NHS
North East and North Cumbria

Corporate	ICBP030 - Physical Security Policy

Version Number	Date Issued	Review Date
2	December 2022	December 2024

Prepared By:	Senior Governance Manager, North of England Commissioning Support Unit (NECS)
Consultation Process:	Integrated Care System (ICS) Integrated Governance Workstream
Formally Approved:	December 2022
Approved By:	Executive Committee

EQUALITY IMPACT ASSESSMENT

Date	Issues
March 2022	None identified

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3-year period.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
1.0	July 2022	Senior Governance Manager, NECS	First issue.
2.0	December 2022	Senior Governance Manager, NECS	Reviewed within the first 6 months of the establishment of the Integrated Care Board (ICB), minor amendments have been made.

Approval

Role	**Name**	**Date**
Approver	ICB Board	July 2022
Approver	Executive Committee	December 2022

Contents

1. Introduction

For the purposes of this policy the NHS Integrated Care Board (ICB) will be referred to as 'the ICB'.

The ICB aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients, their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the ICB will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

The ICB is committed to promoting and improving security for all of its staff, patients and visitors. The ICB aims to provide and maintain a calm, pleasant and secure working environment, where patients, visitors and staff are confident of their personal safety and the security of their property, buildings and equipment are safeguarded. Whilst the ICB recognises that it would be impossible to prevent every security incident it will provide resources to assist in handling such matters.

All ICB employees have a responsibility to ensure that security measures and procedures are observed at all times. Managers of the ICB should take a leading role in promoting and developing a security conscious culture.

1.1 Status

This policy is a corporate policy.

1.2 Purpose and scope

The ICB is committed to promoting and improving the security of its premises/assets and the safety of staff, patients and visitors to the ICB. The ICB will do its utmost to safeguard against crime and against loss or damage to property and equipment.

The ICB recognises and accepts its responsibility to provide a safe and healthy workplace and working environment for all employees and for those using its premises as required by the Health and Safety at Work etc. Act 1974.

Security is the responsibility of all staff in not only safeguarding their own wellbeing and personal property but also that of visitors and ICB property. The primary objectives of security management are:

- the prevention of violent or aggressive behaviour towards ICB staff, patients, clients and visitors;
- the protection of life from malicious criminal activity or other hazards;
- the protection of premises and assets against fraud, theft and damage;
- the smooth and uninterrupted delivery of health care;
- the detection and reporting of suspected offenders committing offences against patients, clients, staff, property or private property within ICB premises;
- the education of all staff in proactive security and general security awareness.

Security management can be defined as an environment where the risks to people and property are minimised from any actions that may lead to personal injury, threat to life or the disruption of the business activity of the ICB.

Effective security management is linked to other policy areas, including but not limited to counter fraud, the management of violence and aggression and lone working.

2. Definitions

The following terms are used in this document:

ICB – Integrated Care Board,
NHS – National Health Service,
LSMS – Local Security Management Specialist.

2.1 Designated Manager for Security

The Designated Director for Security within the ICB is the Director of Corporate Governance, Communications and Involvement.

3. Security Policy

3.1 Responsibilities of ICB managers

All managers in the ICB are responsible for security within their work area. Managers are required to assess security risks as part of the general assessments for their department/service, develop action plans and implement security measures.

Managers' responsibilities are summarised in section 8, below.

3.2 Responsibilities of ICB employees

All ICB employees, whether permanent, temporary or working through an agency or other third party, are responsible for acquainting themselves with this policy, following the guidance contained in it and complying with all security measures in their department.

Employee responsibilities are summarised in the schedule of duties and responsibilities.

3.3 Security of Physical Environment

Appropriate security controls and processes will be implemented to ensure the physical and environmental security of facilities. These processes will include controls to prevent unauthorised physical access, damage, loss, theft and interference to the organisation's facilities.

The following measures are in place within ICB to ensure physical security:

- within ICB offices there may be restricted areas in line with the organisation's requirements;
- communication rooms formally known as IT server rooms are "secure areas", and can only be accessed by identified staff;
- ICB sites will only be accessible using security access devices (Cards, Fobs, Tokens, digital locks) or lock and key;
- authorised staff must follow appropriate guidelines for working in secure areas, eg communication rooms, please refer to ICT CSU for guidance;
- 'tailgating' is not permitted on any ICB sites;
- arrangements are in place for the unlocking and locking-up of premises;
- lone working/ personal safety please refer to 'ICB's Lone Working Procedure';
- contractors attending site should be agreed with ICB and Landlords/NHS Property Services (NHSPS);
- power and telephone cabling is protected from interception, interference and damage.

3.4 Unauthorised visitors

Staff should be alert to the fact that the organisation may receive unauthorised visitors. Staff who identify potential unauthorised visitors to ICB sites should alert their line manager immediately. Any such visitors should be approached only if it is thought safe to do so. If someone is identified in ICB work areas who has no legitimate reason to be there, they should be asked respectfully to leave.

3.5 Bomb Threats

The vast majority of bomb threats are hoaxes. Making such malicious calls is an offence contrary to S*ection 51 of the Criminal Law Act 1977* and should always be reported to the Police with support from the LSMS. Any member of staff receiving such a call should seek the immediate advice of the most senior manager available and contact necsu.healthandsafety@nhs.net. Any suspicious packages must not be moved and should be reported to the Health and Safety Team for advice.

4. Building Access

4.1 Security access devices (cards, fobs, tokens)

Security devices are allocated/returned to staff via the HR new starter/leavers process.

- Lost security devices should be reported via the incident reporting system (SIRMS) before a replacement fob can be issued.
- Lost devices should also be reported to your Line Manager.
- Security devices should not be shared with others.

4.2 Identification Badges

ID Badges are issued to all staff on commencement of employment. ID badges must be worn at all times whilst on ICB premises or when undertaking ICB business. Persons not wearing an ID badge should be challenged and asked to identify themselves.

When staff leave ICB employment, all ID badges should be returned to the Line Manager and destroyed as per the HR leavers process. If an ID badge is lost or stolen this must be reported to the Line Manager and reported onto the incident reporting system (SIRMS) before a new ID badge is supplied.

4.3 Visitors / Contractors

All visitors/contractors are to be signed in and out of ICB premises and issued with a visitor pass, which must be displayed at all times whilst on ICB premises. For security reasons all visitors must be escorted to and from their destination within ICB buildings.

5. ICB Property/Assets

All ICB property should be securely managed. Managers and staff should follow the roles and responsibilities set out within this procedure. All IT equipment is secured behind door access controls with the exception of some reception areas where the desktop PCs are encrypted.

It is an offence for members of staff to remove property belonging to the ICB without receiving prior authority from their Line Manager or the custodian of the equipment. Failure to seek authority could result in disciplinary action or criminal proceedings being taken.

5.1 **Personal Property/assets**

Staff should be aware that the ICB cannot accept liability for loss or damage to staff property brought onto its premises.

- Staff are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work. Where storage has been provided for personal use, the individual to whom it is allocated will be responsible for ensuring it is locked.

- Staff must report any loss of or damage to their belongings and co-operate in any consequent inquiry into the loss or damage. If private property has been stolen, then it is the owner's and not the ICB's responsibility to report the matter to the Police. This should be after notifying a Line Manager and reporting the incident on the ICB incident reporting system (SIRMS). Any incident management or Police reference number assigned should also be recorded on the incident log.

6. Security of Information

All safeguards should be taken by staff who handle, receive and use confidential patient/personal information. It is essential that all staff within the ICB understand and follow relevant Information Governance policies which can be found on the ICB's intranet or website.

7. Security of Motor Vehicles

7.1 The ICB cannot accept liability for any motor vehicle or its contents when they are parked on an ICB site or when the vehicle is in being used by staff on ICB business, please refer to the ICB Driving at Work Policy.

7.2 **Lease Cars**

In the event of an incident or accident involving a lease car, the employee must notify their manager and the lease company in accordance with the car lease agreement and also report onto the incident reporting system.

8. Prevention of Violence to Staff

The ICB has a duty to provide a safe and secure environment for all employees and visitors and has a zero-tolerance approach to violence or abusive behaviour. The ICB takes a very serious view of violence, abuse and aggression at work and recognises its responsibility to protect employees and others who may be subjected to any acts of violence, abuse or aggression whether or not the act results in physical or non-physical assault and whether carried out by members of the public, patients, relatives or by members of staff. Violent or abusive behaviour will not be tolerated, and decisive action will be taken by the ICB to protect staff and visitors.

Please refer to lone working procedures available on the ICB's intranet site and the Violence Aggression and Abuse Management Policy.

9. Reporting of Security Incidents

All staff have a responsibility to report all crimes and breaches of security and should refer to the Incident Reporting and Management Policy.

Reporting falls into the following categories:

- **Assault or abuse of a staff member or visitor**. All incidents of assault or abuse must be reported through the incident reporting system and should be reported as soon as practical after the incident. All physical assaults to staff should be reported by the Manager through the incident reporting system (SIRMS). Visitors and staff should always be asked if they would like the Police to be involved.

- Where a **security incident or crime is in progress** it should be reported immediately to the Police and the senior manager on site and advice sought from the LSMS if required. The incident must be reported via the incident reporting system (SIRMS) as soon as possible after the incident and passed on as per the ICB's Incident Reporting and Management Policy.

- Where a **criminal incident is discovered after the fact** and the time of the offence is not known, the incident must be reported as soon as the crime is discovered and then dealt with in line with the ICB Incident Reporting and Management Policy. The manager should then inform the Police as it may be necessary to obtain a crime reference number for insurance purposes etc.

- Where a security incident involved the **theft of personal information** this must immediately be reported via SIRMS. Any theft or loss of data storage e.g. computer, laptop etc should all be reported in this way. Also, incidents where systems are suspected of being compromised should be reported on SIRMS.

- Where a security incident involved the **theft of patient identifiable information** this must immediately be reported to the Senior Information Risk Owner, Caldicott Guardian; Data Protection Officer and the Director of Corporate Governance, Communications and Involvement (or nominated deputy). Any theft or loss of data storage e.g. computer, laptop, should all be reported in this way as well as via the incident reporting form.

- All cases of **suspected fraud or corruption** should be notified immediately to the relevant director who will then give advice or arrange investigation of the incident.

10. Prevent Duty

The ICB should have due regard to compliance with the requirements of the Prevent Duty guidance for England and Wales. With regard to security management this will include:

- Using meeting request forms with relevant information detailing who to contact should there be a concern if rooms or buildings are being used for radicalisation/terrorism;
- Ensuring staff know which personnel to contact if there are concerns relating to the use of the building - this will include contact details for the Governance Manager for H&S who has responsibility for Security within the ICB demised area and to also ensure the Prevent Referral Pathway is followed if applicable.
- Ensure staff have received Prevent training as per Prevent Policy and that staff report issues to relevant managers for escalation relating to terrorism and radicalisation
- Have an identified Prevent Lead.

11. Implementation

11.1 This policy will be available to all staff for use in the circumstances described on the title page.

11.2 All managers are responsible for ensuring that relevant staff within the ICB have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

12. Training Implications

It has been determined that there are no specific training requirements associated with this policy.

13. Related Documents

13.1 Other related policy documents

- Violence, Aggression and Abuse Management Policy
- Prevent Policy
- Lone Working Policy

13.2 Legislation and statutory requirements

- Health and Safety Executive (1974) *Health and Safety at Work etc Act 1974*. London HSE.

14. Monitoring, Review and Archiving

14.1 Monitoring

The ICB Board will agree with the sponsor Executive Director a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

14.2 Review

14.2.1 The ICB Board will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

14.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Executive Director (or nominated deputy) will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

14.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

14.3 Archiving

The ICB Board will ensure that archived copies of superseded policy documents are retained in accordance with the NHS Records Management Code of Practice 2021.

15. Equality Analysis

Equality Impact Assessment
Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Lee Crowe
Job Title: Senior Governance Manager
Organisation: NECS

Title of the service/project or policy: Physical Security policy

Is this a;
Strategy / Policy ☒Service Review ☐ Project ☐
Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:
The aim of the policy is to ensure ICB considers Health and Safety along with its other business objectives and to ensure that the ICB follows the details stipulated within H&S Regulations.

Who will the project/service /policy / decision impact?
(Consider the actual and potential impact)

- **Staff ☒**
- **Service User / Patients ☐**
- **Other Public Sector Organisations☐**
- **Voluntary / Community groups / Trade Unions ☐**
- **Others, please specify** Click here to enter text.

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community	☐	☒

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

The policy is a review of an existing policy and has received only minor updates. There is no fundamental change to the content therefore the previous EIA which concluded 'no impact' remains appropriate

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Claire Riley	Executive Director of Corporate Governance, Communications and Involvement	June 2022

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

Schedule of Duties and Responsibilities

ICB Board	The ICB Board has responsibility for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Executive Committee	The Executive Committee is responsible for formal review and approval of organisational process documents.
Chief Executive	The Chief Executive has overall responsibility for the strategic direction and operational management, including ensuring that ICB process documents comply with all legal, statutory and good practice guidance requirements.
Director of Corporate Governance, Communications and Involvement	The Designated Director for Security within the ICB is the Director of Corporate Governance, Communications and Involvement
Management responsibility	All directors, managers and supervisory staff are responsible for the adherence and monitoring compliance with this policy. In particular they shall ensure: • Arrangements are in place to ensure the security of premises and assets and the safety of staff, patients and visitors taking all preventative measures to safeguard people and property (including occupied but not owned by the ICB). • That risk assessments are in place and where significant security risks exist local procedures are in place to minimise or reduce the impact. • That staff are aware of local and ICB security procedures and the results of risk assessments by effective training and communication. • Security arrangements are reviewed following incidents and ensure necessary changes in procedures are implemented. • Disciplinary procedures are initiated for staff who breach security arrangements. • That all criminal activities are reported to the Police and that all security incidents are reported and safeguard are completed. • That all staff are briefed with regard to their own personal security and local procedures, and where appropriate, are supported to attend security training. • That all staff are issued with staff identification badges (ID badges).

	• That work areas under their control are operated in accordance with this policy and any associated procedures. • That all breaches of security arrangements are investigated and reported immediately in accordance with laid down procedures. • That all staff on leaving the ICB return their ID badges, uniforms, keys and electronic passes. • That rules with regard to confidential paperwork are adhered to. • That advice is sought, as appropriate, from the LSMS and others where there is any doubt as to the standards that are to be applied in adhering to this policy. • That arrangements are in place to summon the Chief Executive or appointed deputy directly in the event of any serious incident occurring in the area under their control. • That official visitors/contractors are issued with the relevant visitor badge and this is monitored to ensure they are carried at all times when on ICB premises. • That all security incidents are recorded using the ICB's incident reporting system (SIRMS). • That any suspicion of fraud is reported to the local counter fraud service. • That a response is made at the earliest opportunity to any request from employees for advice on security concerns. • That appropriate support is given to staff involved in any security related incident.
Employees' responsibility	All employees have a duty to co-operate with the implementation of this policy. In particular it should be ensured: • That they are vigilant and responsible in the workplace, bringing to the attention of their immediate manager, as appropriate, any suspicious activity they observe on ICB premises. • That they attend appropriate security training or education. • That they co-operate with managers to achieve the aims of the security policy, highlighting any identified risks. • That they complete incident report forms for all security related incidents. • That they wear their staff identification badges at all times. • That they report immediately to their departmental manager any loss of or malicious harm to their own patients.

	• Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.