Bolton Clinical Commissioning Group

Security Policy

Policy Number	**SECUR001**
Target Audience	**CCG Board** **CCG Staff**
Approving Committee	**CCG Health & Safety Committee** **CCG Executive**
Date Approved	
Last Review Date	**June 2015**
Next Review Date	**June 2017**
Policy Author	**CCG Board Secretary**
Version Number	**Draft v0.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
Draft v0.1	June 2015	Risk & Complaints Manager NHSPS Manager	
Draft v0.1		H&S Committee	
Final v1.0		CCG Executive	

Analysis of Effect completed:	By:	Date:

Contents Page

1. Introduction

The CCG can be exposed to a number of security risks relating to staff, patients, premises and assets. Security breaches can have a significant impact on the organisation and its staff.

This policy fits within the framework of the CCG's health and safety arrangements and associated risk management processes. The incident reporting process is important, in the management of security risks. Members of staff are actively encouraged to report all types of incidents, no matter what their severity, to support proactive as well as reactive risk management.

2. Purpose

The CCG intends to maintain a secure environment where staff are confident of their own and any visitor/patients personal safety, the security and safekeeping of information and property of the CCG and other parties. This policy will apply to all CCG leased premises, vehicles, assets and activities. It applies to all members of staff, contractors and visitors.

The main aim of the policy is to minimise potential loss by strict control, as well as minimising violence towards staff, but it also aims to:

- Protect the safety, security and welfare of staff, contractors and the general public, whilst on CCG property.

- Provide safe systems and safeguards against crime, loss, damage or theft or property, equipment or other CCG assets.

The CCG adopts a pro-active approach towards ensuring suitable security arrangements throughout their premises. Its primary objectives are to:

- Undertake security risk assessments at St Peters House to evaluate and resolve any security problems.

- Provide protection to both staff and visitors and their personal effects.

- Establish a security conscious environment to raise awareness amongst staff.

- Support and assist staff who have been subjected to violence at work.

The term "security" applies to the elimination or reduction of the risk of crime across the CCG. It includes:

- Offences against individuals – assault and bodily harm, harassment, theft.

- Offences against property – criminal damage, burglary, theft.
- Offences against assets – fraud, theft, bribery or corruption.

3. Responsibilities

Chief Officer

- The CO has responsibility to ensure that systems are in place to ensure that the risk to employees is minimised as far as is reasonably practicable.

Managers

- Responsible for their own teams' security in terms of providing a safe and secure environment.
- Ensuring their staff understand and comply with this policy.
- Ensuring all significant security risks are identified and measures are implemented to establish a safe and secure environment.
- Actively encouraging the reporting of incidents relating to security issues in accordance with the CCG's incident reporting procedures.
- The initial investigation of any incident related to a security issue and/or violence at work.

Employees Responsibilities

All employees have a duty to co-operate with the implementation of the policy. In particular it should be ensured:

- 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.
- Familiarise themselves with the content of this policy and associated procedures.
- Undertake mandatory conflict resolution training
- Take reasonable precautions for their own security and that of persons who may be affected by their acts or omissions at work.
- Comply with all relevant security procedures for the areas in which they work.
- Use all security systems in accordance with any training and instructions given.

- Report any shortcomings relating to security arrangements as soon as possible.

- Reporting all incidents relating to security and violence at work, via the incident reporting process, and to their line manager.

- Remain alert to the presence of unusual and unexplained packages, which cannot readily be identified. Any such package should be reported immediately to a supervisor or line manager. Under no circumstances should a suspect package be handled.

- Wear CCG identity badges at all times.

- Challenge those without ID badges, making sure people sign in and out and are escorted and accounted for where necessary.

- Store personal items securely at all times, either in a locked room, locked drawer, cupboard or locker. Personal items should not be left accessible. This means staff are responsible for the security of digital lock codes, keys or padlocks that may be in their possession.

- Be alert to the possibility that others might be attempting to deceive and if they do suspect fraud or on-going fraudulent activity they must report the matter in line with the CCG's Anti-fraud & Bribery Policy.

4. Personal Security

a. Physical Assault –

"The intentional application of force to the persons of another, without legal justification, resulting in physical injury or personal discomfort"

Physical assaults include being shoved, pushed, punched, kicked, head-butted, etc.

b. Non-Physical Assault –

"The use of inappropriate words or behaviour causing distress and/or constituting harassment"

The following are examples of non-physical assault:

Offensive language, verbal abuse and swearing, which prevents staff from doing their job or makes them feel unsafe.

- Loud and intrusive conversation

- Negative, malicious or stereotypical comments

- Invasion of personal space
- Brandishing of objects / weapons
- Offensive gestures
- Threats of violence (NB staff on staff bullying should be dealt with via HR policy and procedure)
- Stalking
- Spitting
- Unreasonable behaviour and non-cooperation.

5. Premises security

Directors and senior managers are responsible for ensuring adequate security arrangements are in place for the buildings where they are responsible for service delivery. Site security is an issue for all staff and a general level of awareness is essential. Any untoward findings should be reported immediately to the manager responsible for the site and/or service.

All members of staff should ensure that their work areas are secured at the end of the working day (where applicable,) and that departmental keys are held in a secure place at all times.

The loss of any key(s) must be reported to the manager and to the CCG's Health and Safety Officers. It is important to avoid delay so as to ensure premises can be secured.

NHS Property Services Facilities Management staff will be responsible for issuing and holding all spare keys associated with suited or security locks and on no account must replacements be cut without prior permission.

Members of staff, who require access through any door, which is controlled via digital door locks, will be issued with the appropriate code numbers, to ensure the security of the area is maintained at the highest level. Code numbers must not be issued to unauthorised personnel.

All access codes should be changed:

- Annually, or
- Whenever it is felt that the code may have become compromised, or
- Following the departure of a member of staff.

Members of staff should be aware of anyone trying to 'tailgate' – i.e. gain access to a controlled access area by closely following them as they enter. If the person is not recognised as a member of staff, or authorised visitor, he/she should be asked to:

- Wait at the door or in a designated waiting area.
- Give details of the person with whom they have an appointment.
- Await the arrival of an identified member of staff to escort him / her into the controlled access area.
- At the end of the appointment / meeting, the visitor should be escorted out of the controlled access area.

6. Visitors

Where appropriate, visitors should sign in at the reception area. They should wait in the reception area until they are escorted to their destination.

At the end of the meeting, the visitor will be directed back to the reception area to sign out, prior to departure.

7. Staff property

Each member of staff is responsible for the safe keeping of his / her own property. Staff should consider what personal belongings they need to bring to work and ensure they are held securely in the building. The loss of personal belongings must be reported immediately to the employee's line manager and an incident report completed. Where appropriate, the police must be contacted.

8. Reporting and Investigations

All security incidents must be reported via the incident reporting procedures as quickly as possible so that an internal investigation may be initiated. When a criminal offence is committed or alleged to have been committed on CCG premises by any person, staff should inform their line manager and also contact the police without delay.

The Manager will liaise with the police, affected staff and the line manager regarding any investigation or offence. The Manager will conduct an internal investigation into any significant security breaches. Investigations involving staff or patients will be handled fairly, in line with the CCG's equality and diversity arrangements.

9. Monitoring and Review

Managers will be responsible for monitoring and reviewing their own local security risk assessments and associated building arrangements. The review of policies will also be based on the prioritisation of risk within the CCG and as a consequence of any serious incidents.

Security breaches and other loss events will be reported on a regular basis to the Governance & Risk Committee and Health and Safety Committee. The investigation of such incidents will be used as a tool to identify common causes, assist police, prevent reoccurrence and assess the effectiveness of policy controls.

10. CCG Premises

Following risk assessment, managers are responsible for developing any local procedures required to ensure 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.

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

11. Car Park Fobs

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.

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.

12. Identification Badges

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.

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

13. Visitors/Contractors

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. For security reasons all visitors must be escorted to and from their destination within CCG buildings.

14. CCG Property/assets

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.

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.

15. Personal Property

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

Staff are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work. Where storage has been provided for personal use, the individual to whom it is allocated will be responsible for ensuring it is locked.

Staff must report any loss of or damage to their belongings and co-operate in any consequent enquiry into the loss or damage. If private property has been stolen then it is the owners 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.

16. Security of Information – Confidentiality

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.

17. Security of Motor Vehicles

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 being used by an employee on CCG business.

18. Lease Cars

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 company issued to them.

19. Prevention of violence to staff

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.

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

20. Bomb Threats and the law

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.

21. Reporting of Security Incidents

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

Reporting falls into the following categories:

- **Assault or abuse of a staff member, contractor 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, CD's, 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's Standing Financial Instructions.

22. Implementation

- This policy will be available to all staff for use in the circumstances described on the title page.

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

23. Training Implications

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

24. Documentation

- **Other related policy documents.**

- **Legislation and statutory requirements**
  Health and Safety Executive (1974) Health and Safety at Work etc. Act 1974. London HSE.

- Best practice recommendations

25. **Monitoring, Review and Archiving**

- **Monitoring**

  The Chief Officer will oversee, on behalf of the governing body, a method for monitoring the dissemination and implementation of this policy.

- **Review**

  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.

  Staff who become aware of any chance 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.

  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.