NHS
Cornwall and
Isles of Scilly

Security policy

Date approved: 28 February 2023

NHS Cornwall and Isles of Scilly Integrated Care Board

Call us on 01726 627 800
Email us at ciosicb.contactus@nhs.net
Visit our website: cios.icb.nhs.uk

Part 2S, Chy Trevail,
Beacon Technology Park,
Dunmere Road,
Bodmin, PL31 2FR
Chair: John Govett
Chief executive officer: Kate Shields

Document control

Title of document: Security policy
Lead directorate: Local security management (via corporate governance)
Lead team: Local security management (via corporate governance)
Document type: Policy
Subject category: Health and safety
Author(s) name: Jess James, head of corporate governance and Carver Tedstone, local security management specialist (LSMS)
Date ratified: 28 February 2023
Ratified by: Director for strategy, planning and corporate affairs
Review frequency: 3 years (standard, unless otherwise indicated)
To be reviewed by date: 28 February 2026
Target audience: All staff
Can this policy be released under FOI? Yes
Give reasons for exemption if no: N/A

Version control

Version number	Revision date	Revision by	Nature of revisions
V1.0	March 2019	J. James	Initial draft.
V1.1	May 2019	T. Corsellis and M. Jackson	Clarifications and review by LSMS
V2	20 May 2019	J. James	Ratification information updated and amendment of words ‘staff or patients’ to read ‘people.’
V2.1	July 2022	ICB	Adopted by NHS Cornwall and Isles of Scilly ICB
V1.0	October 2022	C. Tedstone	Amendments to reflect transition to ICB. Review by LSMS
V1.1	October 2022	Corporate governance office and head of corporate governance	Review and rebranding – minimal changes
V.2	February 2023	Carolyn Andrews, director for strategy, planning and corporate affairs	Updated policy ratified by relevant executive director

You can request any document published on our website in alternative formats. Email our engagement team for more information.

Contents

1. Introduction 4
2. Purpose 4
3. Responsibilities 5
   Local security management specialist (LSMS) 7
4. Security procedures 7
   4.1 Staff Identification 7
   4.2 Visitors and contractors 8
   4.3 Access and egress 8
   4.4 Security of goods 8
   4.5 Security of personal belongings 8
   4.6 Security of motor vehicles 8
   4.7 Property and Assets 9
   4.8 Lone Working 9
5. Violence and aggression 9
6. CCTV 9
7. Emergency preparedness, resilience and response 10
8. Bomb threats 10
9. Reporting of security incidents 10
10. Assisting the police or other law enforcement agencies 11
11. Fire 11
12. PREVENT 11
13. Counter fraud 11
14. Monitoring compliance and effectiveness 12
15. Training 12
16. Associated policies 12

Appendix 1: Equality impact assessment 13
   Aims, objectives and purpose of the policy 13
   Differential impacts 13
   Human rights values 14
   Public Sector Social Value Act 2012 15
   Equality impact assessment action plan 16

1. Introduction

NHS Cornwall and the Isles of Scilly Integrated Care Board (ICB) is committed to promoting the security of its staff, its assets and the people who use the services it commissions. This policy has been produced by the local security management specialist (LSMS), with the support of the corporate governance team, and is intended as a guide for all employees on all ICB security matters.

The ICB aims to provide a safe working environment, where people 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.

All ICB employees are responsible for ensuring that security procedures are always adhered to. Managers should take a leading role in promoting a pro-security culture to ensure the safety of all colleagues.

The LSMS is an expert in all matters regarding security and can be contacted via the corporate governance team should a potential security concern arise. In the case of an immediate emergency, the ICB's nominated LSMS can be contacted directly on 07876 547691 c.tedstone@nhs.net or carver.tedstone@tiaa.co.uk

The ICB does not tolerate violence and aggression towards people, the theft of (or criminal damage to) ICB assets or criminal damage to ICB buildings. To reduce the likelihood of these acts being carried out, the ICB has adopted the following operational framework.

Strategic governance - not tolerating violence and aggression towards people or theft and/or damage caused to ICB assets; making this clear to all staff; and monitoring, the effectiveness of the arrangements in place. The ICB has appointed a qualified LSMS to support this commitment.

Inform and involve - through setting clear policies and a code of conduct for all staff; raising awareness of the risks; and liaising with other organisations to develop a shared resistance to violence and aggression, theft and criminal damage.

Prevent and deter - through focused assessment of risks in existing processes and the creation of recommendations to improve identified system weaknesses.

Hold to account - through the investigation of security-related incidents, should such situations arise, and through the application of appropriate sanctions.

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

2. Purpose

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 ICB employees 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

This policy applies to all ICB employees, regardless of position held, as well as consultants, vendors, contractors, and/or any other parties who have a business relationship with the ICB.

3. Responsibilities

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 and deterrence of violent or aggressive behaviour towards ICB staff, visitors, or the people who use the services we commission.
- the reporting of these incidents and their 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 people, assets and property within ICB premises.
- ensuring sanctions and redress are in place for offenders, to prevent recurrence and to protect our staff, assets and property.
- the education of all staff in security awareness.
- the smooth and uninterrupted delivery of health care and commissioning services.

The board of the ICB has delegated to the workforce committee its responsibility 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 health and safety sub- committee is responsible for gaining assurance that:

- the ICB has appointed a qualified LSMS to lead the drive to maintain and improve the standards and processes for deterring, detecting and investigating wrongdoings and seek prosecution where wrongdoing is discovered
- the annual security management workplan is adequate and provides a reasonable balance between raising security awareness across the organisation and evaluating the effectiveness of the ICB's security systems and controls

The sub-committee will also receive annual reports from the LSMS on the progress against the security management workplan and updates of the progress of any investigations.

The workforce committee will receive regular reports from the health and safety sub-committee as well as be responsible for receiving and responding to or approving recommendations from any investigations or matters escalated.

The deputy director of corporate governance is the lead for all security management work in the ICB and is responsible for:

- managing the continuity of appointment of a qualified LSMS for the ICB.
- overseeing the delivery of services from the LSMS.
- providing the relevant required support to the LSMS in any investigations or pro-active work that they carry out.
- informing appropriate senior management accordingly, depending on the outcome of investigations (whether on an interim and/or on-going 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 management arrangements (for example, a workplan and annual report) as per service condition 24 of the NHS England standard commissioning contract, as reviewed and reported by the LSMS in liaison with the contracts team.

The head of corporate governance supports the deputy director in this role providing operational support to the LSMS on a regular basis.

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 place of work; and
    - the action to take in the event of a security incident
- safeguard themselves, colleagues, visitors and other people so far as is reasonably practicable 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 ICB ID is worn and visible whenever on ICB premises or on ICB business
- notify their line manager of any potential security problems and report all incidents involving criminal activity to the appropriate manager
- report any crime or breach of security

Managers at all levels have a responsibility to:

- ensure 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 security issues known to them are reported accordingly.
- ensure their staff are aware of how to report an incident, and that this process is easy to access.
- ensuring every member of staff obtains a security ID badge and that the badge is always worn and visible whilst the staff members is on ICB premises or on ICB business.
- ensure all employees for whom they are accountable for, are made aware of the requirements of the policy.

Local security management specialist (LSMS)

The ICB's nominated LSMS is provided by TIAA. The overall objective of the LSMS will be to work on behalf of the ICB to provide a safe and secure working environment with a pro-security culture. The LSMS will:

- report to the deputy director of corporate governance on security management work locally
- lead on day-to-day work within the ICB to tackle violence against staff and professionals in accordance with national guidance
- ensure that lessons are learned from security incidents, and that actions to mitigate the risks arising from incidents are carried out promptly
- carry out risk-based site security reviews. If a serious security incident occurs, or at the request of the committee, the LSMS will carry out additional reviews
- investigate security incidents, as directed by the director of transformation and partnerships, in a fair, objective and professional manner so appropriate sanctions and preventative action can be taken
- ensure that the security management policy addresses all relevant, identified risks within the ICB and contains useful guidance
- assist managers with completion of risk assessments
- produce an annual security management workplan aligned to the resource made available

4. Security procedures

4.1 Staff Identification

Every employee, including employees on short and/or fixed term contracts will be issued with an ID badge on commencement of employment with the ICB, which must always be worn and made visible whilst on ICB premises or on official business.

Each member of staff is personally responsible for their badge and its validity. Any radical changes in physical appearance, job title or department must result in the issue of a new ID badge.

ID badges must be returned to the employee's line manager when a member of staff leaves the employment of the ICB. It is the responsibility of the line manager to recover the ID badge from the member of staff concerned.

Lost or missing ID badges should be reported immediately via ciosicb.incidents@nhs.net. Should a reported lost badge be subsequently found; the original must be returned to the ICB, and the incident report updated.

4.2 Visitors and contractors

External visitors and contractors should be escorted while on site. Regular visitors, who are known to staff and familiar with the site may not require escort. The member of staff who is responsible for the visitor and/or contractor should notify the reception staff that they are expecting a visitor and, where not a regular visitor, arrange for the individual(s) to be met at reception. Visitor badges must be signed in upon issue and signed out upon return.

4.3 Access and egress

Access to ICB offices is restricted via the use of electronic ID badges and/or coded keypads.

Electronic ID badges must not be swapped, loaned or given to unauthorised personnel at any time.

To avoid incidents of tailgating all staff must challenge any unknown and/or unfamiliar person attempting to gain access, in particular if an ID badge or visitor permit is not visible.

4.4 Security of goods

Goods received into the organisation must be checked against delivery notes prior to signing for acceptance.

All ICB departments receiving goods must ensure that there are procedures in place to monitor the receipt of goods and safe and secure systems are in place to protect goods from theft or misappropriation.

Staff should receive relevant training in the handling of post to recognise suspicious packages and deal with these safely.

4.5 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.

4.6 Security of motor vehicles

In the absence of negligence, the ICB cannot accept liability for any private motor vehicle or its contents when parked on an ICB occupied site or when the car is being used by an employee on ICB business.

4.7 Property and Assets

Managers should review ICB property held by their department on a regular basis to ensure that all items are securely managed. Changes in allocation or status of assets, such as laptops and mobile phones, should be reported to the ICB information management and technology team.

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 or fail to return 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.

4.8 Lone Working

Working alone can bring additional risks to an activity. The ICB has developed policies and procedures to control the risks and protect employees and staff should refer to the ICB agile working policy.

The 3 most important aspects of lone working are that:

1. the lone worker has full knowledge of the hazards and risks to which they are exposed
2. the lone worker knows what to do if something goes wrong
3. someone else knows the whereabouts of the lone worker, the type of work they are doing and the expected time of completion

5. 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.

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.

The ICB may take sanctions against any member of the public, person who uses the services we commission or otherwise who are violent towards ICB staff. They may also be refused treatment and/or taken to court by the ICB in line with national guidance.

Staff should report any incidence of violence and aggression to their line manager and via ciosicb.incidents@nhs.net and refer to the acceptable behaviour policy.

6. CCTV

External CCTV is in place on premises used by the ICB. This is managed by the landlord who owns the building and CCTV system. Requests for access to CCTV

images are deemed to be a subject access request and as such should be made via the information governance team (ciosicb.caldicottincidents@nhs.net). who will then approach NHS Property Services. For any request other than subject access, the requestor must state a lawful basis which would allow the processing of CCTV images. The information governance team and/or LSMS will determine whether the CCTV images can be disclosed. This would also include requests made by police officers or other law enforcement agencies.

This policy takes into account the following legislation relevant to CCTV:

- Data Protection Act 2018
- Surveillance Camera Code of Practice
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

7. 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 required the implementation of special procedures and may involve one or more of the emergency services, the wider NHS or a local authority. Please refer to the incident response plan and business continuity plan.

8. Bomb threats

Most 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 Bomb threats | ProtectUK.

A bomb threat checklist for action to be taken on receipt of a bomb threat is also available Bomb threat checklist | ProtectUK.

9. Reporting of security incidents

All employees have a responsibility to report all crimes and breaches of security and should refer to the incident reporting and management policy.

Any crimes in progress should be reported to the police immediately and subsequently reported via ciosicb.incidents@nhs.net. The corporate governance team will report these and any other reported crimes, security related incidents or near misses to the LSMS as soon as possible.

If a security incident involves the assault or abuse of a staff member of visitor, this should be reported via ciosicb.incidents@nhs.net as soon as possible. Managers must offer any staff assaulted support via a meeting to identify any needs, such as

counselling. Visitors should be signposted to an organisation such as victim support (Home - Victim Support, freephone 0808 16 89 111).

If the security incident involves the theft of person identifiable or corporate confidential information (for example, theft of records, data storage, laptop) this should be reported immediately to the data protection officer or head of information governance and an information governance breach proforma completed. Please refer to the data protection policy or contact the information governance team for further information.

Other security incidents to be reported might include large crowds demonstrating outside ICB property; unauthorised access to staff areas; and suspicious packages.

10. Assisting the police or other law enforcement agencies

Occasionally, the police or other law enforcement agencies 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 LSMS or deputy director of corporate governance as the initial point of contact.

Staff should obtain guidance from the information governance team if they are asked to disclose confidential information to the police.

11. Fire

The overlapping interests of security and fire safety policies are fully recognised. There is full co-operation between fire and security staff.

12. PREVENT

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

- if there are concerns around rooms or buildings being used for radicalisation or terrorism, that these are reported immediately to the safeguarding adults team, who take the lead on PREVENT
- relevant staff have received PREVENT training as per the PREVENT policy, and that because of this training, staff report issues to relevant managers for escalation
- there is an identified PREVENT lead. Within the ICB the safeguarding adults team take the lead on PREVENT

Please refer to the ICB PREVENT policy for more details.

13. Counter fraud

The overlapping interests of security management and counter fraud are fully recognised. The LSMS will liaise closely with the local counter fraud specialist

(LCFS) to ensure incidents which could be constituted as theft or fraud are appropriately investigated.

14. Monitoring compliance and effectiveness

The deputy director of corporate governance and the LSMS will agree annual and specific measures of the effectiveness of this policy.

As a minimum, the LSMS will report annually on the number and nature of instances of security incidents. This report will include details of outcomes and consequences to the individuals involved.

The LSMS will, through the annual programme of work, determine the effectiveness of the ICB's controls and other efforts to prevent and deter security breaches.

The LSMS annual report to the health and safety sub-committee will include the results of these risk assessments. The health and safety sub-committee will monitor the delivery of actions agreed to address any weaknesses and lapses identified in the implementation of the policy.

15. Training

All staff should be made aware of the policy and their responsibility to report security incidents and crime in the NHS through a mixture of targeted security awareness items in staff bulletins and the staff intranet.

16. Associated policies

Adult safeguarding policy
Agile working policy
Acceptable behaviour policy
Business continuity plan - to request a copy contact ciosicb.corporategovernance@nhs.net
Child protection policy and procedure
Data protection policy
Grievance and dignity at work policy
Disciplinary policy and procedure
Health and safety policy
Incident management policy
Incident response plan - to request a copy contact ciosicb.corporategovernance@nhs.net
Prevent policy
Subject access request policy
Violence prevention reduction standard policy (this policy is under development)

Appendix 1: Equality impact assessment

Name of policy or service to be assessed: Security policy
Department or section: Corporate governance
Date of assessment: October 2022
Person(s) responsible for the assessment: Head of corporate governance
Is this a new or existing policy? Existing

Aims, objectives and purpose of the policy

Describe the aims, objectives, and purpose of the policy.
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 ICB employees 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.

Who is intended to benefit from this policy, and in what way?
Staff, visitors, members of public, people who use the services we commission, through increased safety and security, protection from harm, loss, theft etc. Increased well-being of staff through working in a safe environment.

What outcomes are wanted from this policy?
Improved awareness of structures and process in place for security management in the ICB.

What factors or forces could contribute or detract from the outcomes?
Lack of staff awareness of policy and processes involved.
Colleagues unfamiliar with systems (this will be mitigated through regular reminders through weekly bulletin)

Who are the main stakeholders in relation to the policy?
This policy applies to all employees of the ICB, regardless of position held, as well as consultants, vendors, contractors, and/or any other parties who have a business relationship with the ICB.

Who implements the policy, and who is responsible for the policy?
Corporate governance team and LSMS.

Differential impacts

Does this have a positive or negative impact on people from an ethnic minority background? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?

No differential impact is anticipated on these groups.

What is the positive or negative differential impact on people from the perspective of disability? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies. How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary, or gender fluid? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

Does this have a positive or negative impact on people who are pregnant, breast-feeding mothers, or those on maternity leave? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

Are they any other identified groups? How will any negative impact be mitigated?
No differential impact is anticipated on these groups.

Human rights values

How have the core human rights values of fairness, respect, equality, dignity, and autonomy been considered in the formulation of this policy, service, or strategy?
The policy has been written to ensure that people are treated with dignity and respect by protecting them from harm and loss.

Which of the human rights articles does this document impact?

☒ To life
☒ Not to be tortured or treated in an inhuman or degrading way

☒ To liberty and security
☐ To a fair trial
☐ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience, and religion
☐ To freedom of expression
☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☒ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?
Policy covers processes around personal safety and security and that of possessions.

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?
The Human Rights Statement and Guidance accompanies the Equality Impact Assessment guidance and Comprehensive Impact Assessment guidance, to provide comprehensive information for staff. These policies are available for staff on the ICB website and have been proactively disseminated via the staff bulletin.

Public Sector Social Value Act 2012

NHS Cornwall and Isles of Scilly is committed and obliged to fulfil the requirements of the Public Sector Social Value Act 2012. This Act requires the organisations to consider how services commissioned or procured might improve the economic, social, and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system, and community.
Not applicable.

Describe how the policy contributes towards eliminating discrimination, harassment, and victimisation.
Policy cross references with the acceptable behaviour policy and the incident management policy both of which contribute towards eliminating discrimination, harassment and victimisation.

Describe how the policy contributes towards advancing equality of opportunity.
Policy contributes to equality of opportunity by seeking to provide a safe, secure working environment for all our staff.

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
Policy contributes to promoting good relations by seeking to provide a safe, secure working environment, and cross references the acceptable behaviour policy and the

incident management policy both of which contribute towards eliminating discrimination, harassment and victimisation.

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and or the working environment for that group of people.
No differential impacts identified.

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
None

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.
Not applicable.

Equality impact assessment action plan

Issue to be addressed	Action required	Responsible person	Timescale for completion	Action taken
N/A	N/A	N/A	N/A	N/A

Comments on action plan:
N/A

Signed (completing officer): Jess James

Date: October 2022

Signed (head of department or section): Trudy Corsellis

Date: October 2022

Please ensure that a signed copy of this form with the policy is sent to both the corporate governance team and equality and diversity lead.