Security Policy

Complete the blank cells in the table below. The rest will be added by the corporate team once the policy approved and before it is added to the website.	
Policy ref no:	45
Responsible Executive Director:	Sarah Truelove, Deputy Chief Executive Officer and Chief Finance Officer
Author and Job Title:	Sarah Smith, Senior Local Counter Fraud Specialist
Date Approved:	ICB Board
Approved by:	1st May 2025
Date of next review:	1st May 2028

Policy Review Checklist

	Yes/No/NA	Supporting information
Has an Equality Impact Assessment Screening been completed?	Yes	See Appendix A
Has the review taken account of latest Guidance/Legislation?	Yes	Produced by LCFS
Has legal advice been sought?	N/A	
Has HR been consulted?	Yes	At CPRG
Have training issues been addressed?	Yes	See implementation plan – via the Hub
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by Staff Partnership Forum?	N/A	
Are there financial issues and have they been addressed?	N/A	
What engagement has there been with patients/members of the public in preparing this policy?	N/A	Not required
Are there linked policies and procedures?	Yes	See Associated Policies Section
Has the lead Executive Director approved the policy?	Yes	Shane Devlin
Which Committees have assured the policy?	Yes	Audit and Risk Committee at is meeting in April 2025
Has an implementation plan been provided?	Yes	
How will the policy be shared with staff		See implementation plan – via the Hub
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	
Has a DPIA been considered in regards to this policy?	Yes	Not required
Have Data Protection implications have been considered?	Yes	Through input at the Corporate Policy Review Group

Version	Date	Consultation

Table of contents

Security Policy..... 1

Policy Review Checklist 2

Table of contents..... 3

Security Policy..... 4

1 Introduction 4

1.1 BNSSG ICB Values 4

2 Purpose and scope.....4

3 Duties – legal framework for this policy 5

4 Responsibilities and Accountabilities 5

5 Security Procedure 7

6 Violence and Aggression 9

7 CCTV.....9

8 Emergency Preparedness, Resilience and Response.....9

9 Bomb Threats.....9

10 Reporting of Security Incidents 10

11 Assisting Police Investigations 10

12 Training Requirements 11

13 Equality Impact Assessment 11

14 Implementation and Monitoring Compliance and Effectiveness 11

15 Countering Fraud, Bribery and Corruption 12

16 References, acknowledgements and associated documents.....12

17 Appendices 12

Equality Impact Assessment – Appendix A.....12

Security Policy

1 Introduction

Bristol, North Somerset and South Gloucestershire Integrated Care Board (BNSSG ICB) is committed to promoting the security of its staff, and its assets. This policy has been produced by the Local Counter Fraud Specialist (LCFS) and is intended for use by all employees on all ICB security matters.

BNSSG ICB aims to provide a safe office working environment, where staff, clients and visitors can be confident of their personal safety and security of their possessions and where the ICB can be assured of the security of its buildings and assets. The ICB has a separate policy on Health and Safety which is supported through the provision included in this policy. The ICB operations are run from one site there is a dependency on landlords and other tenants for the provision of a secure working environment. Collaboration between relevant stakeholders will be required to maintain effective security together with, the adherence of staff to the guidance set out within this policy. Staff also work from domestic settings as dictated by the Hybrid Working Policy.

All ICB employees are responsible for ensuring that security procedures are adhered to at all times and will secure assets. Managers should take a leading role in promoting a pro-security culture to ensure the safety of all colleagues including covering key aspects as part of local induction.

BNSSG ICB does not tolerate violence and aggression towards staff the theft of (or criminal damage to) ICB assets or the criminal damage of ICB premises

Effective security management is linked to other policy areas, including fraud and bribery, bullying and harassment, counter terrorism and PREVENT, incident reporting, site security, conflict resolution, emergency preparedness, resilience and response (EPRR), personal safety and lone working.

1.1 BNSSG ICB Values

This policy supports the ICB values by ensuring that the ICB does the right thing, acts with integrity and assists the ICB in promoting a culture of support.

2 Purpose and scope

The ICB recognises its responsibility to provide a safe and secure working environment for all employees. This policy relates to all matters of security including the security of staff, property and assets. The overall aims of this policy are to:

- Improve the knowledge and understanding of all employees in BNSSG ICB, irrespective of their position, about security within the organisation.
- Assist in promoting a climate of openness and a pro-security culture where staff feel able to raise concerns sensibly and responsibly.
- Ensure the appropriate sanctions are considered following an investigation. Breach of this policy may lead to disciplinary action.

This policy applies to:

- All ICB employees (including temporary staff, students, apprentices, trainees, agency staff, seconded staff, self-employed consultants, sessional staff or those on short term or honorary contracts, self-employed consultants and individuals working for the ICB under a contract for services).
- Any work experience staff or volunteers.

3 Duties – legal framework for this policy

There is currently no NHS Security Standard and therefore no mandatory requirement for NHS organisations to employ a qualified LSMS however, the ICB retains an inherent obligation to protect and safeguard its staff and its assets, and does so by ensuring it puts in place and maintains suitable security arrangements and policies which address the risks associated with security, employee and public safety.

4 Responsibilities and Accountabilities

Security is the responsibility of all staff in not only safeguarding themselves and their property, but also property belonging to the ICB. The primary objectives of security management are:

- The prevention of violent or aggressive behaviour towards ICB staff, clients and visitors;
- The reporting of these incidents and compliance with any resulting investigation
- The protection of life from malicious criminal activity or other hazards.
- The protection of premises and assets against theft and damage.
- The detection and reporting of suspected offenders committing offences against clients, staff, property or private property within ICB premises.
- The education of all staff in security awareness.
- The smooth and uninterrupted delivery of health care and commissioning services.

The BNSSG ICB Board is responsible for gaining assurance that:

- Adequate arrangements are in place to ensure that all staff are aware of the standards of personal and professional behaviour expected of them; and that all staff have access to this policy.

The **BNSSG ICB Audit Governance and Risk Committee** is responsible for gaining assurance that:

- The BNSSG ICB has a robust policy and effective controls in place to adequately mitigate the risks of security related incidents.

The Chief Financial Officer is the lead for all Security Management work in BNSSG ICB, and monitors, ensures compliance with this policy and is responsible for:

- Ensuring the ICB has a suitably robust policy and effective controls in place to adequately mitigate the risks of security related incidents.
- Ensuring the ICB reports any such incidents to the relevant investigating authority and complies with any resulting investigation.
- Informing appropriate senior management, accordingly, depending on the outcome of investigations (whether on an interim and/or ongoing or concluding basis) and/or the potential significance of suspicions that have been raised.
- Ensuring the ICB gains assurance that providers awarded contracts with the ICB have suitable security arrangements in place.

Individual members of staff are required to:

- Actively co-operate with managers to achieve the aims and objectives of this policy, and to familiarise themselves with:
    - Any special security requirements relating to their work, team or place of work; and
    - The action to take in the event of a security incident.
- Safeguard themselves, colleagues, visitors and patients so far as is reasonably practicable against risks to their own security and ensure that equipment and property are not put in jeopardy by their actions or omissions, either by instruction, example or behaviour.
- Comply with all training requirements concerning security issues
- Ensure all visitors are wearing appropriate visitor badges and have signed in at reception when they collect them.
- Ensure that ICB ID is worn and visible whenever on ICB premises or on ICB business – except when doing so would place the individual at risk.
- Notify their line manager of any potential security problems and report all incidents involving criminal activity to the appropriate manager.
- Ensure all doors into the offices are secure at all times and not left open. Any issues with security doors should be reported to the Corporate Services Team Office Manager or site manager immediately so these can be resolved.
- Report any crime or breach of security.
- Maintain records which support security including calendars and contact details
- Safely taking steps to challenge individuals who are not recognised and are not wearing ID.

Managers at all levels have a responsibility to :

- Ensure that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively.
- Complete any risk assessments required in relation to the security of staff, premises or assets.
- Ensure that security issues known to them are reported accordingly.
- Ensure that every member of staff obtains a security ID badge and that the badge is worn and visible at all times whilst the staff member is on ICB premises or on ICB business.
- Ensure that members of their team are ensuring that all visitors have visitor badges and have signed in at reception when being collected.
- Ensure that all employees for whom they are accountable for, are made aware of the requirements of the policy as part of local induction and on an ongoing basis.
- Arranging retrieval of assets and ID badges at the end of employment.

5 Security Procedure

5.1 Staff Identification

- Every employee, including temporary employees will be issued with an identification badge on commencement of employment with the ICB, which must be worn and made visible at all times whilst on ICB premises or on official business.
- Each member of staff is personally responsible for their ID badge, security access fob(s), smart cards and their validity. Any radical changes in physical appearance, job title or department must result in the issue of a new ID badge triggered by the individual.
- ID badge, security access fob(s), smart cards and any equipment including laptops must be returned to the ICB when a member of staff leaves the employment of the ICB. It is the responsibility of the line manager to recover all items from the member of staff concerned and return items to Corporate Services.
- External visitors must be escorted while on site and wear a visitor badge at all times. The member of staff who is responsible for the visitor must notify the reception staff that they are expecting a visitor and arrange for the individual(s) to be met at reception. Visitor badges must be signed in upon issue and signed out upon return.
- Lost or missing ID badges, security access fob(s) or smart cards should be reported immediately via the ICB incident reporting system. Should a reported lost badge be subsequently found; the original must be returned to the ICB and the incident report updated.

5.2 Access and Egress

- Access to BNSSG ICB offices is restricted via the use of electronic ID badges (swipe cards).

- Electronic ID badges must not be swapped, loaned or given to unauthorised personnel at any time.
- Tailgating - All staff must challenge any unknown/unfamiliar person attempting to gain access. Especially if an ID badge or visitor permit is not visible.

Lock Down of 100 Temple Street Building

- A Lockdown protocol produced in conjunction with building tenants exists and is published on the Hub.

Security of Goods

- Goods received into the organisation must be checked against delivery notes prior to signing for acceptance. Arrangements will involve close working with the landlord.
- All ICB departments expecting good to be delivered goods must ensure that there are procedures in place to monitor the receipt of goods and safe/secure systems are in place to protect goods from theft or misappropriation.
-

Security of Personal Belongings

- All staff should ensure that personal belongings are stored in a secure location, for example in locked cupboards, desks or drawers. In the absence of negligence, the ICB cannot be held responsible for the theft of personal items and cannot accept responsibility for loss or damage to staff property.

Security of Motor Vehicles, bicycles and scooters

- The ICB cannot accept liability for any private motor vehicle or its contents when parked on a ICB occupied site or when the car is being used by an employee on ICB business.
- Managers should ensure that all staff have appropriate insurance to use their motor vehicles for business, which should be confirmed prior to authorising any mileage claims. Refer to Travel and Expenses policy and the pre-requisite submission of relevant documents on the EASY expenses system.
- The ICB cannot accept liability for any bicycle, scooter, or associated equipment when left on a ICB site or when it is used by an employee on ICB business

ICB Property and Assets

- Where appropriate, items should be placed on an asset register as dictated by the finance department. This is likely to be only for capital items. SCW maintain a register of assets for laptops.
- Managers should review ICB property held by their department on a regular basis to ensure that all items are securely managed and retrieved when no longer required.
- All managers and staff should take reasonable steps to safeguard ICB property whilst it is in their care. It is an offence for members of staff to remove property belonging to the ICB without prior authority from their line manager or the custodian

of the equipment. Failure to seek authority could result in disciplinary action and/or criminal proceedings being undertaken.

6 Violence and Aggression

The ICB has a duty to provide a safe and secure environment for all employees and visitors and will not tolerate violence and abusive behaviour nor any behaviour which conflict with the values of the organisation.

The ICB takes a very serious view of violence, abuse and aggression at work and realises its responsibility to protect employees and others who may be subjected to action of violence, abuse or aggression whether or not the act results in physical or non-physical assault.

Any member of the public, patients or otherwise who are violent towards ICB staff may have sanctions taken against them, be refused services, and/or taken to court by the ICB in line with national guidance.

7 CCTV

External CCTV is in place on premises occupied by the ICB. This is managed by the landlord who owns the building and the CCTV system. All requests for access to CCTV images must be made to the landlord.

8 Emergency Preparedness, Resilience and Response

A significant incident or emergency can be described as any event that cannot be managed within routine service arrangements. Each requires the implementation of special procedures and may involve one or more of the emergency services, the wider NHS or a local authority. In the event of a significant security threat, please refer to the Emergency Preparedness, Resilience & Response Plan and Business Continuity Plan for further information.

9 Bomb Threats

The vast majority of bomb threats are hoaxes. Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act 1977 and should always be reported to the police. Any member of staff receiving such a call should seek the immediate advice of the most senior manager available.

For immediate guidance on how to deal with bomb threats, go to the gov.uk website. This can be found at: https://www.gov.uk/government/publications/bomb-threats-guidance

A bomb threat checklist for action to be taken on receipt of a bomb threat is also available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/552301/Bomb_Threats_Form_5474.pdf

10 Reporting of Security Incidents

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

All security related incidents and near misses should be reported on Datix relevant line manager, if urgent but not criminal.

All incidents of crime should be reported initially to the relevant line manager and reported on Datix. In cases of violence and aggression or threat to staff and/or visitor safety, the police should be contacted immediately. The LCFS should be notified as soon as possible by telephone or email of any suspicions of fraud, bribery or corruption, and security incident.

Examples of reportable incidents and the processes to follow are below:

Assault or abuse of a staff member or visitor:

All incidents of this type must be reported through the ICB incident reporting system as soon as possible. All physical assaults towards staff should be reported by the appropriate manager through the incident reporting system.

Visitors and staff should always be asked if they wish for the police to be involved.

Security incident/crime is in progress:

Staff safety is paramount, and therefore staff should go to a place of safety. The incident should be reported to the police immediately, and then to the senior manager on site. An incident must be logged into the incident reporting system as soon as possible.

Criminal incident discovered after the offence has occurred:

These incidents which may include theft of loss of assets/property should be reported as soon as the crime is discovered, as per the incident reporting process. The manager should then inform the police.

Data Breaches – including Theft of identifiable information:

This must be reported immediately to the Data Protection Officer and the IG manager and recorded on Datix.

11 Assisting Police Investigations

Occasionally, the Police may contact the ICB for information relating to an ongoing investigation. Any individual who is contacted in such a manner should refer the police to the LCFS or Chief Finance Officer as the initial point of contact.

Staff should obtain guidance from Information Governance should they be asked to disclose confidential information to the police.

PREVENT

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

- Ensuring that if there are concerns around rooms or buildings being used for radicalisation or terrorism, that these are reported immediately to an appropriate individual within the ICB.
- Ensuring staff have received PREVENT training as per the PREVENT policy, and that as a result of this training, staff report issues to relevant managers for escalation.
- Ensuring that there is an identified PREVENT lead.

The ICB has a separate PREVENT policy.

12 Training Requirements

All staff should be made aware of the policy, their responsibility to adhere to the guidance given and to report security incidents and crime in the NHS..

For those with additional responsibilities e.g. fire safety, PREVENT, relevant role appropriate training will be provided by the ICB.

13 Equality Impact Assessment

An Equality Impact Assessment has not been carried out in relation to this policy, as the Equality Impact Screening anticipated no barriers to accessing the policy and a fair approach to Security Management once implemented. This screening can be found at Appendix A.

14 Implementation and Monitoring Compliance and Effectiveness

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
ICB Board	Ensure ICB Board is aware of the ICB's responsibilities Security Management.	Policy and Cover paper to be presented by the ICB Board after approval by Audit, Governance and Risk Committee.	LCFS /RH	Upon approval at AGRC	April 25	LCFS time AGRC time
Staff	Awareness of policy	Information included in the Voice	RH	May 25	June 25	Comms support
Staff	Access to policy	Available on the Hub	RH	May 25	Jun 25	Comms support

15 Countering Fraud, Bribery and Corruption

The ICB is committed to reducing and preventing fraud, bribery and corruption in the NHS and ensuring that funds stolen by these means are put back into patient care. During the development of this policy document, we have given consideration to how fraud, bribery or corruption may occur in this area. We have ensured that our processes will assist in preventing, detecting and deterring fraud, bribery and corruption and considered what our responses to allegation of incidents of any such acts would be.

In the event that fraud, bribery or corruption is reasonably suspected, and in accordance with the Local Counter Fraud, Bribery and Corruption Policy, the relevant Team will refer the matter to the ICB's Local Counter Fraud Specialist for investigation and reserve the right to prosecute where fraud, bribery or corruption is suspected to have taken place. In cases involving any type of loss (financial or other), the ICB will take action to recover those losses by working with law enforcement agencies and investigators in both criminal and/or civil courts.

16 References, acknowledgements and associated documents

The following list is not exhaustive:

- Safeguarding Policy
- Health and Safety Policy
- Business Continuity Plan
- Incident Reporting
- Bullying and Harassment Policy
- Disciplinary Policy
- PREVENT Policy
- EPRR Plan
- SCW policies reviewed by the ICB Information Governance Group.
- Acceptable Use of IT Policy

17 Appendices

Equality Impact Assessment – Appendix A