NCL CCGs Clear Desk, Multi-Function Device (MFD) Printing & Physical Security Procedure V0.3

January 2020

Document revision history

Date	Version	Revision	Comment	Author
November 2018	0.1	New Procedure	Creation of Procedure	NEL IG Hub
November 2019	0.2	Revised Procedure	Revision of Procedure	IG Compliance Manager
January 2020	0.3	Review and formatting	Review of Procedure	IG Compliance Manager

Table of Contents

1. Introduction

This procedure relates to NHS Barnet, Enfield, Camden, Islington and Haringey Clinical Commissioning Groups, hereafter referenced as NCL CCGs

This procedure reduces the risk of data loss by ensuring no confidential information is left unattended throughout NCL CCGs locations. This protects the confidentiality and of information by ensuring it is not accessible to unauthorised persons outside normal working hours or when the custodian of the information is not there.

This procedure should also be read in conjunction with any other related documents that are or may become available across NCL CCGs.

1.1 Objectives

The objectives of this procedure are to create, maintain and ensure;-

- The safety of all who work within NCL CCGs
- The confidentiality and security of patient and staff information.
- The protection of property and assets against fraud, unauthorised access, loss, theft and wilful or accidental damage.

NCL CCGs aims to manage risks systematically and consistently. Everyone has a part to play in ensuring the highest possible standards of security are met throughout the organisation.

2. Scope

This procedure is intended to reflect the structure of NCL CCGs. The details on the roles, responsibilities and arrangements implemented in order to meet the obligations that apply to NCL CCGs are set out within this procedure. This procedure applies to all staff, teams and activities managed by NCL CCGs including interim, consultancy and agency staff based at all CCG localities.

This procedure aims to effectively manage safety of staff and information through proactive security measures, effective management systems and appropriate policies and procedures within NCL CCGs

3. Roles and Responsibilities

3.1 Managing Director

The Managing Director/Accountable Officer has overall responsibility for ensuring a safe working environment across NCL CCGs and ensuring that this procedure is implemented and adhered to by all CCG staff.

3.2 All Managers

All NCL CCGs managers are responsible for;-

- Familiarising themselves with this Procedure and raising awareness and understanding of Clear Desks, Multi-Function Devices, Printing and Physical Security within their work area.
- Reviewing their areas of work to identify any related risks, agree appropriate actions and escalate risks as necessary. `
- Fostering a supportive work environment to facilitate the reporting of security or data protection breaches in relation to this Procedure.
- Developing and implementing any local guidance or procedures necessary to the effective implementation of this Procedure.
- Ensuring staff have access to opportunities for training and development to further support this Procedure.
- Ensuring they and their staff wear their ID badge at all times whilst on the premises/in the building – see Appendix A.

- Ensuring that physical security and maintenance of clear desks are regular items of discussion at directorate and team meetings.
- Ensuring that agreed starters and leavers processes are adhered to when staff leave the organisation, e.g. Returning of assets, ID Cards and Smartcards.

3.3 All Staff

All NCL CCGs staff should;-

- Attend statutory and mandatory training,
- Co-operate with arrangements for minimising security and data protection risks,
- Work to organisational guidance, procedures and policies,
- Take reasonable care for their own safety and security and that of others,
- Take care of NCL CCGs buildings, equipment and other assets,
- Clear and lock away as appropriate all confidential and commercially sensitive data and information,
- Report risks, incidents and near misses,
- Not remove, interfere with or misuse, intentionally or recklessly, anything provided for security purposes,
- Return all assets and access cards to the organisation upon termination of their employment,
- Feel confident to challenge anyone unknown or not displaying an ID badge within restricted areas in the workplace.
- Be conscious of people acting suspiciously, and report any instances of this to a senior member of staff,
- Ensure that doors are closed securely behind them to prevent unauthorised access and tailgating.
- Not lend their ID badge or access card to any other person,
- Report the loss of and ID card or smartcard to their line manager immediately.

4. Clear Desks

As part of maintaining a secure and compliant workplace, staff should;-

- Ensure that all confidential and commercially sensitive data and information including paper based records are locked away as appropriate. It will be the responsibility of each member of staff to retain the key securely and for their use only.
- Confidential documents must not be left on desk or table tops overnight. All confidential documents must be locked away. NHS offices are routinely targeted by thieves.
- Ensure that where possible, electronic documents are used as an alternative to printing out paper copies.
- Dispose of documentation containing patient identifiable data in a secure manner, using either a confidential waste bin or an approved shredder.
- Not leave smartcards in readers when away from desks to prevent theft, loss or misuse.

5. Printing and Multi-Function Devices

5.1 Secure/Locked Printing

Locked Print can help prevent printing confidential information in error. It enables users to prevent confidential information being printed until they are ready to print out. The following are guidelines for ensuring secure printing.

All NCL CCGs staff should;-

- Review and test all printers installed on their computer to ensure print jobs are sent only to printers NCL CCGs use. Mistakenly printing to printers in another building after moving office is a common cause of breaches.
- Ensure that if a document fails to print, it should not just be re-printed. Staff should check whether there is paper in the printer first to prevent two copies being printed.
- Regularly check the default printer on PC's and Laptops.
- Ensure that if a document has been sent to a printer in error, take action to have that document collected and shredded.

- Where the Locked Print facility is not available and staff members need to print confidential documents, NCL CCGs must ensure the printer is kept in a controlled environment which only provides access to authorised users.

5.2 Multi-Function Devices

A Multi-Function Device (MFD) is a device that performs a variety of functions that would otherwise be carried out by separate devices. As a rule, an MFD includes at least two of the following: printer, scanner or copier.

When using an MFD NCL CCGs staff should;-

- Ensure that after copying or scanning documents, documents are removed from the scanner or copied section.
- Scan or copy documents direct to their NHS Mail account rather than to paper.
- Double check email addresses before scanning or copying direct to them.

6. Physical Security

Physical security involves more than just technical controls. It also involves security awareness, business processes, operating procedures, and organisational policies. These various aspects of physical security must harmonise with one another and support the organisation's mission and vision. A Physical Security Risk Assessment helps improve an organisation's physical security program so that these goals can be met. It is vital for the organisations to take a proactive approach to physical security governance because doing so will help NCL CCGs protect their most valuable assets.

It is the responsibility of all staff working in NHS premises to keep their work area and buildings secure.

6.1 General Physical and Environment Security

The following controls will apply across NCL CCGs premises;-

- The premises will be controlled and protected with security barriers and access controls to limit access on a strict need-to-access basis only.
-

CCTV cameras will be installed and operated for the safety of staff and visitors, and for the prevention and detection of crime.

- ID Badges and access cards will be issued for each member of staff.
- All storage cabinets and cupboards must be locked to prevent unauthorised access or tampering at the end of each day or when offices or departmental areas are vacated.
- Intruder alarms will be operated and maintained as appropriate.
- Fire detection systems are in place and tested regularly.
- Staff should not prop open fire doors or disable access-controlled doors.
- At the end of the day windows should be secured, particularly those located on the ground floor, as these can provide an easy access to unauthorised individuals.

6.2 Visitors and Third Party Access

The following controls should be followed on NCL CCGs premises;-

- Third party access to any NCL CCGs premises, assets and services will be based on an approved contract between the organisation and the third party.
- All third party and visitor access to NCL CCGs premises will be logged, including the name of the individual, time of arrival/departure and reason for visit.
- Where necessary, the audit trail for third party and visitor access will be maintained for 12 months after the visit.
- Off-site facilities and storage services provided by third parties must comply with the above requirements in full.

7. Confidentiality Audits

A Confidentiality Audit reviews organisational practice and security and focusses on the day-to-day procedures, controls and behaviours throughout the organisation.

This audit is nationally mandated and NCL CCGs must provide the audit report, based on the findings of the audit to NHS Digital as part of overall annual information governance compliance standards assurance. This is done through upload to the Data Security and Protection Toolkit.

As part of the audit, staff may be asked some general questions about day-to-day practice for handling patient, organisational or staff data. Staff engagement with this audit and honest responses helps the organisation formulate staff communications and procedures around important processes and areas of knowledge.

8. Training

Training will be delivered to all staff (including Senior Management) in line with NCL CCGs Statutory and Mandatory training. Mandatory training will be given to all new starters at induction. This will include Health & Safety Training and Information Governance. Further essential training will be identified by managers during appraisals.

9. Dissemination and Implementation

This procedure will be disseminated throughout NCL CCGs via the Communications team, relevant managers, team meetings and staff briefings. It is also available on the intranet.

Specific responsibilities for upholding this procedure will be outlined in the Job Descriptions of relevant members of staff.

10. Review

This procedure will be reviewed in one year, or earlier if there are changes to National Guidance or significant changes to the management of risk across the organisation.

Appendix A - NCL CCGs ID Badge Protocol

Introduction

Security is increasingly important, affecting visitors and staff. This protocol details one of the processes NCL CCGs have introduced to ensure a safer and more secure working environment.

The ID Badge will carry a photograph of the individual, along with their name, job title, department, location and the organisation logo.

Scope

This protocol applies to all staff employed within the organisation on a permanent or temporary basis including agency staff and contractors.

Responsibilities

All staff have a responsibility to;-

- Work to NCL CCGs guidance, policies and procedures.
- Wear (visibly) their ID Badge at all times whilst on the premises.
- Not lend their ID Badge or access card to any other person.
- Report the loss of and ID Badge or Access Card immediately to a senior manager, and complete an incident form.
- Challenge anyone not displaying an ID badge within restricted areas of the workplace – staff should not, under any circumstances, place themselves in confrontational positions which places them in personal danger.
- Take the time to secure doors behind them to prevent unauthorised access to the premises via tailgating.
- Return all assets and security cards to the organisation upon termination of employment.

All managers are responsible for;-

- Ensuring that they and their staff wear their ID badge at all times whilst on the premises.
- Ensuring agreed checklists are adhered to when staff leave, e.g. returning of assets, ID Badge and Access Cards.