NHS
Staffordshire and Stoke-on-Trent
Integrated Care Board

Security Management Policy

Job Title of Policy Author	Associate Director of Special Projects
Review/Development Body	Staff Engagement Group
Ratification Body	People Culture and Inclusion Committee
Date of Ratification/Effective from	June 2025
Review Date	June 2028
Document Reference Number *(supplied by Governance Team)*	CG-P-008
Target audience	All ICB staff, non-executive Directors, temporary staff and contractors

Contents

CONSULTATION SCHEDULE	
Date	**Groups consulted**
March 2025	Staff Engagement Group
May 2025	ICB Policy Group
June 2025	

IMPACT ASSESSMENTS		
	Date Completed	**Comments**
Equality Impact Assessment (EIA)	07/03/2025	*No impact identified*
Quality Impact Assessment (QIA)	NA	(*for no impact insert: No impact identified)* *(If non-applicable insert N/A)*
Data Protection Impact Assessment (DPIA)	NA	(*for no impact insert: No impact identified)* *(If non-applicable insert N/A)*

VERSION CONTROL				
Version	**Job Title of Lead/Policy Author**	**Ratification Date**	**Ratification Body**	**Summary of Amendments**
1.0	Andy Collins CSU	Apr 2013		New
2.0	Tracey Revill	Sep 2019		Combined for 6 ICB
3.0	Jane Chapman	Jul 2022		Adapted for ICB
4.0	Kirsten Owen		Integrated Care Board	Update and rewrite

Document Status: This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

1. Introduction

For the purposes of this policy Staffordshire and Stoke-on-Trent 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.

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.

The ICB recognises that it is not feasible to eliminate all security incidents, it is committed to providing the necessary resources and support to effectively manage and respond to such occurrences, as outlined in this policy.

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

2. Purpose

The purpose of this policy is to detail the ICB's aims and responsibility for the effective management of security in relation to staff, patients, visitors and property. The ICB is committed to the provision of safeguards against crime and the loss or damage to its property and/or equipment.

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

It is responsibility of all staff, to ensure their own personal property, patients, visitors and ICB property are managed securely.
The primary objectives of security management are:

- Prevention of violent or aggressive behaviour towards ICB staff, patients,
- clients and visitors.
- Protection of life from malicious criminal activity or other hazards.
- Protection of premises and assets against fraud, theft and damage.
- Smooth and uninterrupted delivery of health care.

- Detection and reporting of suspected offenders committing offences against patients, , staff, property or private property within ICB premises.
- Education and awareness 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.

3. Scope

This Policy applies to all directorates, services and departments of the ICB including contracted or embedded staff and in all aspects of its activities.

This Policy covers the security of staff, contractors, visitors and property within. It focuses on improving and sustaining physical and personal security.

4. Definitions

Physical Assault	**The intentional application of force to the person, without lawful justification, resulting in physical injury or personal discomfort.**
Non-Physical Assault	The use of inappropriate words or behaviour causing distress and/or constituting harassment.

5. Duties and Responsibilities

5.1 Director of Corporate Governance

The Director of Corporate Governance has the responsibility for raising the profile of security management work within the organisation and at ICB Board level , in gaining their support and backing for important security management strategies and initiatives

5.2 Associate Director for Special Projects

Associate Director for Special Projects supports the Director of Corporate Governance in the delivery of their responsibilities, developing and refreshing the organisations policies, procedures and plans to ensure the safety and security of ICB members of staff, visitors and contractors.

5.3 Directors

It is the responsibility of all Directors to disseminate the Security Management Policy within the area of their responsibility. Ensure the co-ordination of security issues with other employers who share the worksite with the ICB. Ensure the implementation of the Security Management Policy within the area of their responsibility by providing support and advice to their managers.

5.4 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 appendix A

5.5 All Staff

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.

Annual leave plays a vital role in supporting employee wellbeing, productivity, and work-life balance by ensuring time is allocated for rest and recuperation. Staff are strongly encouraged **not** to take **work laptops, phones, or undertake work-related tasks during their holidays**, as this detracts from the intended benefits of leave. Unless required for work purposes, employees should leave work equipment at home to maximise their break. If it is necessary to use work devices—for example, during a "workation"—staff must first confirm compliance with company policy and insurance guidelines.

For both domestic and international travel, formal agreement and documentation must be obtained in advance from your Line Manager, with technical feasibility confirmed through the Health Informatics Service (via a Service Desk ticket). While it may be technically possible to arrange such access, approval is subject to specific exemptions and circumstances. Explicit authorisation from your Line Manager, documented by email, is required for audit purposes.

Prior to travel, employees must review ICB and SSHIS IG-IT data security, data protection, and networking policies, and arrange a secure VPN via the Health Informatics Service. Consider all relevant legal and country-specific data import/export restrictions, including those concerning encrypted ICB devices, as advised by the Foreign travel advice - GOV.UK service.

If using personal or "Bring Your Own Device" (BYOD) equipment, it may only be used for O365 connections to ICB Teams meetings and must not be used to access the corporate network. IT-IG security and insurance liability for personal devices remain solely with the employee; ICB coverage does not extend to personal equipment. Even when only personal devices are taken abroad, prior approval from SSHIS is required, as this may trigger security alerts or breach data protection regulations.

To mitigate IT and cyber security risks, always use a secure VPN, ensure full disk encryption is enabled, and keep all ICB software up to date. Avoid using public Wi-Fi networks unless appropriate protections are in place.

International travel may subject your laptop to customs or security inspections, and certain countries impose strict regulations on technology, data, and encrypted devices. Some destinations prohibit the entry of devices entirely (refer to Foreign, Commonwealth & Development Office advice for areas that UK citizens should not travel to). Devices should be carried in hand luggage to minimise the risk of loss or damage.

Employee responsibilities are summarised in in appendix A

6. Subject Matter of Policy

6.1 Security of the 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
- '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 Policy'
- contractors attending site should be agreed with ICB and Landlords/NHSProperty Services (NHSPS)
- power and telephone cabling is protected from interception, interference and damage.

6.2 Unauthorised visitors

Staff should be alert to the fact that the organisation may receive unauthorised visitors. Staff who identify potential unauthorised visitors to the ICB site should alert their line manage immediately. Any such visitors should be approached only it is thought safe to do so. If someone identified in the ICB work areas who has no legitimate reason to be there, they should be asked respectfully to leave. If they refuse to leave the Police should be alerted managers in the ICB are responsible for security within their work area, see appendix C reporting incidents to the police.

6.3 Security access devices (cards, fob, token)

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

- Lost security devices should be reported via the incident reporting management system (IRMS) 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.

6.4 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 management system (IRMS) before a new ID badge is supplied.

6.5 Authorised visitors

Authorised visitors who are attending ICB offices, should be issued with a NHS visitor pass which must be displayed at all times while they are on the premises.

This will be signed for in the register held at the appropriate reception area. The member of staff who is responsible for the visitor will then arrange for them to be escorted to the relevant department.

On leaving, the visitor's pass should be reclaimed. All relevant times should be recorded in the register held within the department.

6.6 ICB Property / assets

The ICB will provide staff with equipment e.g. phones and laptops, for staff members to conduct their work. Staff must take care of equipment and ensure it is secure at all times. Staff must take care when off site and travelling to another meeting or venue, with the ICB's equipment/assets.

Staff who are deemed to have acted carelessly with the ICB's equipment/assets may be subject to disciplinary proceedings.

Should a department want to replace this item then replacement would be at the discretion of the Director of Corporate Governance and may have to be funded out of that department's budget.

6.7 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 their Line Manager and reporting the incident on the ICB incident reporting management system (IRMS). Any incident management or Police reference number assigned should also be recorded on the incident log.

6.8 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.

6.9 Security of motor vehicles

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 being used by staff on ICB business.

6.10 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 (IRMS).

6.11 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.

Refer to the **lone working** procedures available on the ICB intranet site and the **Violence Aggression and Abuse Management** policy.

6.12 Reporting of security incidents

All staff have a responsibility to report all crimes and breaches of security and should refer to the incident reporting information in appendix B and reporting any incidents to the Police appendix C.

Reporting falls into the following categories:

- **Assault, abuse or aggressive behaviour to a member of staff or visitor:** All incidents of assault, abuse or aggression 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 management system (IRMS). Staff and Visitors 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 should seek advice from the Director of Corporate Governance if required. The incident must be reported via the incident reporting management system (IRMS) as soon as possible after the incident.
- 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 possible after the crime has been discovered, to the **Director of Corporate Governance** and reported on the incident reporting management system (IRMS). The **Director of Corporate Governance or** the **Associate Director for Health and Safety** should then inform the Police to report the incident, ideally the person who discovered the crime should also be available for the call. It may be necessary to obtain a crime reference number, for insurance purposes etc.
- Where a security incident involved the theft of **Personal Information, patient identifiable information**, this must immediately be reported to the Senior Information Risk Owner, Caldicott Guardian; Data Protection Officer, details can be found in the Information Governance Handbook and policy.
- 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, details can be found in IAN regarding fraud or corruption.

7. Training and Implementation

This is an established policy which has been embedded within the organisation for a number of years, hence no implementation plan is needed as relevant processes are already in place.

8. Monitoring

The ICB People and Inclusion Committee 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.

9. Review, Ratification and Archiving

The policy will be reviewed every 3 years, or earlier if national policy or guidance, organisational changes are required to be considered. The review will then be subject to review and re-ratification.

The Corporate Governance Team is responsible for ensuring that archive copies of superseded working documents are retained. All policies which have been superseded will be archived.

10. Dissemination and Publication

Dissemination of the final policy is the responsibility of the author. They must ensure the policy is uploaded on the intranet via the Communications Team. The Communications team is responsible to issue an organisation-wide notification of the existence of the Policy.

Heads of Departments/Managers are responsible for ensuring that all staff (including bank, agency, contracted and volunteers) have access to and are made aware of policies that apply to them.

All staff will be able to access copies of policies via the policy section of the ICB intranet.'

11. References and Associated Documents

Other related policy documents

- Information Governance Handbook
- Health and Safety policy
- Lone working policy
- Domestic abuse policy
- Violences, Aggression and Abuse Management Policy (link pending)

Legislation and statutory requirements

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

12. Impact Assessments

This policy has been through an Initial Assessment process and no identifiable or potential adverse impact against any protected characteristics or inclusion health group have been identified or mitigating actions have been taken. In the event of any new data, information or reporting, identifying any adverse or potential adverse impact, this assessment will be reviewed, and a full impact assessment will be carried out where it is deemed necessary to do so. Accessible and inclusive Information and equality monitoring (where it is practical to do so) have been considered.

13. Appendices

Appendix A Schedule of Duties and Responsibilities

ICB Board	The ICB board has responsibility for setting the strategi context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents
Chief Executive	The Chief Executive has overall responsibility for the strategic direction and operational manager, including ensuring the ICB process documents comply with all legal and statutory and good practice guidance requirements
Director of Corporate Governance	The Designated Director for Safety and Security within the ICB is the Director of Corporate Governance.
Associate Director for Special Projects	The specific responsibilities of the Associate Director for Safety and Security are to: • ensure the ICB is tackling violence against staff across the organisation, acting as lead for the reporting of all verbal and physical abuse of staff and ensuring that relevant incidents are reported to external bodies as necessary. • the development, implementation and maintenance of an effective Security Management Policy, and other security related documents, in consultation with staff representatives, ensuring compliance with current guidance. • to prepare a written work plan, with the Security Management Executive Director (CoS) and preparing regular reports on progress against that plan. • assist local managers in carrying out investigations into security related incidents, liaising as required with local Police, the Criminal Justice Unit and where necessary preparing case files for submission to Court as part of the prosecution process. • instigate regular campaigns to highlight the importance of security and the responsibilities of all ICB employees. • advise the ICB of any statutory requirements, and other by the preparation of procedures, for dealing with crime prevention, supply of security systems and maintenance. • to foster links with local agencies and bodies, such as Police, Crime and Disorder Reduction Partnerships, Prevent (Counter Terrorism) leads and other security professionals in neighbouring NHS organisations.

	• to develop processes and undertake monitoring of the security management arrangements of providers of NHS funded care in accordance with NHS Protect Standards for Commissioners.
Management responsibility	All directors and managers 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 presentative 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 the local and ICB security procedures and the results of risk assessments by effective training and communication • Security arrangements are reviewed following incident and ensure necessary changes in procedures re 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 safeguards are complete • 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 reporting immediately in accordance with the laid down procedures. • That all staff on leaving the ICB return their ID badges and electronic passes. • That rules with regards to confidential paperwork are adhered to. • That advice is sought, as appropriate, from the Director of Corporate Governance 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 areas under their control.

	• The official visitors are issued with the relevant visitor badge and monitored to ensure they are carried at all times when on ICB premises • That all security incidents are recorded using the ICBs incident reporting management system (IRMS). • 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 for the workplace, bringing to the attending of their immediate manager, as appropriate, any auspicious 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 always wear their staff identification badge, while on ICB premises • That they report immediately to their manager any loss or malicious harm to their own patients • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken • Co-operation 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 in 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 brining to them to the attention of their line manager.

Appendix B Reporting incidents

All instances of concerns about and / or incidents of violence, aggression, bullying, harassment, discrimination or potential vexatious/ unreasonably persistent behaviours should be reported using the ICB Incident Reporting System found on IAN Health and Safety site.

Incident reporting management system (IRMS)

Ideally the individual employee raising the concern should report the incident including the following information:

- Date, time, and location of incident.
- What was said and done by whom.
- Detail of any witnesses to the incident.
- Any other information that is relevant to the incident i.e., how it made them feel.
- Possible resolutions.
- Reasons why they are considered vexatious/ unreasonably persistent

What happens when you report an incident

- All incidents will be logged via the IRMS will send an automatic notification through to the Security Director and Health and Safety Officer.
- They will make initial contact with the person reporting the issue to establish any immediate actions that are required to be taken.
- Following this there will be investigation into the incident and any required actions will be taken and logged on to the system.
- It is important that all incidents are logged, to ensure that patterns of incidents are noted and if required for any further police intervention that may be required,

Appendix C Reporting Incidents to Police

Whereby incidents occur and staff members wish to report a matter to the police with regard to perceived criminal offences. **Adhering to the following guidance will assist in provoking a more favourable response from police, assist an investigation and improve the likelihood of a positive outcome for staff members**-

- Produce a brief written record of the incident, evidencing the circumstances. These 'original notes' must include the time and date of the incident and also display the time and date that the 'original notes' were made (it is important to demonstrate that the 'original notes' were made as soon as practicable after the event, whilst the events were still fresh in the memory of the person making the notes). Any direct speech, including threats made must be recorded verbatim (word for word)
- Document the incident on the Incident Reporting Management System (IRMS) reporting system. Ensure that any witness details are also added to the entry so that the Health, Safety and Security Manager is aware of the existence of the witness details
- For instances of assault etc. the report to police must be made by the 'injured party' personally. Police will not accept a formal complaint from a third party

- Contact police by calling 101. **Alternatively for a quicker, more efficient method, by making contact *online* via the specific police online reporting system which enables criminal reports to be submitted by completing a live online form which is reviewed accordingly. This method enables staff to report incidents such as anti-social behaviour and criminal offences etc. within minutes. Simply Google the relevant force area (for example – Staffordshire Police Online Crime Reporting) to be redirected to the appropriate site/page.**

Follow the below points (1 - 3) when making a report to police to ensure that upon review the 'complaint' made is more likely to be progressed to an investigation stage:

1. Ensure that the call taker is aware that the call is being made to make an 'official complaint' regarding the incident that has occurred and that this includes the wish to pursue the matter through the criminal justice system. Ask for an appointment in order to give a 'witness statement' to police, either in person or by way of telephone appointment. Simply 'reporting' the matter to police will mean that police 'log' the incident, but may potentially take no further action
   Ensure your wishes as the 'victim' are clear to any officer reviewing the report and use clear phases- "I want to report this matter. I want to see an officer. I want to give a statement. I want this matter to be investigated"

2. Inform the call handler of the details of any witnesses to the incident to demonstrate that there is good evidence available from a number of persons present. This simple measure will mean that when the incident is reviewed by police, it will be clear that there is greater weight of evidence available due to the

number of witnesses. An officer reviewing an incident where there are no witness details listed may believe that the evidence is 50-50, one person's word against another. Whereas passing the names and contact information of 4 x colleagues, who were all present during an incident and who are willing to give statements, increases the evidence available (together with that of the victim) to 5 - 1

- Request a crime number
- Contact the Health, Safety and Security team for support and advice

When reporting a criminal offence, please note that generally the *victim* must be willing to make an official complaint. This cannot be made by the Trust or a third party.
Making an official complaint and wishing for the police to investigate means that the victim / witnesses must be willing to-

- Give a witness statement (obtained in writing by police)
- Support a police prosecution
- Possibly attend court as a witness and give their evidence orally in court

Immediate assistance from police

Whereby incidents occur and staff members require immediate assistance from police, make contact by way of 999 (101 for non-emergency matters) , the person who is calling the police is the site coordinator.

- Describe the nature of the incident, verbalise the identified **immediate risks** to persons or property regarding continuing offences or the commission if a serious offence (police will be responding to a number of live incidents and will need to assess the response required)
- Where necessary request urgent assistance to regain control of an area or prevent ongoing offences affecting the safety of others or serious damage to property
- **Explain whether this incident is occurring in a public place (*such as a reception area)* where there are members of the public, staff and vulnerable persons who are immediately at risk of harm due to the actions of the *offender***
- Explain the limitations of staff members to control the incident
- Explain that security staff are not present (and that their role would likely to be that of initiating police contact anyway)
- Ensure that police have the contact details of the site coordinator so they can continue to communicate and confirm attendance
- Ensure that staff are able to receive police onsite and direct them immediately to the required area

- If a negative response is received from police, the site coordinator should ask to speak to the Duty Inspector or Duty Officer (24 hour) and raise this with their Director and the Director of Corporate Services.