NIPEC/23/10

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Clear Desk and Screen Policy

November 2023

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

4th Floor
James House
2-4 Cromac Avenue
BELFAST
BT7 2JA

https://nipec.hscni.net

Developed by:	Business Manager
Reviewed:	August 2017 December 2020 November 2023
Approved by / date:	BTM: 8th December 2020; 27 November 2023 Council: 31st December 2020; 6 December 2023
Date of next Review:	November 2026
Equality Screened by / date:	December 2020

CONTENTS

1. Introduction and Purpose

NIPEC has adopted a clear desk policy for papers and removable media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorised access, loss of and damage to information during and outside normal working hours.

This policy applies to **all staff** including Council members, regular full-time, regular part-time, associates, contractors, consultants, agency staff and temporary employees.

This policy should be read in conjunction with NIPEC's:

- Records Management Policy
- Information Governance Policy
- ICT Security Policies
- Data Protection Policy
- Security of NIPEC Property and Personal Property
- Provision, Usage and Security of NIPEC Mobiles and Smart Phones
- Relevant guidance, to include The Department of Health's (DoH) 'Good Management, Good Records' (February 2020).

The purpose of this policy is to protect Northern Ireland Practice and Education Council's (NIPEC) information from unauthorised disclosure, loss or damage. It establishes minimum requirements for a clear desk and screen environment, addressing the protection of hardcopy information, removable media and on-screen information.

2. Data Classification

All staff must be careful when handling any HSC information and especially when dealing with sensitive or personal data.

The Code of Practice on Protecting the Confidentiality of Service User Information document issued by DHSSPS in January 2009 provides guidance on the handling of personal information. The document can be found on the DHSSPS web site http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf

Examples of sensitive and personal information include but are not limited to: -

- Copies or extracts of data from clinical systems;
- Commercially sensitive information;
- Contracts under consideration;
- Budgets;
- Staff reports;

- Appointments – actual or potential not yet announced;
- Information containing personal identifiable information (i.e. names, addresses, personal email addresses, contact numbers);
- Disciplinary or criminal investigations.

Personal data is further defined in the UK General Data Protection Regulation (2018) which was implemented in the UK through the Data Protection Act 2018.

3. The Desk/Office Environment

The following controls should be adhered to:

- Keep filing cabinets, desk drawers and cupboards containing personal sensitive information closed and locked – store keys securely – do not leave keys in their locks;
- Papers and computer media containing personal or sensitive information (e.g. Iron keys) must be stored in a locked cabinet/cupboard when not in use, especially outside normal working hours;
- Confidential and sensitive information must be locked away when not required, especially when the office is not in use;
- Where possible, desks and PCs should be positioned so that sensitive material is not visible to people entering the office, or from either the windows or the hallway;
- Erase whiteboards at the end of meetings;
- Paperwork should be routinely cleared, shredding sensitive documents or placing these in confidential waste bags for authorised disposal;
- Personal information, e.g. salary slip or bank statement, should not be left on show or unattended as this contains key private information;
- Keep mobile devices with you, lock phones with a password;
- Keep your office area clear of clutter and clear your desk at the end of each day;
- Notify the Head of Corporate Services or Business Manager immediately if any confidential or personal information goes missing;
- Equipment in public areas must be locked with an approved locking cable or locked away in a drawer when left unattended;
- Where audio or video conferencing is used, it should take place in a non-public area with staff avoiding personal information or business sensitive information being seen or heard by unauthorised individuals;
- Staff must only store information in hardcopy form if absolutely necessary. Where appropriate, documents should be scanned, or information transferred, and stored digitally within an appropriate NIPEC Information System. Hardcopy versions must be disposed of in line with NIPEC record management policies and procedures. Where information is stored in hardcopy form, it must be stored in line with NIPEC

Records Management Policy. Staff must label the information in accordance with the local classification policy, and store it in a way that is commensurate to the classification of the information.

4. The PC Environment

The following controls should be adhered to in line with the ICT Security Policy:

- Never write passwords down for others to use or hide them in the office;
- Always 'lock' computers and laptops when leaving these unattended, even for a short period of time, by pressing Ctrl + Alt + Del and clicking on 'Lock this Computer' or by pressing the windows logo key + L;
- Shut down / turn off and secure computers and laptops if you leave at the end of the day or if leaving the office for a significant part of the day (computers and other IT equipment should be unplugged during periods of extended absence, e.g. annual leave);
- Minimise computer applications to prevent others from viewing sensitive data – this can be done by pressing the windows logo key + M;
- Staff must not leave removable media unattended;
- All staff must protect authentication information and devices from unauthorised disclosure.

5. Printers / Photocopiers

The following controls should be adhered to:

- When printing sensitive information, this should be picked up immediately. Where applicable, access controls must be implemented on printers and photocopiers to ensure staff are present during the print process;
- Staff should always log out in full of the MFD when printing is completed and should never use the device under another users' password.

6. Disposal Procedures

The following controls should be adhered to:

- Staff must continuously review any paper they hold and dispose of waste immediately;
- Where HSC information has been taken home or generated at home, in paper format always return it to the office for disposal;
- Never dispose of any HSC information via normal office cleaning services;

- Waste paper must not be allowed to build up in cupboards, drawers, filing cabinets, desks, floor space, around printers or communal areas as this is a fire hazard;
- Where information is extremely sensitive it should be shredded immediately using the office shredder;
- Bigger amounts of sensitive paper information for disposal should be placed in Confidential Waste bags (where possible this should be shredded) and stored in a locked area before being removed from the premises by the approved supplier;
- No bags should be allowed to become over full (i.e. cannot be comfortably and safely carried by one person) before sealing and removal to the nearest designated collection point;
- All removable media that contained HSC information and is no longer required must be disposed of via the approved Asset disposal company for destruction. Such transactions should be updated on the NIPEC Asset Register.

7. Monitoring Compliance

A copy of this policy will be given to all staff, who should be aware of and ensure this policy is followed on a daily basis. Line managers are required to ensure this policy is deployed within their area of responsibility.

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.

Staff must be aware that any data on the organisation’s systems and equipment remains the property of NIPEC. NIPEC reserves the right to monitor and record any use of organisation information and systems to ensure they are used for legitimate purposes, and that policies and standards are being complied with.

All monitoring must be undertaken in accordance with the appropriate legislation such as Regulation of Investigatory Powers Act (2000), Human Rights Act (1998), and good practice guidance such as “Employment Practices Code Part 3: Monitoring at Work” issued by Information Commissioners Office.

NIPEC may at any time, and without notice, conduct clear desk and screen compliance checks or audits, and may remove any information or equipment that is in breach of this policy. All users must co-operate fully with any such audit.

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

9. Review

This policy is based on a regional HSC policy. It will be monitored and reviewed in November 2026, or sooner, if a revised HSC policy is issued or following any significant incidents, changes to applicable UK or EU legislation or changes to the HSC structure or functional responsibilities.