NHS
Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

70 YEARS OF THE NHS 1948 - 2018

Security Policy

Shaping better health

Policy ref no:	45
Responsible Executive Director:	Sarah Truelove, CFO
Author and Job Title:	Elias Hayes, Local Security Management Specialist
Date Approved:	October 2019
Approved by:	Governing Body
Date of next review:	October 2022

	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	
Has legal advice been sought?	N/A	
Has HR been consulted?	Yes	Chance to review at CPRG
Have training issues been addressed?	Yes	Please see implementation plan at Appendix B
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by JCC?	No	
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?		
Which Committees have assured the policy?		
Has an implementation plan been provided?	Yes	The Chief Financial Officer (CFO) and the LSMS will agree annual and specific measures of the effectiveness of this policy
How will the policy be shared with: • Staff? • Patients? • Public?	Intranet Internet	
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	The policy will be launched to staff at Stand Up and then shared through the Voice and be available on the Hub

Contents

Security Policy

Preface

Bristol, North Somerset and South Gloucestershire Clinical Commissioning Group (BNSSG CCG) is committed to promoting the security of its staff, its assets and its patients. This policy has been produced by the Local Security Management Specialist (LSMS) and is intended for use by all employees on all CCG security matters. The CCG's nominated LSMS can be contacted on 01173 420 828.

1. Introduction

1.1. BNSSG CCG aims to provide a safe working environment, where staff, visitors and patients can be confident of their personal safety and security of their possessions and where the CCG can be assured of the security of its buildings and assets. The CCG has a separate policy on Health and Safety which is supported through the provision included in this policy. The CCG operations are run from multiple sites and 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.

1.2. All CCG employees are responsible for ensuring that security procedures are adhered to at all times. CCG Managers should take a leading role in promoting a pro-security culture, to ensure the safety of all CCG staff.

1.3. The LSMS is an expert in all matters regarding security, and should be contacted regarding any potential security concern.

1.4. BNSSG CCG does not tolerate violence towards staff or patients, the theft of CCG assets or the damage of premises. In order to reduce the likelihood of these acts being carried out, the CCG has adopted the following operational framework:

- Strategic Governance - not tolerating violence and aggression towards patients/staff or theft/damage caused to CCG assets; making this clear to all staff; and monitoring the effectiveness of the arrangements in place. BNSSG CCG will appoint a qualified Local Security Management Specialist (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.

1.5. Effective security management is linked to other policy areas, including fraud and bribery, bullying and harassment. EPRR and lone working.

1.6. This policy supports the CCG's values

2. Purpose and scope

2.1. The CCG 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:

2.1.1. Improve the knowledge and understanding of all employees in BNSSG CCG, irrespective of their position, about security within the organisation.

2.1.2. Assist in promoting a climate of openness and a pro-security culture where staff feel able to raise concerns sensibly and responsibly.

2.1.3. Ensure the appropriate sanctions are considered following an investigation. Breach of this policy may lead to disciplinary action.

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

3. Duties and responsibilities

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

3.1.1. The prevention of violent or aggressive behaviour towards CCG staff, patients, clients and visitors;

3.1.2. The protection of life from malicious criminal activity or other hazards;

3.1.3. The protection of premises and assets against theft and damage;

3.1.4. The detection and reporting of suspected offenders committing offences against patients, clients, staff, property or private property within CCG premises;

3.1.5. The education of all staff in security awareness;

3.1.6. The smooth and uninterrupted delivery of health care and commissioning services.

3.2. **The BNSSG CCG Governing Body** is responsible for gaining assurance that:

3.2.1. 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.

3.3. The **BNSSG CCG Audit Governance and Risk Committee** is responsible for gaining assurance that:

3.3.1. The BNSSG CCG has appointed a qualified Local Security Management Specialist (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.

3.3.2. The annual Security Management Workplan is adequate and provides a reasonable balance between raising security awareness across BNSSG CCG and evaluating the effectiveness of the BNSSG CCG's security systems and controls.

3.3.3. It receives annual reports from the LSMS on the progress against the Security Management Workplan and updates of the progress of any investigations.

3.3.4. Providers awarded CCG contracts have suitable security management arrangements as reviewed and reported by the LSMS.

3.4. **The Chief Financial Officer** is the lead for all Security Management work in BNSSG CCG, and monitors and ensures compliance with SC24 of the NHS England standard commissioning contract and is responsible for:

3.4.1. Managing the continuity of appointment of a qualified LSMS to the BNSSG CCG; and ensuring that the counter-fraud service

continues to be delivered in the event of the departure, or long term absence of the appointed LSMS.

3.4.2. Overseeing the delivery of services from the LSMS.

3.4.3. Providing the relevant required support to the LSMS in any investigations or pro-active work that they carry out.

3.4.4. Depending on the outcome of investigations (whether on an interim/on-going or concluding basis) and/or the potential significance of suspicions that have been raised, inform appropriate senior management accordingly.

3.5. **Individual members of staff** are required to:

3.5.1. Actively co-operate with managers to achieve the aims and objectives of this policy, and to familiarise themselves with:

3.5.1.1. Any special security requirements relating to their work, team or place of work; and

3.5.1.2. The action to take in the event of a security incident.

3.5.2. 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.

3.5.3. Ensure all visitors are wearing appropriate visitor badges and have signed in at reception when they collect them.

3.5.4. Comply with all training requirements concerning security issues.

3.5.5. Ensure that CCG ID is worn and visible whenever on CCG premises or on CCG business – except when doing so would place the individual at risk.

3.5.6. Notify their line manager of any potential security problems and report all incidents involving criminal activity to the appropriate manager.

3.5.7. 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.

3.5.8. Report any crime or breach of security.

3.5.9. Maintaining records which support security including calendars and contact details

3.6. **Managers at all levels** have a responsibility to :

3.6.1. Ensure that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively.

3.6.2. Complete any risk assessments required in relation to the security of staff, premises or assets.

3.7.1. Ensure that security issues known to them are reported accordingly.

3.7.2. Ensuring 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 CCG premises or on CCG business.

3.7.3. Ensure that members of their team are ensuring that all visitors have visitor badges and have signed in at reception when being collected.

3.7.4. Ensure that all employees for whom they are accountable for, are made aware of the requirements of the policy as part of induction and on an ongoing basis.

3.8. **Local Security Management Specialist (LSMS)**

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

3.8.1.1. Report to the Chief Finance Officer on security management work locally.

3.8.1.2. Lead on day to day work within the CCG to tackle violence against staff and professionals in accordance with national guidance.

3.8.1.3. Ensure that lessons are learned from security incidents, and that actions to mitigate the risks arising from incidents are carried out promptly.

3.8.1.4. Investigate security incidents, as directed by the CFO, in a fair, objective and professional manner so that appropriate sanctions and preventative action can be taken.

3.8.1.5. Ensure that the Security Management policy addresses all identified risks within the CCG and contains useful guidance.

3.8.1.6. Assist managers with completion of risk assessments.

3.8.1.7. Produce an annual Security Management Workplan aligned to the resource made available.

4. Security Procedure

4.1. Staff Identification

4.1.1. Every employee, including temporary employees will be issued with an identification badge on commencement of employment with the CCG, which must be worn and made visible at all times whilst on CCG premises or on official business.

4.1.2. 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.

4.1.3. ID badge, security access fob(s), smart cards and any equipment including laptops must be returned to the CCG when a member of staff leaves the employment of the CCG. It is the responsibility of the line manager to recover all items from the member of staff concerned and return items to Corporate Services

4.1.4. 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.

4.1.5. Lost or missing ID badges, security access fob(s) or smart cards should be reported immediately via the CCG incident reporting system. Should a reported lost badge be subsequently found; the original must be returned to the CCG and the incident report updated.

4.2. Access and Egress

4.2.1. Access to BNSSG CCG offices is restricted via the use of electronic ID badges.

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

4.2.3. Tailgating - All staff must challenge any unknown/unfamiliar person attempting to gain access. Especially if an ID badge or visitor permit is not visible.

4.3. Lock Down of Building

4.3.1. In the event of a serious incident outside of the building which poses a security threat to CCG staff or assets, the procedure for lockdown will be activated. This will restrict access to the CCG areas as well as to other areas of the building.

4.3.2. No staff should leave buildings during a security lock down until they have been given the all clear to do so and that it is safe.

4.4. Security of Goods

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

4.4.2. All CCG departments receiving 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.

4.5. Security of Personal Belongings

4.5.1. All staff should ensure that personal belongings are stored in a secure location, for example in locked cupboards, desks or drawers. The CCG 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 and bicycles

4.6.1. The CCG cannot accept liability for any private motor vehicle or its contents when parked on a CCG site or when the car is being used by an employee on CCG business. Managers should also ensure that all staff have appropriate insurance to use their motor vehicles for business, which should be confirmed prior to authorising any mileage claims.

4.6.2. The CCG cannot accept liability for any bicycle or associated equipment when left on a CCG site or when it is used by an employee on CCG business

4.7. CCG Property and Assets

4.7.1. Where appropriate, items should be placed on an asset register. Managers should review CCG property held by their department on a regular basis to ensure that all items are securely managed.

4.7.2. All managers and staff should take reasonable steps to safeguard CCG property whilst it is in their care. It is an offence for members of staff to remove property belonging to the CCG 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

4.8.1. When agreed working arrangements result in an employee working alone, their manager will be responsible for following the lone working guidelines. Ensuring that a risk assessment has been undertaken, and that a related safe system of work is put in place. The employee will be required to conform to these arrangements to safeguard both themselves and the CCG.

4.8.2. Working alone can bring additional risks to an activity. The CCG has developed policies and procedures to control the risks and protect employees. Employees should follow these procedures.

4.8.3. The four most important aspects of lone working are that:

4.8.3.1. The lone worker has full knowledge of the hazards and risks to which they are exposed.

4.8.3.2. The lone worker knows what to do if something goes wrong.

4.8.3.3. Someone else knows the whereabouts of the lone worker, what they are doing and the duration of the work.

4.8.3.4. Managers or their nominated deputy are aware that an employee who is lone working has returned home safely if they have been off site working alone.

5. Violence and Aggression

5.1. The CCG has a duty to provide a safe and secure environment for all employees and visitors and will not tolerate violence and abusive behaviour which conflict with the values of the organisation.

5.2. The CCG 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.

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

6. CCTV

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

7. Emergency Preparedness, Resilience and Response

6.1. 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. Please refer to the Emergency Preparedness, Resilience & Response Plan and Business Continuity Plan for further information.

8. Bomb Threats

8.1. 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.

8.2. 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

8.3. 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

9. Reporting of Security Incidents

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

9.2. All security related incidents and near misses should be reported on Datix and to the LSMS, if urgent but not criminal.

9.3. All incidents of crime should be reported initially to the LSMS and reported on Datix. The LSMS should be notified as soon as possible by telephone or email.

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

9.4.1. **Assault or abuse of a staff member or visitor:** All incidents of this type must be reported through the CCG 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, patients and staff should always be asked if they wish for the police to be involved.

9.4.2. **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.

9.4.3. **Criminal incident discovered after the offence has occurred:** These incidents should be reported as soon as the crime is discovered, as per the incident reporting process. The manager should then inform the police.

9.4.4. **Theft of patient identifiable information:** This must be reported immediately to the Caldicott Guardian, SIRO and Deputy Chief Executive and Associate Director of Corporate Operations. Any potential theft or loss of data storage e.g. computer, laptop, etc. should be reported in this way.

10. Assisting Police Investigations

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

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

11. Fire

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

12. PREVENT

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

12.1.1. 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 CCG.

12.1.2. 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.

12.1.3. Ensuring that there is an identified PREVENT lead.

13. Counter Fraud

13.1. 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

14.1. The Deputy Chief Executive / Chief Financial Officer and the LSMS will agree annual and specific measures of the effectiveness of this policy.

14.2. 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.

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

14.4. The results of these risk assessments will be reported in the LSMS annual report to the Audit, Governance and Risk Committee. Delivery of actions agreed to address weaknesses and lapses identified in the implementation of the policy will be monitored by the Audit, Governance and Risk Committee.

15. Associated Documents

The following list is not exhaustive:

15.1. Lone Working Guidelines
15.2. Safeguarding Children and Adults Policy
15.3. Health and Safety Policy
15.4. Business Continuity Policy
15.5. Incident Reporting
15.6. Bullying and Harassment Policy
15.7. Disciplinary Policy
15.8. EPRR Plan

16. Training requirements

16.1. 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 Presentations and general security presentations conducted by the LSMS at CCG Corporate Induction.

17. Equality Impact Assessment

17.1. 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.

18. Appendices

18.1. Equality Impact Screening

18.2. Implementation plan

Appendix A – Equality Impact Screening

<table>
<tr><th colspan="4">Equality Impact Screening</th></tr>
<tr><td>Query</td><td colspan="3">Response</td></tr>
<tr><td>What is the aim of the document?</td><td colspan="3">To facilitate issues of concern being heard quickly and fairly.</td></tr>
<tr><td>Who is the target audience of the document (which staff groups)?</td><td colspan="3">All staff and other groups as identified in section 3 of policy.</td></tr>
<tr><td rowspan="6">Who is it likely to impact on and how?</td><td>Staff</td><td>√</td><td rowspan="6">This Policy will impact on all groups by protecting staff, visitors and patients from possible security risks. This policy will inform all individuals of the action to take following certain security incidents to reduce the risk of injury or loss.</td></tr>
<tr><td>Patients</td><td>√</td></tr>
<tr><td>Visitors</td><td>√</td></tr>
<tr><td>Carers</td><td>√</td></tr>
<tr><td>Visitors</td><td>√</td></tr>
<tr><td>Other – governors, volunteers etc</td><td>√</td></tr>
<tr><td rowspan="10">Does the document affect protected groups (as defined in the Equality Act 2010) more or less favourably?</td><td colspan="2">Age (younger and older people)</td><td>No</td></tr>
<tr><td colspan="2">Disability (includes physical and sensory impairments,
learning disabilities, mental health)</td><td>No</td></tr>
<tr><td colspan="2">Gender (men or women)</td><td>No</td></tr>
<tr><td colspan="2">Pregnancy and maternity</td><td>No</td></tr>
<tr><td colspan="2">Race (includes ethnicity as well as gypsy travellers)</td><td>No</td></tr>
<tr><td colspan="2">Sexual Orientation (lesbian, gay and bisexual people)</td><td>No</td></tr>
<tr><td colspan="2">Transgender people</td><td>No</td></tr>
<tr><td colspan="2">Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)</td><td>No</td></tr>
<tr><td colspan="2">Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)</td><td>No</td></tr>
<tr><td colspan="4">Proceed to full EIA: No
Reasons: It is anticipated that there will be no barriers to accessing the policy, and that implementation will enable a fair approach. Should a need to review this in the future emerge, a full EIA will be undertaken accordingly.</td></tr>
</table>

Appendix B – Corporate Policy Implementation Plan

Policy Name: Security Policy
Policy Owner: Rob Hayday

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	Promotion of Security Policy	Launch at Stand up and through the Voice	RH	2/10/19	2/10/19	Time on Stand Up agenda, material supplied to Comms
Staff	Access to Policy	Policy available on the Hub	Comms	2/10/19	4/10/19	Document and staff time
Building occupiers	Awareness of contribution required to provision of security for CCG staff	Communication through existing channels eg Tenants Forum	RH	2/10/19	31/10/19	Time on agendas