

# Security Policy and Strategy

Reference No:	P_HS_05
Version:	9.1
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Local Security Management Specialist
Name of responsible committee/individual:	Health and Safety Committee
Date issued:	August 2018
Review date:	December 2021
Target audience:	All Staff
Distributed via:	Website

**Lincolnshire Community Health Services NHS Trust**

**Security Policy and Strategy**

**Version Control Sheet**

<b>Version</b>	<b>Section/Para/ Appendix</b>	<b>Version/Description of Amendments</b>	<b>Date</b>	<b>Author/Amended by</b>
1		TO BE ARCHIVED		
2	Policy Statement  Introduction  Section 3.3 Section 3.4  Section 3.10 Section 4  Section 4.4 Section 4.6  Section 7.1 Appendix 1 added	Responsibility of LSMS amended. Training paragraph amended.  1 <sup>st</sup> paragraph added in "visitors"  Updated.  Updated to include the production of an annual work plan.  Updated to include quarterly reports of security management work.  Bullet point 3; as soon as practicable added.  Section added to include RIPS; this updates and overrides HS007 which is to be archived.  Amended.  Amended.  Simple Risk Qualification.	December 2009	Carl Ramsdale LSMS

3	Section 4.7	Lockdown added.	July 2010	Carl Ramsdale LSMS
4	Responsibilities	Insert Finance Director/Deputy Chief Executive as SMD.	November 2011	Carl Ramsdale LSMS
	Titles amended			
	Section 4.7	All reference to NHS CFSMS changed to NHS Protect.		
	Dissemination			
	Trust Title	Amended.		
	Section 3.4	Amended.		
	Section 3.6	Amended		
	Section 3.7	Amended		
Section 3.8	Amended			
Section 4	Policy number changed from HS010 to P_HR_05			
5	Responsibilities and title amended	Insert Director of Human Resources and Organisational Development as Security Management Director	September 2012	Carl Ramsdale
	Policy	Reference to Directions replaced by NHS Protect standards.  Titles amendment Clinical Governance and Risk Committee.	September 2013	Carl Ramsdale
	Section 3	Insertion of NHS Protect requirements and responsibilities amended.		
	Section 4			
	Section 5	RIPA amended. Bomb alerts amended.		
	Section 6	Lockdown amended.		
	Section 7	Risk Assessment amended.  Insertion of NHS Protect annual SRT requirements.  Guidance and training amended.		
7	Review	All sections no change.	June 2015	Carl Kisby

8	Full Document	All sections reviewed.  Updates and amendments made to reflect changes with other policies and organisational structure.  Policy title changed.  Strategy added.	March 2016	Craig Evans
9	Full Document	Update with new Trust Branding, general review	March 2018	Craig Evans Carl Kisby
9.1	Entire document	This document has been checked by the policy owner who has confirmed that it is fit for use and that it will be fully reviewed and updated as appropriate before the end of the extension period granted by LCHS Trust Board on 12/1/2021	January 2021	Corporate Governance Team
10				

Copyright © 2021 Lincolnshire Community Health Services NHS Trust, All Rights Reserved. Not to be reproduced in whole or in part without the permission of the copyright owner.

# Lincolnshire Community Health Services NHS Trust

## Security Policy and Strategy

### Policy Statement

#### Background

Lincolnshire Community Health Services NHS Trust recognises its duties and responsibilities to provide a secure environment for its staff, patients, and visitors. All employees of the organisation, wherever they work, are responsible for ensuring a secure environment by adherence to this, and associated policies and procedures. Patients and visitors using the organisation's services are expected to conduct themselves in a reasonable manner and not adversely affect the security of the healthcare environment.

#### Statement

Lincolnshire Community Health Services NHS Trust takes extremely seriously the health, safety and welfare of all staff. It recognises that the need to provide and protect a secure environment for its staff, service users, visitors and others affected by our activities is paramount. Lincolnshire Community Health Services NHS Trust also recognises the importance of the protection of its assets and the premises of which it operates out of, as well as the personal property of staff, service users, and visitors.

#### Responsibilities

Compliance with the policy will be the responsibility of all Lincolnshire Community Health Services NHS Trust managers.

#### Training

Directors, Heads of Service, and Workforce Development are responsible for ensuring that awareness training is available and that staff members access this as appropriate.

#### Dissemination

Website

# Lincolnshire Community Health Services NHS Trust

## Security Policy and Strategy

### Contents

i. Version Control Sheet .....	2
ii. Policy Statement .....	5
1. Introduction .....	7
2. Aims and Objectives .....	7
3. Responsibilities .....	8
3.1. Statutory Responsibilities .....	8
3.2. Chief Executive .....	8
3.3. Director of Workforce and Transformation .....	8
3.4. Directors .....	9
3.5. Clinical Service Managers .....	9
3.6. Managers at all Grades .....	9
3.7. Local Security Management Specialist .....	10
3.8. Staff .....	11
3.9. Health and Safety Committee .....	11
3.10. Quality Scrutiny Group .....	12
4. Security Strategy .....	12
5. Local Arrangements .....	13
5.1. Security Alerts and Advanced Warnings .....	13
5.2. Contractors Working on Trust Premises .....	13
5.3. Staff Lone Workers .....	14
5.4. CCTV .....	14
5.5. The Regulation of Investigatory Powers Act 2000 .....	14
5.6. Bomb Alerts .....	14
5.7. Access and Control .....	14
5.8. Lockdown .....	14
6. Risk Assessment .....	15
7. Developing and Review of Trust-wide Action Plan Following Risk Assessment .....	15
8. Guidance and Training .....	15
8.1. Induction Training .....	15
9. Consultation and Management Review .....	16
10. Monitoring Compliance .....	16
11. Associated Policies and Procedures .....	16
Appendix A .....	17
Appendix B .....	18

# Lincolnshire Community Health Services NHS Trust

## Security Policy and Strategy

### 1. Introduction

Lincolnshire Community Health Services NHS Trust (from here on referred to as 'the Trust') duties and responsibilities to provide a secure environment for its staff, patients and visitors. All employees of the organisation, wherever they work, are responsible for ensuring a secure environment by adherence to this and associated policies and procedures. Patients and visitors using the organisation's services are expected to conduct themselves in a reasonable manner and not adversely affect the security of the healthcare environment.

To achieve these aims:

- We recognise the security, safety, and welfare of our staff, service users, visitors, and others affected by our activities, is paramount.
- We must protect the organisation's staff and assets to ensure the quality of healthcare is not adversely affected.
- We shall comply with legislation and work to raise standards wherever possible.
- We shall be open and transparent about our security performance.
- We shall promote best practice and understanding of statutory responsibilities by effective management systems, communications, training, and use of expert advice.

### 2. Aims and Objectives

The aim of this policy is to ensure that the organisation provides a secure environment for staff, service users, and visitors. The key objectives of the policy are;

- The protection of staff, service users, and visitors,
- The protection of the personal belongings of staff, service users, and visitors,
- The protection of the Trust's property,
- The effective management of violent and aggressive incidents,
- The effective management of non-violent incidents,
- Effective and widely understood procedures for calling for assistance (e.g. Police),
- Reporting of all incidents, including near misses,
- Availability of information regarding crime, and on reducing crime.

### **3. Responsibilities**

#### **3.1. Statutory Responsibilities**

The current Health and Safety requirements, require every employer to provide comprehensive and relevant information to employees on the;

- Risks to their safety and welfare, identified on risk assessments,
- Preventative and protective measures to be implemented,
- Emergency procedures and details of assembly points, and staff affected,
- Risks notified by others, which might affect the organisation's employees.

The Acts also require every employer to provide adequate information, instruction, training, and supervision.

#### **3.2. Chief Executive**

The Chief Executive has the overall statutory responsibility for security management within the Trust. The operational responsibility for security management is delegated to the Director of Workforce and Transformation.

#### **3.3. Director of Workforce and Transformation**

##### **Security Management Director (SMD)**

The NHS Security Management Service, part of NHS Protect was established in April 2003 with statutory responsibility for the management of security within the NHS (Statutory Instrument 3039/2002). These delegated responsibilities are exercised on behalf of the Secretary of State for Health. Under the NHS Standard Contract for 2013/14, General Condition 6.1; *"The Provider must put in place and maintain appropriate Counter Fraud and Security Management Arrangements"*. In accordance with previous NHS Protect requirements, the Security Management Director (SMD) is therefore responsible for ensuring that adequate security management provisions are made within the Trust.

The Security Management Director is responsible for:

- Promoting security at board level and for monitoring and ensuring compliance with the requirements previously set by NHS Protect, and Secretary of State for Health Directions relating to security.
- The promotion and realisation of a pro-security culture throughout the organisation, assisted by the LSMS, who has a legal responsibility for this assistance.

Subject to any contractual and legal restraints, the SMD requires the entirety of the Trust's staff to co-operate with the Local Security Management Specialist, particularly those responsible for human resources, and disclose information which arises in connection with any matters (involving disciplinary matters) which may have implications for the investigation, prevention, or detection of security breaches.



### **3.4. Directors**

Each Director is responsible for the implementation of this policy, for the security of financial and physical resources. These responsibilities include;

- The clear communication of the roles and responsibilities of staff in respect of security management and mandatory training,
- Ensuring that General Managers have clearly defined their responsibilities in respect of security management, as a minimum requirement to ensure that staff members within their service/departments meet the minimum mandatory training requirements.

### **3.5. Clinical Service Managers**

The Clinical Service Managers are responsible for ensuring;

- The implementation of the Trust's Security Policy in their services,
- That risk assessments are undertaken in relation to security management concerns as required, and escalated to the appropriate risk register,
- The allocation of sufficient resources in order to manage the risk(s) identified effectively, in line with the action plan developed,
- Reporting all security related incidents in line with the incident reporting policy.

### **3.6. Managers at all Grades**

The Trust's Service/Department Managers are responsible for ensuring;

- That staff within their service or department have read and understood the Security Policy and Strategy,
- That staff report security related incidents in accordance with the Trust's Incident Reporting Policy,
- That they implement the Trust's Risk Assessment Policy as necessary, within areas of their organisational responsibilities,
- That staff understand their responsibility to identify and assess security risks to service users, visitors, other members of staff, and the Trust's assets in their area of work and escalate these to their Line Manager/General Manager as appropriate,
- The attendance of staff on the appropriate mandatory training for their role/service area,
- Security issues are raised with the Local Security Management Specialist and that any changes identified as a result of a risk assessment or incident, involve the input of the Local Security Management Specialist,
- New employees and agency staff receive initial induction training and specialist training as deemed necessary, to ensure awareness of their responsibilities, in relation to security management.
- Responsibility for assisting the Trust through the provision of guidance, to realise the requirements and guidance previously issued by NHS Protect, relating to security training standards.

### 3.7. Local Security Management Specialist

The Local Security Management Specialist (LSMS) reports directly to the Trust's Director of Workforce & Transformation, Security Management Director. The LSMS is responsible for;

- Assisting the Trust to realise the requirements previously issued by NHS Protect relating to security, including the *Concordat between the Health and Safety Executive and the NHS Counter Fraud and Security Management Service (March 2005)*,
- Undertaking Crime Reduction Risk Surveys of Trust properties and activities, which may place service users, staff, visitors or members of the public, at risk,
- Producing an annual work plan for submission to the Security Management Director, in order to outline security management work for the coming year, and complete a Self-Review Tool relating to the historical NHS Protect security requirements,
- The provision, where necessary, of specialist information, guidance, and training, to assist directors, managers, and staff in the performance of tasks and duties,
- Ensuring the SMD is fully aware of security issues which may affect the Trust, its staff, service users, or the levels of service for which it offers,
- Following referral by the SMD, investigate security incidents in accordance with established practice and legislation and liaising with the Police and other relevant parties, to secure suitable sanction where necessary,
- Act as the Trust's single point of contact for the Police, with regard to security matters, in accordance with the Memorandum of Understanding between the Association of Chief Police Officers (ACPO) and the Crown Prosecution Service (CPS),.
- To undertake investigation of all reported incidents of physical and non-physical assault, defined as the following;
  - Physical assault: "intentional use of force by one person against another, without lawful justification, resulting in physical injury or personal discomfort."
  - Non-physical assault: "the use of inappropriate words or behaviour causing distress and/or constituting harassment."  
(Defined by *NHS CFSMS - Non Physical Assault Explanatory Notes*)

### **3.8. Staff**

All members of staff are responsible for;

- Taking reasonable care for the security of themselves and of all other persons who may be affected by their acts or omissions at work,
- Co-operating fully with the organisation, with regard to any duties or requirements imposed upon the organisation, under any of the relevant statutory provisions,
- Fully utilising all equipment, including personal protective equipment (PPE) provided for their security, in accordance to their Line Manager's instructions,
- Obtaining authority from their Line Manager prior to the removal of property belonging to the Trust, from Trust premises. Failure to seek authority from their Line Manager could result in disciplinary action or criminal proceedings being taken,
- Ensuring that reasonable steps are taken to safeguard the Trust's property whilst in their care,
- Informing their Line Manager/Supervisor of any work situation, which may represent an immediate danger to their security, that of other staff, or to service users and/or their cares,
- Informing their Line Manager/Supervisor of any breach of security or Standing Financial Orders, in accordance with the Incident Reporting Policy,
- Reporting any security incidents or breaches to their immediate Line Manager, in accordance with the Incident Reporting Policy,
- Where working in the frontline, members of staff are required to attend conflict management training as soon as possible following appointment, and subsequent refresher training,
- For the protection and safe-keeping of their private property. Any loss or theft of private property should be reported to their Line Manager, in line with the Incident Reporting Policy,
- Ensuring that whilst on duty, their ID card is worn. Any loss of an ID card should be reported in line with the Incident Reporting Policy.

### **3.9. Health and Safety Committee**

The Health and Safety Committee will serve as the forum for the Trust to review the measures taken by the Trust to ensure the health and safety at work of employees, service users, visitors and contractors on site.

The Committee will oversee the implementation of the Trust's Security Policy and Strategy.

The Committee will promote co-operation between employees and managers, in instigating, developing, and carrying out measures to ensure the health and safety at work of employees.

The Committee will review/receive:

- Collation of risk assessment reports relating to security management.
- Quarterly reports of security management activity.
- Aggregated data relating to incidents, serious untoward incidents, complaints, and claims relating to security management and broader health and safety issues.
- Updated reports from the LSMS in relation to the progress of cases currently under their management.

### 3.10. Quality Scrutiny Group

The Quality Scrutiny Group will ensure that there are robust processes in place with the effective management of clinical and corporate risk to underpin the delivery of the Trust's principal objectives.

## 4. Security Strategy

The Trust's Security Strategy is the combination of the identification of the issues and challenges it currently faces, or may face in the future, with the annual work-plan developed by the LSMS. This work-plan sets out how the Trust will deliver a safe and secure environment, combat any issues and challenges it faces, as well as how it will implement any changes to security arrangements in the Trust. This work-plan takes in to account the previous NHS Protect standards, sets out the Trust's actions for delivery, and reaffirms its commitment to providing a safe and secure environment.

The Trust's Security Strategy will aim to ensure that we can;

- Create and maintain a pro-security culture among staff, independent contractors, and the public,
- Protect staff, service users, and visitors,
- Protect the personal belongings of staff, service users, and visitors,
- Protect Trust property; making our services more resilient and less vulnerable to attack,
- Manage appropriately the risks of violence and aggression,
- Develop reporting frameworks and systems for security reports,
- Prevent crime and increase the awareness of criminal activity,
- Ensure that wherever possible, prosecutions are progressed against offenders, and appropriate outcomes are sought.

The Security Strategy frames the role of security resources, processes, and governance, to best support the work of the Trust and the values that we contribute to.

The Department of Health outlines the responsibilities of NHS bodies to manage security, provide a safe and secure environment for staff, service users, and visitors. The standards that comprise the following four areas are:

- **Strategic Governance** sets out the standards for organisational governance, embedding anti-crime measures at all levels throughout the Trust.
- **Inform and Involve** raises awareness of crime risks against the NHS and staff, engaging the public and stakeholders to raise this awareness and understanding of the consequences of crime against the NHS.
- **Prevent and Deter** sets out the requirements to deter those who wish to commit crimes against the NHS or the staff who work within it, and ensuring that opportunities to commit crime are minimised.
- **Hold to Account** sets out the requirement and commitment to detecting and investigating crime, together with the prosecution of those who commit crimes against the NHS or the staff that work for and within it.

## **5. Local Arrangements**

Following the identification of a security incident/breach:

- The staff member must immediately report the incident to their Line Manager or Nominated Deputy in accordance with the Trust's Incident Reporting Policy.
- The staff member involved in the incident must ensure the submission of a completed Incident Report Form by means of DATIX immediately (i.e. within one working day) for each relevant incident, in accordance with the Trust's Incident Reporting Policy.
- The Local Security Management Specialist to be informed of security/incident or breach as soon as practicable. The DATIX system will automatically generate a notification to the LSMS if correctly categorised when the incident is entered on to the DATIX system.
- Line Manager to complete an Incident Investigation Form within 5 working days, and forward to the appropriate Risk Management Team, in accordance with the Trust's Incident Reporting Policy.

### **5.1. Security Alerts and Advanced Warnings**

There will be occasions when the LSMS will need to put out security alerts to all staff, or to certain departments/teams. Issues that may need to be reported include;

- Major theft of equipment, or on-going theft of equipment,
- Child abduction,
- Arrests,
- Court appearances, the outcomes, and prior dates of appearances,
- Violent patient alerts.

### **5.2. Contractors Working on Trust Premises**

A copy of the Trust's Security Policy and Strategy will be made available to all contractors working on Trust premises employing organisation department.

All contractors will be expected to comply with the Trust's Security Policy and Strategy at all times, raising any concerns with the employing organisation department.

All contractors, on appointment, will be given the name of the designated organisation officer who will act as a liaison person between the contractor and the Trust, and/or supervisor of the contract.

All equipment brought on to site by contractors will be their own responsibility and all security measures must be taken to safeguard all equipment which could cause harm if in the wrong hands. This must be agreed prior to commencement of works.

### **5.3. Staff Lone Workers**

The Trust has a policy incorporating the various elements surrounding lone working. Please see the *Lone Worker, and Violence and Aggression at Work Policy* for further guidance regarding the security of lone workers. All managers who have lone workers must ensure that staff have knowledge and understanding of the relevant parts of the policy, and are provided adequate information and training relating to lone working.

### **5.4. CCTV**

The Trust employs the use of CCTV to aid in the security of staff members, service users, visitors, and Trust assets and property. Guidance regarding CCTV surveillance is contained within the Trust's CCTV Policy; *CCTV Policy* (P\_HS\_13).

### **5.5. The Regulation of Investigatory Powers Act 2000**

*The Regulation of Investigatory Powers Act 2000* (RIPA) provides for, and regulates, the use of a range of investigative powers, by a variety of public authorities.

### **5.6. Bomb Alerts**

Guidance relating to bomb alerts and suspicious parcels is contained within the Trust's Emergency Preparedness Portfolio.

### **5.7. Access and Control**

It is essential that access control measures are maintained at all of the Trust's sites. The working practice of the Trust must inevitably provide for close interaction between staff, service users and visitors. However, wherever practicable, access to clinical and non-clinical staff areas should be severely restricted. In addition to this, all services will be made secure outside of normal working hours.

### **5.8. Lockdown**

A lockdown profile is being developed by the Trust's Emergency Planning Lead and LSMS as part of the Emergency Planning and Business Continuity requirements. Each site manager is responsible for the development and implementation of local procedures for lockdown. Additional support and training is provided by the Emergency Planning Lead and LSMS in order to accomplish this aim.

## **6. Risk Assessment**

An essential element in effective implementation of this policy is the application of a robust risk assessment process and the introduction of adequate preventative measures.

Risk assessments will be undertaken in compliance with the Trust's risk assessment policy, *Health and Safety Risk Assessment (P\_HS\_07)*, which reflects the Health and Safety Executive's five steps approach. The Trust's *Risk Management Strategy (P\_RM\_02)*, clearly identifies the risk identification and management process which equally applies to security risk.

## **7. Developing and Review of Trust-wide Action Plan Following Risk Assessment**

Action plans identified as a result of a formal risk assessment will be reviewed in line with the requirements of the Trust's Risk Management Strategy. Significant risks identified in relation to security management will be presented to the Health and Safety Committee together with information on incidents, claims, and complaints, where the identification of trends will be supported and included within an overarching Trust-wide action plan. This will take the form of the NHS Protect annual Self Review Tool for Security Management.

## **8. Guidance and Training**

The Trust is committed to providing information, guidance, and training on security, safety, and welfare to all members of staff to enable them to carry out their work without risk to either themselves or others. A range of security information is available to all staff, from the following sources;

- The Local Security Management Specialist,
- Health and Safety Advisor,
- Clinical Governance Managers,
- Education and Workforce Development Department.

### **8.1. Induction Training**

All new staff joining the Trust will be provided basic security induction training as soon as possible after their commencement of employment. The training provided will include an overview of the Trust's security management arrangements, such as reporting procedures. All staff will be made aware of their security and safety responsibilities, and in addition, will receive mandatory update training. Conflict resolution training is a mandatory requirement for all staff.

## 9. Consultation and Management Review

Current Health and Safety requirements require employers to consult staff and employee staff representatives concerning;

- The introduction of any workplace measure, which may affect security and safety substantially,
- Any security or safety information required to be supplied to employees,
- The planning and organisation of any security or safety training,
- Any security or safety consequences of introducing new technology.

The Trust operates a formal staff consultation process. Security Management will be a standing agenda item for the Health and Safety Committee.

## 10. Monitoring Compliance

The Health and Safety Committee will receive quarterly reports and an annual report from the Locals Security Management Specialist, identifying security management activity and performance against the agreed annual work plan.

## 11. Associated Policies and Procedures

This general policy is supported by a number of policies and procedures covering specific areas and types of incident. These documents should be read in conjunction with this policy, and are listed below.

Corporate Health and Safety Policy	(P_HS_02)
Health and Safety Risk Assessment Policy	(P_HS_07)
CCTV Policy (LCHS Owned Sites)	(P_HS_13)
Lone Worker, and Violence and Aggression at Work Policy	(P_HS_18)
Incident Reporting Policy and Procedure	(P_RM_01)
Risk Management Strategy	(P_RM_02)



## Appendix A

### NHSLA Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individuals/group /committee	Frequency of monitoring /audit	Responsible individuals / group / committee (multidisciplinary) for review of results	Responsible individuals / group / committee for development of action plan	Responsible individuals / group / committee for monitoring of action plan
Security incident & Crime Reduction Survey Reports	Report to Committee	Local Security Management Specialist	Quarterly	LCHS Health and Safety Committee	General Managers	LCHS Health and Safety Committee
Training	Staff training records audit	Workforce Development	Annual	LCHS Health and Safety Committee	Workforce Development	LCHS Health and Safety Committee
Review Datix Reports	Report to Committee	Clinical Governance Managers & Local Security Management Specialist	Quarterly	LCHS Health and Safety Committee	Clinical Governance Managers	LCHS Health and Safety Committee
Review Policy	Policy to Committee	Local Security Management Specialist	2 years, or due to significant change in core standards	LCHS Health and Safety Committee	Local Security Management Specialist	LCHS Health and Safety Committee

## Appendix B

### Equality Analysis

**Title: Security Policy and Strategy**

**Relevant line in:**

**What are the intended outcomes of this work?** To demonstrate the Trusts commitment to providing a secure environment and protection for staff, patients and visitors. To identify the responsibilities of Trust management and individuals in order to identify and minimise the risk and provide effective management of violent and aggressive incidents.

**Who will be affected?** Directly affects Directors, Managers and all Members of Staff. Outcomes will affect patients, carers and visitors.

### Evidence

**What evidence have you considered?** Management of Health and Safety at Work Regulations 1999, Health and Safety at Work etc. Act 1974, Guidance previously issued by NHS Protect (Security Management)

**Disability** policy applies equally to all persons

**Sex** policy applies to sexes equally

**Race** policy applies to all races equally

**Age** policy applies equally to all persons

**Gender reassignment (including transgender)** policy applies equally to all persons

**Sexual orientation** policy applies equally to all persons

**Religion or belief** policy applies equally to all persons

**Pregnancy and maternity** policy applies equally to all persons

**Carers** policy applies equally to all persons

**Other identified groups** policy applies equally to all other persons

## Engagement and involvement

Was this work subject to the requirements of the Equality Act and the NHS Act 2006 (Duty to involve)? **No**

How have you engaged stakeholders in gathering evidence or testing the evidence available?  
**Health and Safety, Fire and Security Committee**

How have you engaged stakeholders in testing the policy or programme proposals?  
**No**

For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:

## Summary of Analysis

**Eliminate discrimination, harassment and victimisation**

N/A

**Advance equality of opportunity**

N/A

**Promote good relations between groups**

N/A

## What is the overall impact?

The impact will be to provide effective recording, monitoring and management of security related incidents and identified risks.

## Addressing the impact on equalities

N/A

## Action planning for improvement

Policy to be ratified by the Health and Safety Committee

Policy to be approved by the Board

Policy to be updated on the website policies section

Policy to be promoted to staff via training

Monitoring to take place as detailed in policy

Policy reviewed using NHSLA guidelines

**For the record**

**Name of person who carried out this assessment:** Carl Kisby, LSMS

**Date assessment completed:** March 2016

**Name of responsible Director/Director General:** Maz Fosh

**Date assessment was signed:**

**Action plan**

Category	Actions	Target date	Person responsible and their Directorate
<b>Involvement and consultation</b>	Health and Safety Committee consulted	10/10/2013	
<b>Data collection and evidencing</b>			
<b>Analysis of evidence and assessment</b>			
<b>Monitoring, evaluating and reviewing</b>	As per Policy		
<b>Transparency (including publication)</b>			