Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

Security Policy and Procedure

August 2021

Version:	V2
Policy Number:	CO033/10/2022
Date ratified:	31 August 2021
Name of originator/author:	Ian Plummer – Health and Safety Manager - South Yorkshire and Bassetlaw Shared Service
Name of Sponsor:	Director of Finance
Name of responsible committee	Governance Sub-committee
Date issued:	September 2021
Review date:	1 October 2022
Target audience:	All staff working within or on behalf of NHS Sheffield CCG

To ensure you have the most current version of this policy please access via the NHS Sheffield CCG Intranet Site by following the link below:

http://www.intranet.sheffieldccg.nhs.uk/policies-procedure-forms-templates.htm

MINDFUL EMPLOYER

disability confident EMPLOYER

Policy Audit Tool

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval

1	**Details of Policy**	
1.1	Policy Number:	CO033/10/2022
1.2	Title of Policy:	Security Policy and Procedure
1.3	Sponsor	Director of Finance
1.4	Author	Ian Plummer, Health and Safety Manager, Health, Safety and Security Shared Service
1.5	Lead Committee	Governance Sub-committee
1.5	Reason for policy:	Legislative requirement
1.6	Who does the policy affect?	All staff and visitors
1.7	Are there national guidelines/codes of practice etc issued?	No
1.8	Has an Equality Impact Assessment been carried out?	Yes
2.	**Information Collation**	
2.1	Where was Policy information obtained from?	Legislation
3.	**Policy Management**	
3.1	Is there a requirement for a new or revised management structure for the implementation of the Policy?	No
3.2	If YES attach a copy to this form.	
3.3	If NO explain why.	Fits with current arrangements
4.	**Consultation Process**	
4.1	Was there external/internal consultation?	Yes
4.2	List groups/persons involved	Health and Safety Group
4.3	Have external/internal comments been included?	
4.4	If external/internal comments have not been included, state why.	N/A
5.	Implementation	
5.1	How and to whom will the policy be distributed?	Staff will be made aware of all new policies via the Weekly Bulletin and Staff Briefing. Policies will be available on the intranet.
5.2	If there are implementation requirements such as training please detail.	
5.3	What is the cost of implementation and how will this be funded	N/A
6.	**Monitoring**	
6.2	How will this be monitored	Governance Sub-committee and Health and Safety Group
6.3	Frequency of Monitoring	Quarterly

Contents

PART A – POLICY

1. Introduction

1.1 NHS Sheffield Clinical Commissioning Group (CCG) is committed to a safe and secure environment that protects staff, patients and visitors, and the property and physical assets of the CCG, via Health and Safety legislation, Department of Health policy and by common law duty of care. This policy aims to deal proactively with the CCG's security arrangements.

1.2 The CCG acknowledges its responsibility for the safety of people within the organisation and wider, and the requirement to have a written statement of general policy under the statutory requirements of the Health and Safety at Work Act 1974

1.3 The policy, together with any subsequent revisions, will be brought to the notice of all CCG employees.

2. Statement of Policy

2.1 The CCG recognises its responsibilities to ensure that reasonable precautions are taken to provide a safe and secure working environment and that steps are taken to prevent issues in relation to security management, in compliance with relevant statutes and code of practice (as identified above). It is the CCG's intention to take all reasonable practicable steps to reduce the associated risks from security issues.

2.2 In pursuance of this aim, the CCG will:

- Protect the safety, security and welfare of staff, patients and the general public whilst on CCG premises.
- Provide systems and safeguards against crime, loss, damage or theft of property and equipment.
- Minimise disruption or loss of service to patients/clients.
- Ensure risk assessments and security audits are implemented to comply with statute.
- The CCG will also ensure, so far as is reasonably practical, that all employees who are required to work alone for significant periods of time are protected from risks to their health and safety.

2.3 The CCG recognises that this Policy Statement is implemented in pursuit of these aims.

3. Scope

3.1 This policy applies to those members of staff that are directly employed by NHS Sheffield CCG and for whom NHS Sheffield CCG has legal responsibility.

3.2 For those staff covered by a letter of authority / honorary contract or work

experience this policy is also applicable whilst undertaking duties on behalf of NHS Sheffield CCG or working on NHS Sheffield CCG premises and forms part of their arrangements with NHS Sheffield CCG.

4. Accountabilities, Roles and Responsibilities

Security is a management responsibility and the provision of a security service in no way relieves management at any level of its obligations to fulfill the stated purpose of security in the CCG. Managers are required not only to exercise preventative aspects but also to take appropriate action where necessary in respect of those who offend against the law, commit misconduct or other breach of security in contravention of the policies of the CCG.

4.1 Accountable Officer

Overall accountability for ensuring that there are systems and processes to effectively manage security lies with the Accountable Officer who takes the risks to the CCG from breaches of security seriously and seeks to reduce the numbers of incidents occurring as a direct result.

4.2 Director of Finance

The Director of Finance has lead responsibility for the development and strategic review of security within Sheffield CCG.

The Director of Finance is responsible for:

- The formulation, implementation and maintenance of an effective Security Policy in consultation with staff representatives, and ensuring that managers co-ordinate and implement the policy in their respective areas
- Reviewing and amending this policy to ensure compliance with any current guidance
- Instituting regular campaigns to highlight the importance of security and the responsibilities of all CCG staff
- Leading security management within the CCG and identifying security initiatives for improving security across the CCG
- Advising the CCG of any requirements, statutory or other, by the preparation of procedures for dealing with crime prevention, supply of security systems and maintenance
- Monitoring the performance of the CCG with regard to the implementation of this policy.

4.3 Corporate Services Facilities Manager

The Corporate Services Facilities Manager is the named deputy for the Director of Finance with regards the responsibility for security management

4.4 Local Security Management Specialist (LSMS) / Competent Person for Security

The nominated Local Security Management Specialist (LSMS) / Competent Person for Security for the CCG is the Head of Specialist Advice, Health and Safety (South Yorkshire and Bassetlaw Clinical Commissioning Groups shared services (SY&BCCGs)). The overall objective of the LSMS will be to work on behalf of NHS Sheffield CCG to deliver an environment that is safe and secure.

This objective will be achieved by working in close partnership with stakeholders within NHS Sheffield CCG, and external organisations such as the police, professional representative bodies and trade unions. The LSMS will aim to provide comprehensive, inclusive and professional security management services for NHS Sheffield CCG and work towards the creation of a pro-security culture within the NHS.

The LSMS will:

- Report to NHS Sheffield CCG Security Management Director (SMD) on security management work locally
- Lead on the day to day work within NHS Sheffield CCG to tackle violence against staff and professionals in accordance with national guidance
- Ensure that lessons are learned from security incidents, and that these incidents are assessed and the impact on the CCG reported to appropriate authorities in accordance with guidelines issued by the NHS SMS
- Investigate security incidents/breaches in a fair, objective and professional manner so that the appropriate sanctions (and allow consideration of preventative action to be taken)
- Ensure that the security management policy addresses all the organisations identified risks and contains all the required elements from guidance
- Ensure that the security management policy is reviewed or evaluated to establish its effectiveness
- Ensure that any corrective or preventative actions identified as a result of the policy review or evaluation is implemented, to ensure that the security management policy continues to address the CCG's identified risks

4.5 Other Service leads or equivalents

Other Executives, on behalf of the Accountable Officer are responsible for ensuring that the CCG's security policy is implemented within the organisation.

This will include responsibility for:

- Planning any capital investment required to address matters arising from risk assessment.

- The preventative measures and appropriate action in respect of persons who are suspected of committing a criminal offence, misconduct or other breach of security in contravention of the policies of the CCG
- Ensuring staff awareness of and how to access this policy and other relevant documents and their responsibilities and also ensure that staff (including temporary staff) receive training appropriate to the risks involved
- Ensuring that security arrangements within their area are being observed and that deficiencies are reported
- Ensuring that any particular security problems known to them are reported accordingly
- 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

4.6 Line Managers

Line Managers are responsible for:

- Ensuring compliance with CCG Security Policy requirements in the areas for which they are responsible
- The completion of any risk assessments required in relation to security of staff or premises
- Ensuring that any security problems known to them are reported accordingly

4.7 Responsibilities of all Staff

Responsibilities of staff (including all employees, whether full/part time, agency, bank or volunteers) are:

- To co-operate with management to achieve the aims and objectives of the Security Policy. Great emphasis is placed on the importance of co-operation of all staff in observing security and combating crime
- The protection and safe keeping of their private property. Any loss of private property must be reported without delay. If private property has been stolen, then it is the owner's responsibility, not the CCG's responsibility to contact the police

Staff to familiarise themselves with the following:

- Any special security requirements relating to their place of work or work practices
- The action to take in the event of a security incident
- To safeguard themselves, colleagues, visitors, patients/clients etc., so far as is reasonably practicable, and ensure that neither equipment nor property are put in jeopardy by their actions or omissions, either by instruction, example or behaviour
- To follow prescribed working methods and security procedures at all times

- To co-operate with managers to achieve the aims of the Security Policy
- To comply with all training requirements concerning security issues
- To wear an identification badge when engaging with the public and/or in a patient setting.
- To notify their line manager of any potential security problems and report all incidents involving criminal activity on to Datix
- To report any crime/breach of security to the CCGs online incident reporting system. This procedure is documented as Appendix 1.

All staff are reminded that it is an offence to remove property belonging to the CCG without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal proceedings being taken.

NHS Sheffield CCG will not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. Motor vehicles are brought onto the site entirely at the owner's risk. NHS Sheffield CCG will take reasonable steps to safeguard vehicles on their property.

In accordance with their job description, individual members of staff may have responsibilities for:

- The appropriate use of security equipment (including secure doors, alarms and detectors) provided by the CCG for the health, safety and security of its staff, and reporting any faults to the Corporate Services Facilities Manager.
- Safeguarding of equipment and property whilst on CCG business.

All staff are required to adhere to safe practices as part of their job description.

4.8 NHS Counter Fraud Authority

The NHS Counter Fraud Authority was established in November 2017 as a specialist organisation with the commitment to protect the NHS by ensuring that resources made available to patient care and services are not lost to fraud and corruption.

5. Dissemination, Training and Review

5.1 Dissemination

The Security Policy is located on the policies page of the intranet. Staff are notified by Weekly Round-Up / Team Brief of new or updated procedural documents.

5.2 Training

5.2.1 An integral requirement for the effective implementation of a security management system is the training of all staff (including temporary staff) in Information Governance.

The training will cover the importance of significant security effects, roles and responsibilities for security management functions, and the consequences of non-compliance.

Information Governance is integrated into mandatory on-going training programmes as required based on risk assessments.

The CCG will ensure that appropriate information, instruction and training is given to employees who may be required to work alone, to ensure that so far as is reasonably practicable a safe system of work is in operation.

Frontline staff should undergo Conflict Resolution Training and attend refresher training on a 3 yearly basis, as well as preventing and reporting crime in the workplace. This training should be included in departmental programmes as part of in-service training, and with periodic refresher courses. Training involves dealing with situations of potential or actual abuse, aggression or violence, and includes:

- understanding the cause;
- recognising the warning signs
- identifying when and where to get help
- interpersonal skills/defusing techniques

5.3 Review

5.3.1 As part of its development, this procedural document and its impact on staff, patients and the public has been reviewed in line with NHS Sheffield CCG's Equality Duties. The purpose of the assessment is to identify and if possible remove any disproportionate adverse impact on employees, patients and the public on the grounds of the protected characteristics under the Equality Act 2010.
The procedural document will be reviewed every two years, and in accordance with the following on an as and when required basis:

- Legislatives changes
- Good practice guidelines
- Case Law
- Significant incidents reported
- New vulnerabilities identified
- Changes to organisational infrastructure
- Changes in practice

PART B – PROCEDURE

1 Rehabilitation of Offenders Act 1974

1.1 All persons applying for a post within the CCG must have completed the section on the application form entitled Rehabilitation of Offenders Act 1974. This section states that 'because of the nature of the work for which you are applying, this post is exempt from provisions of Section 4(2) of the Rehabilitation of Offenders Act, 1974 (Exemption) Order, 1975.' Applicants are therefore, not entitled to withhold information about convictions which for purposes are 'spent' under the provisions of the Act, and in the event of employment, any failure to disclose such convictions or new convictions could result in dismissal or disciplinary action by the CCG.

1.2 This application form also requests details of any convictions, adult cautions or bind-overs, and requires the applicant to sign the statement confirming that the information given is correct. For more information refer to the Recruitment and Selection Policy.

2 Children Act 2004

2.1 In accordance with the provisions of the Children's Act 2004, the CCG must ensure that staff who occupy certain positions that brings them regularly in contact with children have a criminal record check. An application for a Disclosure & Baring Service (DBS) will be requested following appointment of the staff member by the Human Resources Department. Please refer to the Recruitment and Selection Policy.

3 Personal Security

3.1 Specific procedures are available for local needs such as domiciliary visits (e.g. lone workers), staff in other premises, reception staff, agile workers etc. implemented by individual departments. All staff must follow existing health and safety policies and guidelines.

4 Staff Identification

4.1 Every employee including bank staff, will be issued with an identification badge on commencement of employment which must be worn at all times whilst on CCG premises or on official business.

4.2 Each member of staff is personally responsible for their badge, and to ensure that the badge is up to date and that there are no radical changes in physical appearance, job title or department. It is imperative that all staff wear an official CCG identification badge and it is the responsibility of all line managers to ensure that this is implemented.

4.3 The identity badge will state the employee name and job title and must be clearly visible to other staff and visitors.

4.4 Identification badges must be returned to their line manager when a member of staff leaves the employment of the CCG. It is the responsibility of the senior manager completing the termination documentation to recover the identity badge from the member of staff concerned and return it to the Corporate Services Facilities Manager for destruction.

4.5 External contractors should be escorted on site. The member of staff who is responsible for the contractor will arrange for the contractor to be escorted to the relevant area.

4.6 Contractors and visitors are required to use the sign in / out register on reception.

5 Key Holding

5.1 Access to the building out of normal working hours is arranged by the Facilities team.

6 Access and Egress

6.1 Access to NHS Sheffield CCG premises is restricted. The responsibility for the arrangements for daily opening/closing premises rests with the Corporate Services Facilities Manager.

6.2 Access to secure areas where appropriate will be controlled by the use of digital locks

7 Security of Goods

7.1 Goods received into the organisation are checked against delivery notes prior to signing for acceptance. The organisation will provide secure accommodation for goods awaiting distribution.

8 Security of Personal Belongings

8.1 All staff should ensure that personal belongings are stored in a secure location eg locked in cupboards, lockers or desk drawers. The CCG cannot be held responsible for theft of personal items that are not secured.

9 Fraud

9.1 The responsibilities for fraud prevention are described in the CCG Fraud, Bribery and Corruption Policy.

10 Fire

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

11 Information Security

11.1 Information security risk is inherent in all administrative and business activities, everyone working for or on behalf of NHS Sheffield CCG continuously manages information security risk. The aim of information security risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved in all our organisational activities. It requires a balance between the cost of managing and treating information security risks with the anticipated benefits that will be derived.

12 Harassment, Violence and Aggression

12.1 Any member of the public or patients who abuse NHS Sheffield Clinical Commissioning Group staff may have sanctions taken against them, be refused treatment, or taken to court by the CCG.

For any occurrences of violence and aggression by staff to other members of staff or Service users / members of the public, please follow the guidance contained within the Dignity at Work (Prevention of Bullying and Harassment) Policy and Disciplinary Policy

12.2 **Harassment and Violence:**

The Health and Safety Executive (HSE) defines harassment and violence as unacceptable behaviour by one or more individuals that can take many different forms, some of which may be more easily identifiable than others.

12.3 Harassment occurs when someone behaves in a way which offends you or makes you feel distressed or intimidated. This could be abusive comments or jokes, graffiti or insulting gestures. This may occur either inside or outside working hours.

12.4 Violence is the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death or psychological harm, this may occur either inside or outside working hours.

Both may be carried out to staff by service users or members of the public with the purpose or effect of violating a manager's or staff member dignity, affecting his/her health and/or creating a hostile work environment.

12.5 Harassment and violence can:

- Be physical, psychological, and/or sexual.
- Be amongst colleagues, between superiors and subordinates or by third parties such as clients, customers, patients etc.
- Range from minor cases of disrespect to more serious acts, including criminal offences, which require the intervention of public authorities.

12.6 Harassment can be further defined as any conduct which:

- Is unwanted by the recipient
- Is considered objectionable by the recipient
- Causes humiliation, offence and distress (or other detrimental effect)

The key to distinguishing between what does and does not constitute harassment is that harassment is behaviour that is unwanted by the person to whom it is directed. It is the impact of the conduct and not the intent of the perpetrator that is the determinant.

Harassment is a course of conduct which may occur against one or more individuals. Harassment may be, but is not limited to:

- Physical contact – ranging from touching to serious assault, gestures, intimidation, aggressive behaviour
- Verbal – unwelcome remarks, suggestions and propositions, malicious gossip, jokes and banter, offensive language
- Non-verbal – offensive literature or pictures, graffiti and computer imagery, emails, texts, isolation or non- co-operation and exclusion or isolation from social activities
- Unwanted conduct related to a protected characteristic which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, humiliating or offensive environment for that individual.

12.7 Aggression:

- a forceful action or procedure (such as an unprovoked attack) especially when intended to dominate or master
- hostile, injurious, or destructive behaviour or outlook especially when caused by frustration aggression is often the expression of pent-up rage
- spoken or physical behaviour that is threatening to the individual and or involves harm to someone or something

12.8 Assessing the risk of violent behaviour

Violent incidents do not necessarily have to cause physical harm. They can:

- Involve a threat, even if no serious injury results.
- Involve verbal abuse.
- Involve non-verbal abuse, for example gestures, emails, texts.

Involve other threatening behaviour, for example stalking,

In any situation where physical assault is considered imminent, staff should immediately leave the area if able and contact security (if available) or the police (9-999 from an internal phone or 999 from a mobile).

12.9 The process for staff following violent or abusive behaviour from service users or members of the public

All instances of actual or threatened violence and aggression must be reported on to Datix the report will be used to ensure that other members of staff benefit from shared experiences and training can be realistic and relevant.

Staff that have been subjected to violent / abusive behaviour from service users or members of the public should report such incidents to their line manager. The line manager will need to consider whether the matter should be referred to the Police.

Incidents of violence and aggression can have a detrimental effect on the victim out of proportion to the scale seen by outsiders. Managers are to ensure that staff are supported as soon as is reasonably practicable after such incident(s).

It is important that an investigation into the matter is conducted and staff are informed of the basic details of the incident and any counter measures planned to prevent a similar occurrence.

Sheffield CCG will make training available in the management and handling of violence and aggression, based on the training needs analysis. In any cases where a member of staff feels that a service user or member of the public has behaved in an inappropriate manner, the line manager must be informed of the occurrence and a Datix report completed as soon as reasonably practicable.

12.10 Dealing with harassment, violence and aggression pro-actively

Staff should attempt to avoid physical intervention at all costs and be aware of their own verbal and non-verbal communication. Conflict Resolution Training (CRT) is available to members of staff.

Techniques include:

- Simply ask the person who is becoming aggressive to stop, some people will respond to this
- attempting to establish a rapport
- offering and negotiating realistic options
- avoiding threats
- asking open questions and asking about the reason for the service user's concern
- showing concern and attentiveness through non-verbal and verbal responses;
- listening carefully
- attempting to neither patronise nor minimise the service user's concerns

12.11 Possible warnings which may indicate an individual's behaviour is escalating towards physically violent behaviour includes but not limited to:

- Direct prolonged eye contact

- Facial colour may darken / go pale
- Head drops to protect throat
- Lips tighten over teeth
- Eyebrows droop to protect eyes
- Breathing rate accelerates
- Fists clenching and unclenching
- Subject stands tall
- Behaviour may stop/start abruptly
- Kicking the ground
- Large movements close to people
- Hands rise above waists
- Shoulders tense
- Stare is now at intended target
- Stance moves from square to sideways
- Lowering of body to launch forward

12.12 Dealing with harassment, violence and aggression reactively

Dependent on the circumstances, in an incident involving harassment, violence and aggression, the following course of action (12.13) could be pursued in conjunction with any other course of action, but always in consultation with Senior Management. Any and all action must be fully and factually documented and an incident report form completed.

12.13 Actions following violent or abusive behaviour

Where a patient, relative or member of the public is alleged to have carried out an act of violence, abuse or aggression then the CCG reserves the right to respond to the alleged incident, as deemed necessary in light of the circumstances. The level of response will be dependent upon the seriousness of the incident and the outcome of any investigation. The potential responses or actions available to the CCG include:

- Verbal warnings with a follow up letter to the individual
- Recommendation to use advocacy services
- Warning flag applied to patients notes
- Meeting with the individuals
- Written warnings from the CCG
- Withdrawal of services
- Involvement of the Local Security Manager
- Involvement of the police
- Criminal prosecution
- Civil Prosecution
- Support mechanisms

12.14 Dealing with actual or threatened violence and aggression could have an effect on an employee's health and wellbeing, and they may feel that they need further support with this. Sheffield CCG is committed to the health and well-being of staff,

and has therefore put in place an employee assistance programme (EAP) to provide additional support where needed. The EAP will offer employees a variety of support services, including financial, legal, education, consumer and family care advice as well as access to 24 hours a day, 7 days a week health advice lines, staffed by qualified pharmacists and nurses. In addition to this, the programme will also offer staff free access to counselling services. Staff, when experiencing an issue where they feel counselling would be beneficial will be able to contact the employee assistance provider and have up to 5 face to face counselling sessions. The counselling lines are open 24 hours a day 7 days a week and are staffed by qualified counsellors and psychologists.

13 CCTV

13.1 External CCTV is in place at 722 Prince of Wales Road and is managed by the Landlord's Agent on behalf of the landlord.

14 Major Incident

13.1 A major incident is a serious unforeseen occurrence causing disruption to the normal life of the CCG; suddenly with little or no warning and causing or threatening death or serious injury to staff and members of the public; damage or destruction of property which necessitates special mobilisation and organisation. Please refer to the Business Continuity Policy.

15 Risk Assessment

15.1 The Management of Health and Safety at Work Regulations 1999 (Regulation 3) requires that suitable and sufficient risk assessments be undertaken, so that the significance of a hazard can be identified assessed and controlled. Guidance on assessing risks to safety and health can be found on the CCG intranet (http://www.intranet.sheffieldccg.nhs.uk/copy-of-health-and-safety/risk.htm)

It is the responsibility of line managers to ensure that these are carried out, and a copy of the assessment forwarded to the SMD or their deputy.

15.3 Risk Assessments should be completed for all security hazards including physical (buildings, equipment etc.) and people. These risk assessments are the responsibility of the department involved. Staff undertaking risk assessments should have first received training in how to complete a risk assessment.

15.4 Any actions identified from the risk assessment will form part of the CCG health and safety action plan and will be monitored by the Health and Safety Group.

15.5 Risks relating to security are identified on an on-going basis through incident reports, complaints and claims procedures, and the risk assessment procedure.

15.6 It is important that all staff within the CCG are aware of the security risks involved within their work. They must also be aware of formal risk assessments that apply to them, the actions identified to control the risks and the measures to be taken by

them personally to reduce the risks to themselves and others. A copy of the risk assessments can be located here.

15.7 When working arrangements are agreed with an individual which result in that person working alone for regular/significant periods, the manager will be responsible for ensuring that a risk assessment is undertaken and that a related safe system of work is put into place. This will take into account the capability of the individual. The employee will be required to conform to these arrangements, to safeguard both themselves and NHS Sheffield CCG.

15.8 Working alone is not illegal, but it can bring additional risks to a work activity. The CCG has developed procedures to control the risks and protect employees, and employees should know and follow them. Apart from the employee being capable of undertaking the work/detail the three most important aspects to be certain of are that:

- the lone worker has full knowledge of the hazards and risks to which they are exposed
- the lone worker knows what to do if something goes wrong
- someone else knows the whereabouts of the lone worker and what he/she is doing

For further guidance please refer to the CCG's Lone Working Policy

16 Monitoring the Compliance and Effectiveness of this Procedure

The Health and Safety Group will be responsible for monitoring compliance with, and the effectiveness of, this procedure. In discharging this responsibility the Health and Safety Group will take into account:

- Any security incident reported via the CCG's incident reporting system
- The results of the annual security audit

17 References

The following legislation and guidance has been taken into consideration in the development of this procedural document:

- The Regulation of Investigatory Powers Act 2000
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013.
- Data Protection Act 1998
- The General Data Protection Regulations 2018
- The Protection from Harassment Act 1997
- Control of Substances Hazardous to Health 2004 Approved Codes of Practice

- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Criminal Procedure and Investigation Act 1996
- Police and Criminal Evidence Act 1984
- Criminal Justice and Public Order Act 1994
- CCTV Code of Practice 2000
- Equality Act 2010

18 Review of the Procedure

This procedure will be reviewed every two years, and in accordance with the following on an as and when required basis:

- Legislatives changes
- Good practice guidelines
- Case Law
- Significant incidents reported
- New vulnerabilities identified
- Changes to organisational infrastructure
- Changes in practice

Appendix 1

Reporting of Crime/Security Incidents

1 All staff have a responsibility to report any crime/breach of security. This reporting falls into the following categories:

1.1 NHS Sheffield CCG Premises

1. When a crime/security incident is taking place dial 9 999 and report the incident to the police and follow their advice. You must then contact the Security Management Director or their Deputy as soon as practicable and inform them of the incident.
2. A Datix report requires completing

1.2 External Locations

1. When a crime/security incident is taking place, you should call the police immediately by telephoning 999.
2. Where a security incident is discovered, the information should be passed to the Security Management Director or their Deputy as soon as practicable.
3. A Datix report requires completing

1.3 Out of Hours

1. When a crime/security incident is taking place, you should call the police immediately by telephoning 999.
2. Following this; the incident should be reported to the Security Management Director or their Deputy as soon as practicable, who will investigate the incident
3. A Datix report requires completing

1.4 Suspicious (suspect) packages

- A suspect package is a package believed to contain a potentially harmful device or substance.
- Any suspect package or letter when received must immediately be placed in isolation and away from water, chemicals, heated surfaces, naked flames and gaseous substances. It is more likely to be an incendiary device than a bomb; i.e. it is designed to start a fire
- Do not shake it, squeeze, or open the letter or package
- Turn off all fans, photocopiers, printers, computers and heaters within the room where the letter/package is located and evacuate the room, close all doors. Place a clearly visible warning on the door.

- Any suspicious packages found, should NOT be moved and its position should be reported to the Security Management Director or their Deputy or a member of the Senior Management Team

Undertake initial investigation (without touching or moving the package) identifying:

- The listed owner of the package
- Visible wires or electrical components showing from the package, especially where the wrapping has been damaged
- Any greasy marks on the envelope or package
- If an unknown powder or liquid substance is leaking from the package
- Distinctive smells from the package e.g. almonds/marzipan, ammonia or machine oil
- If the package when received was heavy for its size or has an uneven distribution of weight or has excessive wrapping
- If the package was delivered by hand from an unknown source or posted from an unusual place
- If in doubt, dial 9 999 and report to the police and evacuate the building without sounding the fire alarm, closing doors behind you.
- Do not use mobile telephones near suspect packages.
- If you feel you may have been contaminated, go to an isolated room and avoid other people if you can. It is vitally important that you segregate yourself and others who may have come into contact with the suspicious package. It is unlikely that you have been contaminated and you will get medical treatment if required. Signs that people may have been exposed to a chemical incident are streaming eyes, coughs and irritated skin. Do not rub your eyes; touch your face or other people. Thoroughly wash your hands in soap and water as soon as possible.
- Where convenient, fire assembly points can be utilised for the purpose of evacuation, but only if they are located at a distance of at least 400 metres from the suspected bomb site. Safe assembly points are best situated behind a solid building at a distance away from the blast site.
- Complete a Datix report

1.5 Bomb threats

- A bomb threat is a threat to detonate an explosive or incendiary device to cause property damage or injuries, whether or not such a device actually exists. Bomb threats are usually made verbally over the phone.
- Notification of a bomb threat can be made at any time and can be made and delivered by several means, usually anonymous, but all must be considered seriously.

- Any member of staff receiving a telephone threat regarding a suspect package or explosive device should obtain as much detail as possible from the caller. The police should be informed immediately - dial 9 999 and report to police and evacuate the building without sounding the fire alarm and closing doors and windows behind you. Report the situation to the Security Management Director or their Deputy or a member of the Senior Management Team who will decide whether an emergency should be declared in line with the Emergency Preparedness, Resilience & Response Policy.
- Complete a Datix report as soon as is practically possible following the event

Appendix 2

Evacuation Procedure to be followed in the event of a Bomb Threat

[Awaiting details from Landlord's Agents November 2019]