved in the incident?** | **Yes / No** |
|---|---|
| If yes, please provide details | |

---

**For manager use only:**

| | |
|---|---|
| **Name:** | |
| **Date:** | |

**Type of incident** *(please tick as appropriate)***:**

| | |
|---|---|
| **Accident / Health & Safety** | |
| **Breach of Information Governance arrangements** | |
| **Data Breach** | |
| **Serious Adverse Incident (SAI)** | |
| **Near Miss** | |
| **Equipment failure / damage** | |
| **Accidental damage to or loss of NIPEC property** | |
| **Other:** *(give details below)* | |
| | |

| **Action Taken:** |
| --- |
| |

| **Date Closed:** | |
| --- | --- |

| **Outcome:** |
| --- |
| |

| **Learning:** |
| --- |
| |

| **Additional Information:** |
| --- |
| |

**Appendix B**

# NIPEC DATA BREACH REPORT FORM

**N.B. All data breaches should be reported as soon as possible and within 24 hours of occurring**

This form should be completed electronically wherever possible. To do so, first save the form to your desktop and once completed, email this to databreach@bso.hscni.net and NIPEC Head of Corporate Services.

## Section 1: Background Information

| | |
|---|---|
| **Date of Data Breach:** | |
| **Time of Data Breach:** | |
| **Location of Data Breach:** | |
| **Date of Notification:** | |
| **Name and Job Role of individual reporting Data Breach:** | |
| **Contact Email:** | |
| **Contact Telephone:** | |

## Section 2: Incident Details

| | |
|---|---|
| **Summary of the Data Breach:** | |
| | |
| **Department(s) affected:** | |
| **Nature of the Data Breach:** | |
| **Is the Data Breach ongoing?** | |
| **What action has been taken to mitigate the Data Breach?** | |
| | |

## Section 3: Information Compromised

| | |
|---|---|
| **What personal data has been breached?** | |
| **Category of personal data breached:** | |
| **Has a complaint been received by the data subject(s)?** | |
| **Number of people whose information is affected:** | |
| **Is there a risk of harm / danger to the individual(s)?** | |
| **Is there a risk of identity theft?** | |
| **Could the breach make the private aspects of a person's life known to others?** | |
| **Please provide any additional information to support the above:** | |
| | |

Once Sections 1-3 are completed, please save this form and submit it to databreach@bso.hscni.net and the Head of Corporate Services

## Section 4: Investigation

| | |
|---|---|
| **Incident Reference Number:** | |
| **Name and role of Investigating Officer(s):** | |
| | |
| **Can the information be recovered?** | |
| **Details of actions taken to attempt to recover the information:** | |
| | |

| What further action has been taken to minimise the possibility of a recurrence? | |
|---|---|
| | |
| **Is it necessary to notify the data subject(s)** | |
| **Please provide justification for the above:** | |
| | |
| **Is it necessary to inform a regulatory body?** | |
| **Please provide justification for the above:** | |
| | |
| **Has appropriate training been received?** | |
| **Please provide evidence of training:** | |
| | |

**Section 6: Conclusion**

| Please provide any additional information that may be useful: |
|---|
| |