NHS
South Tyneside
Clinical Commissioning Group

Security Policy

Ratified	Final
Status	Draft
Issued	January 2021
Approved By	Executive Committee
Consultation	Internal CCG review
Equality Impact Assessment	Section 9
Distribution	All Staff
Date Amended following initial ratification	Non-Applicable
Implementation Date	December 2020
Planned Review Date	December 2022
Version	V4.1
Author	Governance Manager, Health & Safety NECS
Reference No	CO17

Policy Validity Statement
This policy is due for review on the date shown above. After this date, policy and process documents may become invalid.

Policy users should ensure that they are consulting the currently valid version of the documentation.

Accessible Information Standards
If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact stynccg.enquiries@nhs.net

Version Control

Version	Release Date	Author	Update comments
V1	28 February 2013	Liane Cotterill	Policy provided to Clinical Commissioning Group (CCG) as part of policy suite
V2	13 November 2014	Lee Crowe	Duties and responsibilities. Equality Impact Assessment. Re-formatted to CCG policy standard.
V3	22 November 2016	Lee Crowe	New EIA and Policy Format
V4	12 December 2018	Lee Crowe	Re-view in line with expiration date. Information added on PREVENT DUTY section 3.15
V4.1	January 2021	Lee Crowe	Minor formatting amendments.

Approval

Role	Name	Date
Approval	Executive Committee	14th January 2015 (2)
Approval	Executive Committee	22nd December 2016 (3)
Approval	Executive Committee	30th January 2019 (4)
Approval	Virtual Executive Committee	April 2021 (4.1)

Review

This document will be reviewed two years from its issue date.

Contents

1. Introduction 4

2. Definitions 5

3. Security Policy………………………………………………………………………..5

4. Duties and Responsibilities 10

5. Implementation 12

6. Training Implications 12

7. Related Documents 12

8. Monitoring, Review and Archiving 12

9. Equality Impact Assessment....... ……………………………………………14**Error! Bookmark not defined.**

1. Introduction

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

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

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

1.1 Status

This policy is a Corporate policy.

1.2. Purpose and scope

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

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

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

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

1.2.4 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 CCG.

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

2. Definitions

The following terms are used in this document:

CCG – Clinical Commissioning Group
NHS – National Health Service
LSMS – Local Security Management Specialist

2.2 Designated Manager for Security

The Designated Manager for Security within the CCG is the Chief Finance Officer.

3. Security Policy

3.1 Responsibilities of CCG managers

3.1.1 All managers in the CCG are responsible for security within their work area. Managers are required to assess security risks as part of the general assessments for their department/service, develop action plans and implement security measures. Managers' responsibilities are summarised in section 4, below.

3.2 Responsibilities of CCG employees

3.2.1 All CCG employees, whether permanent, temporary or working through an agency or other third party, are responsible for acquainting themselves with this policy, following the guidance contained in it and complying with all security measures in their department. Employee responsibilities are summarised in section 4, below.

3.3 CCG Premises

3.3.1 Following risk assessment, managers are responsible for developing any local procedures required ensuring security of premises, for example explicit arrangements for the items listed below. This list is not exhaustive and managers may identify other issues.

- Unlocking and locking of premises
- Responding to violent, aggressive or abusive behaviour
- Access to CCG premises including staff identification badges, key codes
- Security of CCG, patient and staff property, providing appropriate secure storage facilities e.g. lockers
- Lone working/ personal safety
- Relevant arrangements for contractors to access premises as required

3.3.2 Managers must ensure that any keypad alarm codes are changed at appropriate intervals to safeguard the security of the building.

3.4 Access Fobs

3.4.1 Where used, access fobs will be given to staff when joining the CCG. When staff leave CCG employment, all fobs should be returned to the Manager and deactivated.

3.4.2 Fobs should not be swapped or given to unauthorised personnel at any time. Lost or missing fobs should be reported to reception immediately. Fobs will not be given to *ad hoc* visitors.

3.5 Identification Badges

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

3.5.2 When staff leave CCG employment, all ID badges should be returned to the Manager and destroyed. If an ID is lost or stolen this must be reported to the Manager and an incident form completed.

3.6 Visitors / Contractors

3.6.1 All visitors/contractors are to be signed in and out of CCG premises and issued with a visitor pass, which must be displayed at all times whilst on CCG premises.

3.7 CCG Property/assets

3.7.1 Managers are responsible for undertaking risk assessments regarding the security of assets held within their departments and this should be included in the service/departmental general risk assessment. Where appropriate, items should be placed on the asset register. Managers should review CCG property held by their department on a regular basis to ensure that all items are securely managed.

3.7.2 All managers and staff should take all 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 or criminal proceedings being taken.

3.8 Personal Property

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

3.8.2 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.

3.8.3 Staff must report any loss of or damage to their belongings and co-operate in any consequent enquiry into the loss or damage. If private property has been stolen then it is the owner's and not the CCG's responsibility to report the matter to the Police. This should be after notifying a line manager and reporting the incident. Any reference number assigned should also be recorded on the incident log.

3.9 Security of Information – Confidentiality

3.9.1 All safeguards should be taken by staff that handle, receive and use confidential patient/personal information. It is essential that all staff taking up employment with the CCG understand and follow the CCG's confidentiality policy. The relevant CCG information governance policies should be referred to.

3.10 Security of Motor Vehicles

3.10.1 The CCG cannot accept liability for any private motor vehicle or its contents when they are parked on a CCG site or when the car is in being used by an employee on CCG business.

3.11 Lease Cars

3.11.1 In the event of an incident or accident involving a lease car, the employee must notify their manager and the lease car management company in accordance with the car lease policy issued to them.

3.12 Prevention of violence to staff

3.12.1 The CCG has a duty to provide a safe and secure environment for all employees and visitors as well as delivering care and treatment to patients and has a zero tolerance approach to violence or abusive behaviour. The CCG 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 CCG to protect staff, patients and visitors.

3.12.2 Please refer to the relevant Violence, Aggression and Abuse Policy.

3.13 Bomb Threats and the law

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

3.14 Reporting of Security Incidents

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

3.14.2 Reporting falls into the following categories:

- **Assault or abuse of a staff member, patient or visitor**. All incidents of assault or abuse must be reported through an incident reporting form and should be reported as soon as practical after the incident. Staff incidents should be dealt with in line with NHS protocols regarding violence and aggression against staff. All physical assaults to staff should be reported by the Manager through the electronic risk management system. Visitors, patients and staff should always be asked if they wish 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. An incident reporting form must be completed as soon as possible after the incident and passed on as per CCG incident reporting policy.

- Where a **criminal incident is discovered after the fact** and the time of the offence is not known, the report form must be completed as soon as the crime is discovered and then passed on as per reporting policy. The manager should assess the need to involve the police, e.g. it may be necessary to obtain a police reference number for insurance purposes.

- Where a security incident involved the **theft of patient identifiable information** this must immediately be reported to the Caldicott Guardian; Information Governance and Risk Manager. Any theft or loss of data storage e.g. computer, laptop, disks, CDs, tapes should all be reported in this way as well as via the incident reporting form. Also incidents where systems are suspected of being compromised should be reported to the Information Governance and Information Technology Manager. Staff should refer to relevant CCG policy.

- All cases of **suspected fraud or corruption** should be notified immediately to the Chief Finance Officer who will then give advice or arrange investigation of the incident, in accordance with the CCG Standing Financial Instructions.

3.15 PREVENT DUTY

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

- Ensuring that if there are concerns around rooms or buildings being used for radicalisation/terrorism that these are reported immediately within the CCG who will then inform the CSU Health and Safety Team for further guidance via necsu.healthandsafety@nhs.net

- Ensuring staff know which personnel to contact if there are concerns relating to the use of the building this will include contact details for Governance Manager H&S who has responsibility for Security within the CCG premises and ensure Prevent Referral Pathway followed if applicable.
- Ensure staff have received Prevent training as per Prevent Policy and that staff, as a result of training report issues to relevant managers for escalation relating to terrorism and radicalisation
- Have an identified Prevent Lead.

4. Duties and Responsibilities

Council of Practices	The council of practices has delegated responsibility to the Governing Body (GB) for setting the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.
Chief Officer	The Chief Officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Management responsibility	• All Executives, managers and supervisory staff are responsible for the adherence and monitoring compliance within this policy. • All managers in the CCG 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 actions plans and implement security measures. • Arrangements are in place to ensure the security of premises and assets and the safety of staff, patients and visitors taking all preventative measures to safeguard people and property (including occupied but not owned by the CCG) • That risk assessments are in place and where significant security risks exist local procedures are in place to minimise or reduce the impact • That staff are aware of local and CCG security procedures and the results of risk assessments by effective training and communication • Security arrangements are reviewed following incidents and ensure necessary changes in procedures are implemented • Disciplinary procedures are initiated for staff who breach security arrangements • That all criminal activities are reported to the Police and that all security incidents are reported and safeguard are completed • That all staff are briefed with regard to their own personal security and local procedures, and where appropriate, are supported to attend security training • That all staff are issued with staff identification badges (ID badges) • That work areas under their control are operated in accordance with this policy and any associated procedures. That all breaches of security arrangements are investigated and reported immediately in accordance with laid down procedures • That all staff on leaving the CCG return their ID badges, uniforms, keys and electronic passes • That rules with regard to confidential paperwork are adhered to • That advice is sought, as appropriate, from the LSMS and others where there is any doubt as to the standards that are to be applied in adhering to this policy

	• That arrangements are in place to summon the Chief Officer or appointed deputy directly in the event of any serious incident occurring in the area under their control • That official visitors/contractors are issued with the relevant visitor badge and this is monitored to ensure they are carried at all times when on CCG premises • That all security incidents are recorded using the CCG's incident reporting system • 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: • All CCG employees, whether permanent, temporary or working through an agency or other third part, are responsible for acquainting themselves with this policy, following the guidance contained in it and complying with all security measures in their department. • That they are vigilant and responsible in the workplace, bringing to the attention of their immediate manager, as appropriate, any suspicious activity they observe on CCG premises • That they attend appropriate security training or education • That they co-operate with managers to achieve the aims of the security policy, highlighting any identified risks • That they complete incident report forms for all security related incidents • That they wear their staff identification badges at all times • That they report immediately to their departmental manager any loss of or malicious damage to their property.
All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical

	standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Attending training / awareness sessions when provided.

5. Implementation

5.1 This policy will be available to all Staff for use in relation to the specific function of the policy.

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

6. Training Implications

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

7. Related Documents

7.1 Other related policy documents

Violence, Aggression and Abuse Policy.

7.2 Legislation and statutory requirements

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

8. Monitoring, Review and Archiving

8.1 Monitoring

The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

8.2 Review

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

8.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

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

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

8.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: Code of Practice for Health and Social Care 2016.

9. Equality Impact Assessment

Initial Screening Assessment (STEP 1)

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

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

Completed at the earliest opportunity it will help to determine:

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

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

Name: Lee Crowe
Job Title: Governance Manager
Organisation: North of England CSU

Title of the service/project or policy: Security policy

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

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

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

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

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

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

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

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

Accessible Information Standard	**Yes**	**No**
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☐	☐
Please provide the following caveat at the start of any written documentation: **"If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact (ENTER CONTACT DETAILS HERE)"**		
If any of the above have not been implemented, please state the reason: Click here to enter text.		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Lee Crowe	Governance Manager	December 2020

Publishing

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