SECURITY MANAGEMENT POLICY

1. INTRODUCTION

1.1 The intention of the security policy is to ensure that the delivery of healthcare takes place in a safe and secure environment, free from the risks of crime which may arise when providing a public service.

1.2 NHS Protect has overall responsibility for all policy and operational matters relating to the management of security in the NHS. NHS Protect is a business stream of the NHS Business Services Authority, a special health authority.

2. POLICY STATEMENT

2.1 The purpose of the security policy is to ensure patients, staff and visitors should be confident they are safe, their personal property is secure and the Trust's buildings and equipment are protected.

2.2 To achieve the intended purpose outlined in section 1.1 the specific aims and objectives of this policy are to have clear processes and procedures in place for;

- The identification of security risks
- The purpose of risk assessment and risk reduction
- Identified risks to feed into the corporate risk register and assurance frameworks
- Ensuring all risks of the Trust are managed properly at all levels.
- Where individuals commit crimes against the Trust and its staff appropriate sanctions are imposed.

3. DEFINITIONS

3.1 Definitions of any key terms used:

No definitions stated.

4. STATUTORY RESPONSIBILITIES

4.1 NHS Protect

NHS Protect was established in April 2003 (Formerly called NHS Security Management Service) with statutory responsibility for the management of security within the NHS. Historically NHS bodies were required to put arrangements in place for security management under the Secretary of State Directions. However since 2012 provisions introduced under the Health and Social Care Act 2012 means that such arrangements will now be set out in standard commissioning contracts rather than in Secretary of State Directions. The clauses relating to security in the commissioning contracts need to be applied.

4.2 Health and Safety Executive

The Health and Safety Executive (HSE) are responsible for ensuring that risks to people's health and safety from work based activities are properly controlled. The HSE role is to enforce health and safety legislation in the healthcare sector and employers have a duty to ensure as far as is reasonably practicable, the health, safety and welfare of employees at work and of non employees affected by our work activity.

4.2.1 Health and Safety at Work Act 1974

The Trust has responsibilities under the Health and Safety at Work Act 1974 (HSWA), particularly in relation to employers, to ensure as far as is reasonably practicable, the

health, safety and welfare of employees at work. The Trust's Health and Safety Policy sets out how the organisation intends to fulfil its responsibility under the HSWA.

4.2.2 The Management of Health and Safety at Work Regulations 1999

These Regulations require employers to assess risks to employees and non employees and make arrangements for effective planning, organisation, control, monitoring and review of health and safety risks.

Department managers with the assistance of the Security Advisor will carry out security related risk assessments of premises, assets and people for all wards and departments. The Environmental Compliance Team have full procedures relating to this process which in summary is as follows:

- Risk assessments will be completed and reviewed within agreed times scales dependent on the level of risk or where alterations have been made.
- The Security Advisor will summarise the findings on a security risk assessment form and agree with the manager any recommendations for action.
- The department manager is responsible for completing the risk assessment action sheets with person responsible and action by date and returning it to the Security Advisor.
- Risk assessments and action plans will be recorded on the security risk assessment database and monitored for compliance by the Health and Safety Management Committee.

4.3 Healthcare Commission

The Healthcare Commission (CQC) has a statutory responsibility for assessing, inspecting and reporting on the performance of both NHS and independent healthcare organisations in England to ensure that they are providing the highest standards of care. In march 2005 the Commission introduced an annual health check. The check is a national assessment of performance against government standards. Core standards C20a requires that health services are delivered in environments which are a safe and secure environment which protects patients, staff, visitors and their property, and the physical assets of the Trust. The Trust has a number of security measures and associated polices are in place to ensure core standard C20a is met.

4.4 NHS Litigation Authority

The NHS Litigation Authority (NHSLA) has a statutory responsibility for the handling of negligence claims made against NHS bodies in England. NHSLA have risk management standards in place for acute, mental health, ambulance and primary care trust, as well as foundation trusts. Within management standard 4, Safe Environment - there are criteria which cover the management of risks associated with the physical security of premises and assets and prevention and management of violence and aggression. The Trust has effective risk management measure in place that meets NHSLA's minimum requirements.

5 ROLES AND RESPONSIBILITIES

5.1 All Staff

All staff have responsibility to ensure the successful delivery of this policy to enable it to fulfil its intended purpose:

- Must comply with all processes and procedures link to the Trust Security Policy.
- Must report all security related incidents as per the Trusts Incident reporting procedures.
- Must always wear their identity badges and ensure it is visibly displayed whenever they are on Trust property.

5.2 Managers

Some staff and managers with more specific roles have greater responsibility to fulfil the requirements of this policy. This includes managers who are responsible for the safety of patients, staff and the security of property and assets.

- Must ensure all incidents of a security nature are reported in line with the Trust incidents reporting procedures.
- Investigate security related incidents in liaison with the Trusts Security Advisor when applicable.
- Ensure staff are aware of security related policies.
- Uphold good security housekeeping in respect of keys, hazardous materials and confidential information within directorates.
- Ensure security related risk assessments are undertaken and reviewed within agreed times scales and any identified actions implemented.

5.3 Security Management Director

The nominated Security Management Director (SMD) is responsible for ensuring that adequate security management provision is made available within the Trust. Final responsibility remains with the SMD regardless of weather or not the Local Security Management Specialist (LSMS) and/or security staff are directly employed by the Trust, or provided by an external company. The nominated SMD is the Director of Finance.

- Must drive forward the security management needs of the Trust, in particular concentrating on the priority areas of work.
- Represent security management work at Executive Board Level to ensure it is discussed at the highest level, enabling compliance with NHS Protect standards.
- Responsible for ensuring affective systems are in place for risk reporting, assessments and management processes.
- Responsible for the nomination and appointment of an LSMS and continues liaison with the LSMS to ensure security management work is being undertaken to the highest standards within the delegated resources.

5.4 Local Security Management Specialist

The Trust has a nominated LSMS that has undergone professional accreditation training to ensure that the highest standards are applied to security management work locally. The Trust Security Advisor is the appointed LSMS within the organisation.

- Carry out work in relation to NHS Protects standards to ensure compliance.
- Produce an annual report and work plan to outline security management work for the coming year.
- Assist local managers in carrying out security related risk assessments.
- Report to the Health and Safety Management Committee on compliance with the Trust risk management process.
- Identifying and reporting security risks and system weaknesses.
- Liaison with Police and other agencies in respect to security incidents and security management work.
- Provide advice, support and assistance in upholding all operational arrangements that effects security.
- Assist managers with the investigation of security related incidents and keep proper records.
- Provide support for staff involved in security incidents.
- Provide Conflict Resolution Training (CRT) for frontline staff in line with the national syllabus for CRT.

5.5 Head of Environmental Compliance

- Advise and inform the Security Management Director to enable the security management needs of the Trust to be driven forward, in particular concentrating on the priority areas of work

- Represent security management work at Facilities Board and Compliance Committee Level to ensure it is discussed at the high level within the Trust, enabling compliance with NHS Protect standards.

- Responsible for advising the Security Management Director to enable affective systems to be in place for risk reporting, assessments and management processes.

- Responsible for the line management of the LSMS and close liaison with the LSMS to ensure security management work is being undertaken to the highest standards within the delegated resources.

- Provide advice, support and assistance in upholding all operational arrangements that effects security.

- Assist managers and the LSMS with the investigation of security related incidents and keep proper records.

- Ensure that regular reports are given to the Health and Safety Management Committee and the Representatives Committee on compliance with the Trust risk management and security process.

6 Roles and Responsibilities of Boards and Committees

6.1 Trust Board

The SMD is responsible for ensuring the Chief Executive and the Board are given assurance that security management processes, security operations, procedures and polices being effectively introduced and implemented across the Trust.

6.2 Health and Safety Management (HSMC) and Representatives (HSRC) Committees

6.2.1 The Health and Safety Management Committee is responsible for ensuring the appropriate health and safety process are in place across all divisions to protect and promote the safety and well being of staff in the work place. A key function of the committee is to agree the Trusts security strategy and to receive action reports on security related issues. For further information on the role and responsibilities see the Health and Safety Management Committee Terms of Reference.

6.2.1 The Health and Safety Representatives Committee is to ensure so far as is reasonably practicable, the health, safety and welfare at work of all employees, visitor and patients by promoting and co-operation between Chesterfield Royal Hospital NHS Foundation Trust, managers and employees at all levels. For further information on the role and responsibilities see the Health and Safety Representatives Committee Terms of Reference.

6.3 Audit Committee

The Audit Committee is responsible for providing an independent and objective overview of all risks within the Trust, This includes overseeing internal and external audit services, reviewing financial systems and monitoring compliance with standing orders, standing financial instructions, asset losses and compensation, as well as giving assurances on all other Trust risk.

6.4 Security Group

The group operates at a sub strategic level and is responsible for reviewing all matters relating to security within the Trust and bringing issues to resolution wherever possible. The Security Group reports to the Health & Safety Management and Representatives Committee. Where matters being dealt with by the working group cannot be resolved by the group, they should be escalated to the Health & Safety Management Committee.

7 Risk Assessment Process

7.1 The Trusts Risk Management Policy sets out the policy and procedures to be followed for managing clinical and non clinical risk. In additional to this the Environmental Compliance Team has specific risk assessment procedures in place. For further information see:

- Risk Management Policy
- Environmental Compliance Team Risk Assessment Procedures

7.2 All new building and major refurbishment projects must include funding for the appropriate level of security. It is the designated project manager's responsibility to consult with the security Advisor to ensure appropriate security measures are included.

8 Security Management Priority Areas

8.1 Strategy

NHS Protect document 'a professional approach to managing security in the NHS (2003) outlines the NHS Protects security management strategy in the NHS in England.

8.1.1 Creating a Pro-Security Culture

The Trust aims to create a pro security culture where responsibilities for security are accepted by all and breeches in security will not be tolerated. The Trust uses a number of measures to achieve a pro security culture which includes:

- Training
- Media
- Incident investigations
- Crime awareness events
- Meetings

8.1.2 Deterrence

Deterring those who may be in mind to breech security, using publicity to raise awareness of what consequences their intended actions could be personally and to the NHS.

8.1.3 Prevention

Preventing security incidents and breeches from occurring, wherever possible or minimising the risk of them occurring, learning from operational experience and sharing best practice. The Trust uses a number of measures to ensure appropriate preventative measures are in place. These measures include:

- Risk Assessment
- On site Security Team
- Security related policies and procedures
- Training
- Incident investigation
- Audits
- Security Systems
- Liaison with internal stakeholders and external agencies

8.1.4 Detecting

Detecting security incidents or breeches and ensuring these are reported across the Trust. The Trust is committed to reducing healthcare risk in order to ensure patients, staff and visitors feel safe, and consider the reporting and investigation of incidents to be an important factor in minimising this risk. The trust use a number of measures to detect incidents and breeches which include, but not restricted to:

- Incident Reporting Policy
- Routine security patrols
- Security systems e.g. CCTV, Intruder alarms and access control
- Lone worker devices

8.1.5 Investigating

Investigating security incidents in a fair, objective and professional manner, to ensure those responsible for such incidents are held to account for their actions. For further information on investigating incidents see the Trusts Incident Reporting Policy. Where incidents are reported to the police the trust is committed to assisting the police with their investigations.

8.1.6 Applying Sanctions

Applying a wide range of sanctions against those responsible for security incidents involving a combination of disciplinary, civil and criminal action as appropriate. The Trust will investigate all reported security incidents and were appropriate seek to apply the most suitable sanction. For further information and guidance on sanctions see:

- Managing violence and aggression Policy.
- Withholding Treatment and Exclusion from Premises of Violent and Aggressive Patients Policy
- Personnel Disciplinary Procedures

Where sanctions are applied to those who commit crimes against the trust, the trust will seek to publicise these through internal and external communication channels and media.

8.2 Reporting

It is the responsibility of all staff to report security incidents whether suspect or real. Incident reporting is an important function to identifying patterns of criminal activity and number and type of security related incidents occurring. It allows incident to be investigated and recommendations to be made to prevent a reoccurrence. Comprehensive reporting of incidents will provide an accurate picture of crime levels across the Trust. The Trusts ability is strengthened by fast, efficient and detailed reporting. For further information on reporting incidents see:

- Trust Incident Reporting Policy
- Security Management Policy - Appendix 1.

8.3 Priority Areas

NHS Protect have highlighted specific areas of work which forms the focus for security management work across the NHS. The Trusts priority areas of work are highlighted below were the main security management work will be focused.

8.3.1 Tackling Violence and Aggression

The trust has a number of separate polices in place which details how violence and aggression will be tackled across the trust. In addition to policy the trust also delivers training in Conflict Resolution and Clinical Holding to frontline staff. This ensures the trust meets with health and safety legislation. For further information and guidance on tackling violence and aggression see:

- Managing Violence and Aggression Policy
- Withholding Treatment and Exclusion from Premises of Violent and Aggressive Patients
- Lone Working Policy
- Incident Reporting Policy

The above policies set the foundation on how violence and aggression will be tackled across the trust and provide staff with information on what action should be taken when a violent or aggressive incident occurs and the support available. The policies cover both clinical and non clinical violence and aggression. The trust Security Advisor has an overview of reported incidents to ensure violence and aggression is managed appropriately across the trust and to ensure a range of sanctions are applied to those responsible where appropriate.

8.3.2 Security of Property and Assets

The security of property and assets is assessed during risk assessments, refurbishment projects and new builds to ensure the appropriate level of security is in place to protect from loss and damage. Where weaknesses are identified action plans are produced to improve security. For further information and guidance on security of property see:

- Patient Property Policy
- Risk Management Policy
- Incident Reporting Policy
- Security Management Policy - Appendix 1

8.3.3 Security of Maternity and Paediatrics

Each maternity and paediatric unit has undergone risk assessment to ensure appropriate security control measures are in place. These measures include access control, CCTV, door alarms and baby tagging systems. In addition to these measures the Trust has a number of polices in place to protect maternity and paediatrics. For further information and guidance see:

- Abduction of Child/Baby Policy
- Schedule One Offender Policy
- Staff Identification Policy
- Security Management Policy – Appendix 1

8.3.4 Security of Drugs, Prescription Forms and Hazardous Materials

The trust has separate polices in place for the security of drugs and hazardous material. Each area has been risk assessed to ensure appropriate security is in place. For further information and guidance on security of drugs, prescriptions and hazardous materials see:

- Medicine Management Policy
- Risk Management Policy

8.4.4 Major Incidents and Contingency Planning.

The Civil Contingencies Act 2004 provides s statutory and regulatory framework for resilience in the UK. The act delivers a single framework for civil protection and sets out clear expectations and responsibilities for front-line responders at the local level, to ensure that they are prepared to deal effectively with the full range of emergencies from localised incidents to full scale emergencies. Outlined in the Act, Category 1 responders are those organisations at the core of emergency response that includes acute foundation trusts.

The trust has a number of policies in place that detail the role and responsibilities of security in a localised incident or full scale emergency. For further information and guidance see:

- Major Incident Policy
- CBRN Incident Policy
- Business Continuity Plan

9 Auditable Standards and Key Performance Indicators

9.1 Internal

Section 10 of this policy (Monitoring) details the governance arrangements on how the trust plan to monitor the effectiveness of this policy in managing security across the trust.

9.2 External

9.2.1 NHS Litigation Authority (NHSLA)

The NHSLA has an active risk management programme to help raise standards of care and reduce the number of incidents that lead to claims against the NHS. The effective and proper management of security risks outlined in this policy should demonstrate to the NHSLA that security risks are managed properly within the trust.

9.2.2 Health and Safety Executive

The Management of Health and Safety Regulations 1999 require employers to have arrangements in place

10. MONITORING

10.1 This section identifies how the organisation plans to monitor compliance with the policy. monitoring arrangements for compliance, i.e. audit, review etc.;

Policy element	**Content to be monitored**	**Monitoring process**
Risk assessments	Process for completing risk assessments of physical security and assets and follow-up of action plans	Via Health & Safety Management Committee detailing the number of: • Risk assessment completed • Outstanding risk assessments to be completed • Risk assessments where action sheets are not completed and returned to Advisor. • Annual completion of NHS Protects Organisational Crime Profile and Self Review Tool. Any deficits arising will be monitored by HSMC until completed and where relevant identified as an organisational security risk.
Security incidents and sanctions	Process for recording and reporting of security incidents, monitoring the application of sanctions.	All reported security incidents are recorded onto the trusts incident reporting system (Datix). The following reports are to be produced: • Bi monthly security incident data to the health & Safety Management Committee. • Annual Security Report that is currently part of the Environmental Compliance

		Report • Special reports in relation to any significant events. • Annual Violence against staff statistics submitted to NHS Protect. • Annual completion of NHS Protects Organisational Crime Profile and Self Review Tool.
NHS Protects Security Standards	Process for monitoring compliance with NHS Protects standards.	• Annual completion of NHS Protects Organisational Crime Profile and Self Review Tool. • Planned assessments undertaken by NHS Protect as part of their quality assurance programme.

11 KEYWORDS

11.1 Security, Violence and Aggression, Risk Assessment, NHS Protect, Police, Offensive Weapons.

12 REFERENCES

12.1
- NHS Protect, A Professional Approach to managing Security in the NHS (December 2003)
- NHS Protect, Standard for Providers 2013/14
- The Management of Health and Safety at Work Regulations (1999) ISBN0110856252
- The Health and Safety at Work Act (1974)

13 RELATED POLICIES

Reference should be made to the following complimentary CRHFT policies. The security management policy should be considered in conjunction with the other relevant policies and guidance listed below. All polices are available on the staff intranet.

- Lone working policy (OP2.6)
- Staff identification policy (OP2.1)
- Emergency evacuation policy (OP3.2)
- Abduction of a child or baby (OP3.9)
- Missing patient policy (OP1.10)
- Bomb threat policy (OP3.5)
- Harassment at work policy (PP15)
- Incident reporting policy (OP2.3)
- Withhold treatment and exclusion from premises of violent and abusive patients (OP2.22)
- Managing violence and aggression policy (OP1.15)
- Patient property policy (FP31)
- Environmental Compliance Policy
- Various procedures underpin and support the polices referred to (see appendices)

14 APPENDICES

- Appendix 1 - Generic security procedures
- Appendix 2 - Access control application form
- Appendix 3 - Key request form
- Appendix 4 - Procedures for the removal of offensive weapons

Date ratified:	Hospital Leadership Team – February 2015
First issued:	April 1999
Date issued:	February 2015
Review date:	February 2017
For review by:	Security Advisor
Director responsible:	Director of Finance

GENERIC SECURITY PROCEDURES

1. Incident Reporting

1.1 It is the responsibility of all staff to report all security incidents (suspected or real). Incident reporting is important to identifying patterns of criminal activity. It allows investigation and recommendations to be made to prevent a reoccurrence. Comprehensive reporting of incidents provides an accurate picture of the levels of crime throughout the organisation. The organisation's ability to fight crime is strengthened by fast, efficient and detailed reporting. (Read with the Trust's Incident Reporting Policy).

1.2 Procedure

- All incidents of a security nature must be reported to Security on ext 3634 or bleep 634. Alternatively the Security Advisor can be contacted in normal working hours on ext 3636 or bleep 636.
- In an emergency call the Police direct on 999, or for an emergency response from the Security call ext 7777.
- Reports to include all available information, for example, location, time, persons involved, items missing, injuries and Police details.
- A Datix incident report must be completed as soon as possible after the incident.
- All confirmed incidents involving assault (where the offender has mental capacity), theft, burglary and robbery should be reported to the Police. If any doubt exists, contact the Security Advisor for advice. All Police attendances on Trust property is to be reported to the Security Advisor - to enable effective management of any later actions that need taking. The Local Police contact number for non emergencies is 101.
- This reporting procedure should be followed 24 hours a day.

2 Access Control

2.1 The Trust user's various systems to control access throughout the premises. These include electronic access control systems, combination locks and keys. The staff identification card has a dual role. It gives relevant staff access to areas with controlled doors. It also provides staff with identification of employment. (Read with the Trust's Staff Identification Policy).

2.2 Staff requiring access to controlled areas must:

- Complete an Access Control Application Form. See appendix 2 – access control application form.
- The Divisional Manager responsible for the area/s that access is required must sign to approve the application.
- Send the form to Environmental Compliance Department for access to be granted.

2.3 Loss of identification card:

- Immediately report the loss to either, Security on 3634, Security Advisor on 3636 or Environmental Compliance Administration Co-ordinator on 3431. This will ensure any lost cards are inhibited on the access control system.

2.4 Interference – Abuse of system:

- No access control doors should be intentionally damaged or interfered with. This includes the door, door closer, reader unit and break glass.
- No access control door is to be wedged open.

- Staff identification cards are only valid for the named member of staff. The sharing of identify cards for access purposes is strictly prohibited.
- Any member of staff found to be interfering with the system may be subject to disciplinary proceeding under the Trusts Disciplinary Policy

2.5 Tailgating:

- The Trust has a strict NO TAILGATING policy. Staff with access to sensitive areas must ensure that no unauthorised person/s gain entry through tailgating (that is following them in or the staff member holding the door open for them).

2.6 Combination Locks

- Combination lock codes should be changed every 6 months. It is the manager's responsibility to action the change of codes. This can be done by calling Estates Help Desk on extension 3307.
-

2.7 Issue of keys:

- Members of staff who require being issued keys must have approval from their divisional approved manager. A key request form must be completed and returned to the Building Team Leader (Estates Department). See appendix 3 - Key Request Form.

2.8 Staff finishing employment:

- Heads or department or managers have responsibility for ensuring return of identification cards to the Security Advisor when a member of staff leaves the trust's employment. This is vital to ensure the integrity of the access control system.
- Heads or department or managers have responsibility for ensuring return of all keys to either the division approved manager, Building Team Leader or Security Advisor.

3 Security Services

3.1 The trusts has an on site security service that operates 24 hours a day 356 days a year. The service undertakes regular security patrols of the hospital buildings and car parks and monitors various security systems. The team can be contacted on extension 3634, bleep 634 or in an emergency on extension 7777.

3.2 The Security Service also provide the following:

- Attend security related incidents such as theft, abuse, assault and burglary. They will assist staff to deal with, and resolve security related incidents.
- A cash escort service.
- Lone worker checks. If any member of staff works alone, in an area not covered by a lone worker alert system, security staff can be contacted on ext 3634 and regular checks of the area will be made.
- An escort service for patients and staff.

4 Crime Prevention Procedures

4.1

- All personal valuables must be secured or kept on the person, and personal property must not be left unattended.
- All rooms/offices must be locked when left unattended, with ground floor windows closed and no items of value left on display.
- At night all rooms must be locked with lights turned off, except security lighting, with window blind closed.
- Always lock your vehicle and ensure your windows are closed. Do not leave items on show; secure them in the boot of your vehicle.

5 Patient Property

5.1 Staff should familiarise themselves with the Patient Property Financial Procedures

which details the procedures to be followed when handling patient property, but the following rules must also apply:

- Patients to be advised to keep the least amount of money and valuables in bedside lockers. The Trust is not responsible for any cash or personal property not handed in for safekeeping.
- Patient property handed in for safekeeping must be done as soon as practicable, to prevent theft or loss. Two members of staff need to be present when taking property from an unconscious patient, or from a patient who has died.
- Patient Property Financial Procedures must be strictly adhered to at all times.

6 Personal Security

6.1 While it is the responsibility of the Security Service to provide a safe and secure environment, it is the responsibility of all staff on hospital property to take reasonable measures to ensure their personal security. When moving around the hospital staff should note the following advice:

6.2
- Try to be familiar with your surroundings and aware of other people.
- Try to avoid isolated and poorly lit areas.
- Report suspicious behaviour on ext 3634, or for an emergency response from security call ext 7777.
- On discovering suspicious or criminal activity, tell (or get a colleague to tell) security on ext 7777. Then if you feel able and suitably trained, question the individual(s) in a friendly and positive manner (i.e. “can I help you?”). Security Staff will, if appropriate, ensure the Police are contacted and a security response is directed to the area urgently. Security staff will only try to detain by agreement and are not to use force in any way. If the individual(s) become argumentative or aggressive, they are to back-off from the situation. They can either follow them at a discreet distance, until off hospital property (they are not to follow them once off Hospital premises), or wait in or around the area until the Police arrive to make an arrest. Security staff should ensure all staff in the immediate area is made aware of the situation.
- If working late, tell security on ext 3634.
- If subjected to threatening or abusive behaviour or language, stay calm, avoid raising your voice and using aggressive body language, (such as finger wagging). Call for help from colleagues or Security on ext 3634, or if an emergency response is needed, call ext 7777.

For further advice and guidance on managing violence and aggression and lone working please see related policies.

7 Building Security

7.1 The Security Advisor and Estates department in liaison with other divisions, will carryout risk assessments to identify shortfalls in the existing buildings (external and internal areas), which affect the overall security of the hospital.

7.2 All new construction and modernisation projects should include funding for the appropriate levels of security.

7.3 Divisions are to develop and implement procedures (working with the Security Adviser) for each type of premise, such as ward, department, health clinics and mobile units:

7.4
- External areas should have adequate physical security measures: lighting, fencing, gates etc.
- Where appropriate CCTV to be considered and installed. Its use must comply

with the Human Rights Legislation and Data Protection Acts.

- Car parks should have suitable lighting and physical security systems. It is the responsibility of staff to place valuables left in their car, out of sight.
- All members of staff have responsibility for internal security.
- A procedure for receiving and managing visitors should be developed for individual sites.
- All premises are to have a risk assessment for physical security. The findings of the risk assessments are to be recorded using the Trust risk assessment forms available in the Trust's Health and Safety Policies, Risk Assessment Code of Practice. The Security Advisor will assist managers carrying out risk assessments and prioritising action plans. Where significant resource requirements are identified these are to be included in the directorate risk registers. Department risk assessments are to be reviewed annually or bi-annually dependant on risk with the Security Advisor.
- The Security Advisor is responsible for ensuring the quality of risk assessments and department/directorate action plans with compliance dates. Managers are to take 'ownership' of the risk assessments and action plans. They are to ensure that the actions plans are adequately funded and completed within the agreed time scales.
- Where risk assessments of areas that affect more than one division and/or identify actions requiring significant capital investment the Security Advisor is to develop action plans and development plans with the Trust Facilities Services.

8 New Security Equipment

8.1 Where the need for new security equipment is identified, either through risk assessment, incident or division the following procedure is to be adhered to.

- An Improvement and Development Request Form is to be completed and sent to the Estates Capital Projects Manager.
- The Security Advisor will be informed and liaise with the Division and Estates to evaluate the need.
- On agreement and approval that the work should proceed the Estates Project Team will organise a quotation for the work.
- The Project Team will oversee all work in liaison with the Security Advisor.
- On completion of the work the Security Advisor and Project Manager will formally inspect and approve the work before handing over to the Directorate.

9 Reporting Faults

9.1 Any malfunction of any existing security measures, (CCTV, access control etc) is to be reported to the Estates Helpdesk on ext 3307. In the event of a malfunction causing a high priority security issue e.g. breakdown of access control system in maternity, Security are to be inform immediately on ext 3634.

10 Security of Attractive Items

10.1

- Each room to have an inventory of all high value items less than £5,000.
- All serial numbers, makes and models to be recorded.
- Regular update of lists (quarterly intervals recommended).
- Appoint one member of staff within each department or ward to have responsibility for carrying out the audit.
- Identify all items with postcode and directorates.

Chesterfield Royal Hospital NHS
NHS Foundation Trust

ACCESS CONTROL AUTHORISATION FORM

PLEASE PRINT ALL DETAILS CLEARLY

Name of Applicant:	
Job Title:	
Department & Division of Applicant:	
Signature of Applicant:	
Please Indicate if a new ID badge is required:	**YES -** ☐ **NO -** ☐
Please Indicate if a Change of Name/Job title Required:	**YES -** ☐ **NO -** ☐

ACCESS REQUIREMENTS

Area of access required: **Please enter the door swipe number from the swipe box – e.g. 17/13/270**
Reason for access:
Please note - staff will automatically be given access to designated All Staff areas
PLEASE NOTE THAT THE PERSON AUTHORISING ACCESS MUST BE THE PERSON RESPONSIBLE FOR GRANTING ACCESS FOR THE AREA AS PER THE ACCESS CONTROL AGREEMENT
Name of Authorised Signatory **(Please Print):**
Signature of Authorised Signatory

FOR ENVIRONMENTAL COMPLIANCE OFFICE USE ONLY

Card Number:	**Date Access Given:**
Please return the completed form to **Jackie Jordan Environmental Compliance Team, Estates or the Security Office**	

Chesterfield Royal Hospital NHS
NHS Foundation Trust

KEY REQUEST FORM

DIRECTORATE/ DEPARTMENT /

ROOM NO	KEY NO	KEY TYPE

NO OF KEYS	COST CODE

NAME OF PERSON WHO WILL BE HOLDING THE KEY/S

REASON FOR REQUEST

SIGNED	DATE
PRINT NAME	
(Authorised key signature ONLY)	

Completed form to be sent to: Building Team Leader (Estates Department)

KEY COLLECTION/RECEIPT DETAILS

NO. OF KEYS	KEY REF

DEPARTMENT	ROOM NO

SIGNED:
PRINT NAME:
DATE:

Procedure and Guidelines for the Removal of Offensive Weapons

1 Introduction

1.1 These procedures provide staff with general information about offensive/dangerous weapons and provide a procedure on what to do if patient or visitor is found in possession of an offensive/dangerous weapon.
Chesterfield Royal Hospital NHS Foundation Trust will not permit any patient or visitor to be in possession of an offensive/dangerous weapon whilst on Trust premises. The Trust will work very closely with Derbyshire Police in following national guidelines and procedures to ensure the safety of patients, visitors and staff on any of the Trust premises.

2 General Information/Definition of a Offensive Weapon

2.1 Offensive weapons are defined in the Prevention of Crimes Act 1953

*'offensive weapons' means any article **made** or **adapted** for **use** for causing injury to a person, or intended by the person having it with him for such use by him or by some other person.*

Below are examples of the words used:

Made - Sheath knife (currently blade 3" or longer), firearm (any gun), bayonets or knuckledusters etc.

Adapted – This includes items which have an innocent use but which have been altered. Such as a length of wood with a nail driven through, broken bottles or glass, a Stanley knife taped to a hammer head or a washing up bottle fixed with acid, etc.

Used – This is the most difficult category to define, as the weapons use is dependent on the intention of the person carrying it. Such incidents will usually be for the police to decide but for example – is there a good reason for going into hospital with a broken chair leg or iron bar and what is the persons intention.

Bladed or pointed articles was introduced to cover items that would not be classed as offensive weapons by the above legislations or cases where it is not possible to show any intent. An example of this is an individual carrying an ice pick who can provide no good reason for carrying it but against whom no intent to use can be proved.

Under current legislation most objects with a blade longer than three inches or that is sharply pointed cannot be carried in public without a good reason.

What constitutes an offensive weapon is any weapon classified under the Prevention of Crime Act 1953 and subsequent amendments, which is made, adapted or used in the course of a criminal act.

3 Procedure for the Removal of Offensive Weapons from Patients and Visitors

3.1 If any member of staff knows or suspects that a patient or visitor is in possession of a weapon:

- Inform the Ward Matron; if out of hours inform the Night/Site Matron and Security.
- The patient or visitor should be requested to voluntarily hand the weapon over to the Matron or Security and asked to complete and sign a disclaimer form in the presence of two members of staff.
- If the patient or visitor refuses to hand the weapon over the Matron must call the Police and Security for assistance. If the individual is a patient staff should

make a record of the refusal and place it in the patient's records.

- If the patient or visitor refuses to hand over the weapon and presents an immediate risk or threatens anyone with the weapon the Matron or staff must call the Police on 999 and Security on 7777 for immediate assistance. If safe to do so reasonable force can be used to remove the offensive weapon from the patient or visitor.
- All incidents must be reported on datix and include the police incident number if applicable.

If the weapons concerned appears to be a firearm the following procedure must be followed.

- Staff should ask the patient/visitor to put the firearm down and then move everyone from the immediate area.
- The Police must be called on 999 who should then come and remove the firearm for safe keeping.
- Call Security on extension 7777 they will attend and assist staff in managing the situation.
- On no account should any member of staff handle the firearm.
- If the patient/visitor refuses to hand over the firearm everyone must be moved from the immediate area. Without endangering yourself or others obtain as much information as possible at the time of the incident to hand over to the Police along with patient/visitors known location and the patients/visitors actions at the time. The Police must be called on 999 as an EMERGENCY call and all the available information passed onto them.

No patient or visitor on Trust premises can hold an offensive weapon for his/her own or anyone else's safety. If a patient or visitor refuses to hand over an offensive weapon staff must call the Police as soon as possible and Security if required.

3.2 Unconscious Patient

3.2.1 Should a patient be unconscious or unable to hand over a weapon voluntarily at the point of admission the patient must be searched and the Trusts Patient Property Policy followed.

4 Retention of Confiscated Items

4.1 All confiscated items should be sealed in an Offensive Weapons Tube. If for any reason an Offensive Weapons Tube is not available and the weapon involved is a knife, or sharp pointed object, a padded envelope must be used as a matter of safety. The envelope must have the patients or visitors name, patient number if applicable and the ward or unit marked clearly on the envelope together with a disclaimer form.

The disclaimer form must be signed by two members of staff and at the earliest opportunity security informed. The Trust Security Team will record all details in the confiscated items register (details will be taken from the disclaimer) A receipt form must be issued by security and kept with the disclaimer form in the patient records. A second copy of the disclaimer and receipt form must be made and will be transferred and kept in the designated safe location.

Where dangerous weapons are found the Trust Security Advisor will assume responsibility for informing the Police.

5 Records of Confiscated Items

5.1 Details of confiscated items are to be entered in the Confiscated Items Register that will be held in the Security Office.

Details to be entered into the register include:

- Time and date of receipt issued

- Description of item
- Patients or visitors name and patient number if applicable
- Ward or Unit
- Matrons or managers name
- Person accepting the item for transportation
- Where item will be stored.

6 Handling and Transfer

6.1 Handling and transfer to the designated safe location will be carried out by Security. Prior to the item being transferred security will issue the Ward Matron or Nurse in charge a receipt and ensure all details have been recorded in accordance with the procedures outline above.

Transfer of the confiscated item will be a single journey from the Ward or Unit to the designated safe location. The transfer is to take place as soon as possible once the item had been confiscated.

All confiscated items will be place in a designated safe location, which will be either an unmarked safe or secure cabinet. The designated key holders for the safe will be security. No unauthorised entry to the safe or secure cabinet is to be permitted.

7 Disposal

7.1 Disposal of confiscated items will normally be carried out by the Police. Details of all disposals must be recorded in the Confiscated Items Register. If the item is not classified as an offensive weapon under the Prevention of Crimes Act written consent will be required from a Director.

Methods of disposal:

- Police pick up direct from the ward or designated safe location.
- Security Advisor to arrange with Police to deliver confiscated item to a specific Police Station.
- Patient, on production of written consent from a Director.

Under no circumstance can any items be removed from the safe location, unless it is for authorised disposal.

8 Returning Confiscated item to Patients

8.1 No item is to be returned to a patient without the written consent of the Director responsible for the unit or ward involved.

9 Police Involvement

9.1 Where the police have been called to remove a weapon the police will assume responsibility for the transfer and disposal of the item. A receipt should be obtained from the Police officer attending and placed in the patient's records.

10 Confidentiality

If the individual in possession of the weapon is on NHS premises for non-medical purposes, e.g. as a visitor, the issue of confidentiality will not normally arise. If they have attended for the purpose of accessing NHS services, a report to the police will usually involve a breach of confidentiality. In the interests of public safety and the prevention and detection of crime, such a breach may be justified as being in the public interest, in accordance with the provisions of the Data Protection Act 1998, the Human Rights Act 1998 and the guidance given in the NHS Confidentiality Code of Practice.

11 Appendices

11.1

- Appendix A - Receipt For Offensive/Dangerous Weapon
- Appendix B - Disclaimer Form
- Appendix C – Confiscated Items Register

CHESTERFIELD ROYAL HOSPITAL

RECEIPT FOR OFFENSIVE/DANGEROUS WEAPON

Unit_____Ward_____

Patients Name_____

Patients Number_____

Date (DD/MM/YYYY)_____Time(HH/MM)_____

Detailed description of weapon:
(*knife is not sufficient –i.e., knife, black handle, blade approximately 4" long*)

_____
_____
_____
_____
_____

Ward Matron or Deputy Security Officer,

_____Print Name_____

_____Signature_____

Storage Location_____

No item will be returned except on production of written consent from a Director of Service

One copy to be attached to patient's notes, if applicable
One copy to be attached to weapons tube or envelope.

Appendix B

CHESTERFIELD ROYAL HOSPITAL

DISCLAIMER FORM

To be completed by the Patient/Visitor in possession of Classified Weapons

I _____ (Patient's/Visitors Name) (*please print*)

hereby confirm, that I have been informed by an authorised member of Chesterfield Royal Hospital staff, that the items listed below, **appear** to be Classified Weapons and I agree to hand them over the management of the unit.

Ward and Unit_____

Description of Confiscated Item(s)_____
_____
_____
_____
_____
_____

(If there is not sufficient room please use the reverse of this form)

I understand that the items listed above **MAY NOT** be returned to me and I give my consent for the item(s) to be disposed of by the management, if it is deemed necessary, in an appropriate manner. I also understand that Hospital may notify the Police that the above item(s) have been found in my possession, if this is done the item(s) will be handed over to the Police.

Signature of Patient/Visitor

Client/Patient Number, if applicable

Date

Time
Signatures of Ward Manager/

Staff Nurse/Authorised Persons _____ Print Name

_____ Print Name

One copy to be attached to patient's notes, if applicable.
One copy to be attached to weapons tube or envelope.

Appendix D

CHESTERFIELD ROYAL HOSPITAL

CONFISCATED ITEM REGISTER

Date	Time											