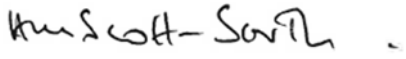
POLICY DOCUMENT

Burton Hospitals
NHS Foundation Trust

SECURITY MANAGEMENT POLICY

Approved by:	**Trust Executive Committee**
On:	**24 October 2017**
Review Date:	**October 2020**
Corporate / Directorate	**Corporate**
Clinical / Non Clinical	**Non-Clinical**
Department Responsible for Review:	**Health & Safety**
Distribution:	
• Essential Reading for:	**All Staff**
• Information for:	**All Staff**
Policy Number:	**279**
Version Number:	**2**
Signature:	 **Chief Executive**
Date :	**24 October 2017**

Burton Hospitals NHS Foundation Trust

POLICY INDEX SHEET

Title:	**Security Management Policy**
Original Issue Date:	**October 2014**
Date of Last Review:	**Policy Review**
Responsibility:	**Head of Health and Safety**
Stored:	**Intranet site**
Linked Trust Policies:	**Health and Safety Policy** **Safe and Secure Environment Policy** **Risk Management Strategy and Policy** **Policy for Reporting and Management of Adverse Incidents and Near Misses** **Lone Worker Policy** **Baby or Child Abduction Policy** **Medicines Management Policy**
E & D Impact assessed?	**EIA355**
Responsible Committee / Group	**Health and Safety Group**
Consulted	**Trust Executive Committee** **Health and Safety Group** **Staff Side**

REVIEW AND AMENDMENT LOG

Version	Type of change	Date	Description of Change
1	New Policy	November 2014	
2	Review of policy	October 2017	Update in light of dissolving of the NHS Protect Service ~~and changes to incorporate the Aggressive Behaviour Marker policy~~ and reference to new Lockdown policy.

BURTON HOSPITALS NHS FOUNDATION TRUST

SECURITY MANAGEMENT POLICY

CONTENTS

Section		Page
1	Introduction	1
2	Purpose	1
3	Definitions	2
4	Duties/ Responsibilities	2
5	Process	6
6	Monitoring Compliance and Effectiveness	12
7	References	12
Appendix I	Procedure for dealing with suspicious packages or letters	13

BURTON HOSPITALS NHS FOUNDATION TRUST

SECURITY MANAGEMENT POLICY

1. INTRODUCTION

Burton Hospitals NHS Foundation Trust is committed, as far as is reasonably practicable, to ensuring the safety and welfare of its staff, patients, visitors, members of the public and the protection of Trust buildings and assets.

The Trust objectives to maintain security of the all premises and assets are based on Trust policies and Government security related legislation. The Management of Health and Safety Regulations 1999 places a specific duty on employers to carry out risk assessments of the hazards that employees and others may be exposed to and determine and implement suitable control measures to avoid or minimise the risk as far as is reasonably practicable.

This policy applies to all staff employed by the Trust, either directly or as part of a contracted service, and to any other person or organisation that uses Trust services or premises for any purpose. All staff have a core responsibility to ensure that local security measures and procedures are observed at all times. Specific roles and responsibilities of nominated staff with regards to security management are detailed in Section 3 of this Policy document.

The Policy directions shall be adopted Trust wide but it should be recognised that local procedures and protocols shall continue to be developed and implemented to support the Policy.

2. PURPOSE

The purpose of this policy is to advise and support Trust staff on security matters and to seek their support and commitment to ensure that all staff undertake an active role to ensure a safe and secure working environment is maintained and pro-security culture is created. This policy will include appropriate precautions, guidance and advice for staff with a role in maintaining a safe and secure environment.

The main aim of the policy is to integrate the management of security into existing practice and governance arrangements adopted by the Trust to ensure the following:

- Local security arrangements within own Ward/ Department
- The requirement to undertake appropriate risk assessments regarding the physical security of premises and assets to protect against theft,

malicious acts and criminal damage and identifying ‘hot spots’ for the Trust.
- Local arrangements for preventing and managing violence and aggression.
- Arrangements for ensuring the safety of lone workers.
- The investigation of security incidents and sharing lessons learnt.
- Training requirements.

Section 5 outlines some examples of the processes in place which contribute to the Management of Security within Burton Hospitals NHS Foundation Trust.

3. DEFINITIONS

Physical Assault
The intentional application of force against a person without lawful justification, this may result in physical injury or personal discomfort.

Non-Physical Assault
Non-physical assault – the use of inappropriate words or behaviour causing distress and / or constituting harassment.

Closed Circuit Television Cameras (CCTV)
Cameras placed in strategic areas of high risk to capture live motion and enable recording of an event where required.

Identified Front Line Staff
Staff who have been identified through risk assessment as working in high risk areas of verbal and /or physical abuse.

Lockdown
A lockdown is the process of preventing freedom of entry to, exit from or movement within the Trust (see separate Lockdown Policy).

4. DUTIES / RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive has overall responsibility and accountability for the implementation of all aspects of this policy and to ensure that the organisational commitment to security management is fully met and monitored. The Board recognises that a successful healthcare organisation ensures that its expertise in service provision is translated into all aspects of its work and that effective security management is an integral part of work practice.

4.2 Director of Governance / Security Management Director

The Director of Governance undertakes the role of Security Management Director (SMD) and takes overall responsibility for overseeing security management work and ensuring compliance with Secretary of State directions as well as ensuring that the Local Security Management Specialist (LSMS) has the necessary resources and support available to carry out their role effectively.

Reporting directly to the board the SMD will be responsible for ensuring that there are appropriate up to date security management services and specialist advice available within the Trust. The SMD will also be responsible for ensuring that effective systems and work practices are in place and for promoting preventative security measures throughout the Trust.

4.3 Health and Safety Group

The Health and Safety Group is accountable to the Quality Committee.

The Health and Safety Group will:

- Provide assurance on health, safety and security performance to the Board.
- Undertake and report back on the Group's annual programme of work.
- Establish and review a performance framework for health, safety and security within the Trust.
- Ensure that the Trust receives adequate specialist advice in all areas of health, safety and security.
- Identify key risks, review and monitor associated incident statistics and trends, and make recommendations for action as appropriate.
- Receive and consider health, safety and security reports, including incident investigations from specialist advisors, external inspectors and staff representatives and make recommendations as appropriate.
- Monitor and analyse associated performance data, for example inspections and training.
- Develop and approve health, safety and security strategies and associated policies.
- Act as the central point for consultation on new and revised policies relating to Health, Safety and Security.
- Oversee the implementation of health, safety and security policies and be responsible for their review.
- Receive pertinent national reports and make recommendations for local practice as required.
- Promote health, safety and security across the Trust.
- Develop annual work plans for health, safety and security.
- Produce an annual report for health, safety and security.

4.4 Head of Health and Safety/ Local Security Management Specialist

The role of the Local Security Management Specialist (LSMS) is primarily to deliver security management work locally to agreed national standards as set out in the Secretary of State Directions. The post holder will be responsible for the following:

- Ensuring that appropriate steps are taken to create a pro-security culture.
- Arrange for security awareness to be included as part of the staff induction process.
- Undertaking crime reduction work including crime reduction surveys.
- Develop and review local and organisational action plans to implement solutions to security risks identified during risk assessments.
- Implement and maintain active and reactive monitoring to ensure adherence to security policies and physical security requirements.
- Undertaking investigations of security breaches and reporting as required.
- Ensuring that where a member of staff has been assaulted that appropriate support and counselling has been made available.
- Ensuring that lessons learned are fed into further risk analysis and crime reduction work.
- Working with the SMD, Legal Team and NHS Legal Protection Unit (LPU) to ensure cases are progressed, sanctions applied and that redress is sought as appropriate.
- Ensuring that security incidents are publicised as appropriate.
- Providing advice and guidance as required to the Trust.
- Producing an Annual Report and work plan.
- Liaising with Regional Security groups and undertaking LSMS duties.

4.5 Heads of Services / Managers and Supervisors

Heads of Service / Managers and Supervisors are responsible for leading on and promoting security, safe working practices within their areas of responsibility, in particular they will be responsible for:

- Ensuring that local procedures and protocols are developed for the security and safety of all persons, property, assets and information within their area of responsibility.
- Inform staff of Security Management Policy and ensure they are aware of local procedures and protocols and of their responsibilities for security.
- Ensure staff are issued with identification badges and wear / carry in accordance with local protocol.
- Ensure staff attend statutory and mandatory training.
- Report, review, manage and investigate security related incidents in line with Trust Policy, ensuring all staff are aware of their responsibilities, and of the process, for incident reporting.
- Undertake and review periodically, or where required, inspections and risk assessments of all work activities and of all environments where

their staff are required to work. This should include the physical security of premises and assets.

- Prepare action plans, and take appropriate action, to eliminate or minimise risk from hazards identified through the risk assessment process.
- Conduct an Annual Health and Safety and Security Departmental Inspection of their ward/ department.
- Where required undertake lockdown risk profiles for each of the sites.
- Managers should ensure that staff are made aware of the Incident Reporting Policy and that all incidents within their area of responsibility are reported in accordance with the policy.

4.6 Head of Estates

The Head of Estates is responsible for:

- The management of maintenance of Trust owned properties and security systems to maintain the physical security of premises.
- Ensuring that the physical security of premises and assets are considered in the planning of new developments and upgrading of existing buildings.

4.7 Staff

Staff are responsible for:

- Ensuring they have read and understood their responsibilities within the Security Management Policy.
- Complying with local procedures and protocols.
- Informing their manager of any actual or suspected security issues and reporting incidents in accordance with Trust policy.
- Wearing or carrying identification badges in accordance with local protocols.
- Attending statutory and mandatory training.
- Ensuring prevention of tailgating and challenging individuals that do not have ID/swipe badges for authorised areas.
- Being vigilant and reporting security incidents on the Datix system and informing the Head of Health and Safety/ Local Security Management Specialist.

4.8 Security Guards

All Security guards, including the in-house team that provide cover during the day and the contracted team that provide cover during the night and weekend, are trained and licenced by the Security Industry Authority (SIA). Security guards are responsible for patrolling areas, and generally basing themselves around the Emergency Department. They will respond promptly to all call outs from wards/departments as required and act appropriately. Any Security incidents or acts of crime will be reported to the Head of Health and Safety/ Local Security Management Specialist.

5. PROCESS

It will primarily be the responsibility of individual services / departments / ward managers and team leaders to ensure that the risk assessment process is applied to security, violence, and the working environment for their areas of responsibility. Specialist and professional advice can be sought from the Head of Health and Safety Local Security Management Specialist.

5.1 Security Alerts

Security Alerts are flagged up by the police, other trusts or the Regional Security group that has caused concern on any NHS premises anywhere in the country. Security Alerts are sent to trusts to be drawn to the attention of any relevant wards or departments.

5.2 Violence and Aggression (Physical and Non-Physical)

It should be recognised that the management of violence and aggression will always present a significant risk to an organisation such as this Trust due to the very nature of the client / patient base that care is delivered to. Staff delivering such care can expect to have to manage challenging behaviour which will at times include the management of violence and aggression. It should also be recognised that the Trust is committed to ensure that relevant control measures are implemented to mitigate against identified risks related to violence and / or aggression and all staff receive the relevant training and have the relevant skills to be able to deal with such situations.

5.3 Paediatric / Security of Children

The provision of a safe and secure environment is recognised by the Trust as a statutory requirement of health and safety legislation and in particular, compliance with the Secretary of State's Directions to NHS Bodies on Security Management measures.

Risk Management will be at the heart of Security Risk Management. The Trust will harness the information and experience of individuals within the Trust (and external expertise as appropriate) and translate that, with their help, into positive action which will either eliminate or reduce risks.

Services are responsible for carrying out suitable and sufficient risk assessments and where required develop local policies, protocols and procedures bringing them to the attention of all stakeholders. Please see the Baby or Child Abduction Policy.

5.4 Physical Security of Building, Premises and Assets

The Trust is committed to ensure that effective control measures and work practices are developed and maintained to enhance the physical security of all its buildings, premises and assets. The following information will detail procedural and operational directions to ensure this is achieved.

5.4.1 New Builds, Redevelopment or changes of use of existing premises

To support this and ensure that effective measures to enhance physical security are implemented from the outset, the Head of Health and Safety / LSMS should be consulted with and informed at the earliest opportunity of any planned new builds, redevelopments or change of use, so that appropriate advice and guidance can be sought. The Head of Health and Safety / LSMS should then be involved at all stages of the planned redevelopments up to the point of when the redevelopment is signed off and functional.

5.4.2 Access Control Systems

Where access control systems are utilised on Trust premises it shall be the responsibility of the designated manager of the ward / unit or department to ensure that local protocols are in place to ensure correct procedures and working practices are adopted for the use and management of such systems.

The following information shall provide guidance, direction and best practice to be adopted by staff where access control systems are utilised.

- Doors that are designated access control points should be kept closed at all times and should never, for any reason, be propped open.
- Keys or access control proximity / swipe cards that have been allocated to an individual member of staff should never be loaned to or used by another person.
- Staff should always be aware of, and safeguard against potential unauthorised access into restricted areas and not allow unauthorised persons attempting to tailgate through access control points into such areas.
- Premises and individual departments vacated for any length of time must be secured to restrict form of unauthorised entry.
- Combinations for key pad locks should never be given to unauthorised persons and should be changed at least twice a year.
- All access control points should be checked on a regular basis to ensure they are working correctly and are secure.

5.4.3 Staff and Visitor Identification

All staff and visitors shall adhere to the following directions and guidance with regards to identification systems whilst on Trust premises or Trust business:

- Whilst on Trust business, all staff will have available on their persons, at all times, a standard Trust ID card.
- ID Cards will bear the Trust name and hospital logo, the individuals name and designation and photographic likeness of the individual.
- Lost or damaged cards must be reported to the individuals line manager immediately and a replacement sought without delay.
- ID cards must be returned to the individual's line manager on leaving the employment of the Trust.
- Individual managers who employ or allow temporary workers, volunteers or contractors on their premises shall ensure that these persons are bona-fide and if these persons are working within the areas for a considerable period of time then consideration should be given to issuing them with a temporary Trust ID card.
- Visitor record systems may vary between sites and areas but all should record similar information that will include name, the date, the purpose of the visit, who they are visiting and the registration of any vehicles parked on the premises.
- All visitor recording systems will include reference to essential safety information that must be brought to the attention of the visitor on their arrival, i.e. action to take in the event of a fire.

5.5 Alarms

5.5.1 Security Alarm Systems

Security alarm systems that are properly selected, correctly installed and properly monitored can help to prevent losses of property through criminal activity and provide better personal protection for staff and patients. It should however be recognised that an alarm system can only monitor areas for breaches in security and will not protect premises, objects or personnel by themselves. To offer protection, an effective response to the alarm activation is essential.

Where security alarms systems are utilised on Trust premises it shall be the responsibility of the designated managers of the ward, unit or department to ensure that local protocols are in place to ensure correct procedures and working practices are adopted for the use and management of such systems.

All staff who are required to use these systems during the course of their work should be given the relevant training and guidance to ensure that they are utilised in the correct manner.

5.5.2 Panic Alarm Systems

In all high risk inpatient areas, staff should have the use of an effective panic alarm system. The requirements for a system will be made following a suitable risk assessment of the area by the department/ ward manager.

It is recommended that as a minimum weekly panic alarm checks are made to ensure the continuous efficiency of the system to ensure it is in good working order and relevant staff are notified that can take action on hearing the alarm.

5.5.3 Personal Alarms / Lone Worker Devices

In areas not covered by panic alarm systems, staff may feel access to a personal attack alarm or Lone Worker Device is beneficial.

Lone working risk assessments undertaken by the ward / department manager will highlight if and where a personal alarm / Lone Worker Device should be issued to the staff member. This will be based on the level of risk to staff health, safety and security.

5.5.4 CCTV

Close circuit television cameras play an important role as part of crime prevention and detection within the Trust. These cameras are monitored on a 24 hour basis. Full operational procedures and Codes of Practice will govern the operation and manning of the scheme.

The objectives of the scheme are to:

- deter and detect crime
- help identify, apprehend and prosecute offenders
- reduce vehicle theft
- reduce the fear of crime and reassure users of the service
- secure a safer environment for those working in the hospital
- provide assistance in Crime Prevention
- provide the Police and the Trust with evidence to take criminal and civil action in the courts
- assist in locating missing patients

Detailed information about CCTV arrangements is available in the CCTV Policy.

5.6 Security of Property (Trust / Patient / Personal)

The Trust is committed to ensure that effective control measures are in place to ensure that Trust patient or personal property is not subject to theft, loss, malicious/criminal damage or misuse. The following information shall detail direction and guidelines to ensure this is achieved.

5.6.1 Trust Property

Staff should ensure adequate measures are taken to protect Trust equipment and that all items of equipment are not left vulnerable to potential theft, loss, malicious / criminal damage or misuse.

When Trust equipment is not in use all items should be stored in a secure environment and not left on general view. When Trust equipment is carried in vehicles it should always be safeguarded by placing items out of sight and locking the vehicle when unattended. All incidents of theft, loss, malicious / criminal damage and misuse of Trust equipment should be reported through the incident reporting process.

5.6.2 Patient Property

Property belonging to patients and clients can be subject to theft, malicious damage or misuse. All patients and clients should be encouraged to leave property or personal items of a valuable nature at home or hand them in for safekeeping. All staff must ensure the following points are adhered to:

- Record all property that is formally handed over and ensure the patient is issued with a receipt.
- To advise patient and their relatives / carers of the risks if they do not formally hand property over for safekeeping.
- A patients property form must always be completed even if patients do not hand over property.
- If patients are likely to be away from the Ward / Unit for a period of time, staff must encourage them to hand over all valuables for safekeeping.
- Individual Directorates must develop processes for the recording of all patient property brought into ward and / or units.

5.6.3 Staff Property

All staff must take responsibility for their personal property and to make use of locker facilities where available. Only essential items and minimum quantities of cash should be brought to work. Staff should not leave valuable items unattended at any time. The Trust does not take responsibility for losses of or damage to personal property at work.

5.7 Security of Drugs, prescription forms and hazardous material

The strategy for safe and secure handling of drugs, controlled prescription stationery and disposal of pharmaceutical waste is handled by the Pharmacy team (see Medicines Management Policy).

5.8 Lockdown (Emergency Procedures)

Lockdown is the process of controlling the movement, access and egress of people around NHS property, or other specific building / area in response to an identified risk, threat or hazard that might impact on the safety and security of people and assets or, indeed the capacity of that facility to continue to operate.

A lockdown may be implemented by the Trust as part of a security incident or the major incident plan. This may be in partnership with other organisations both NHS and external e.g. due to Police intelligence – please see the Trust Lockdown Policy and Procedure for more information.

5.9 Major Incident and Contingency Planning

The Civil Contingencies Act 2004 is an important legislation providing a statutory and regulatory framework for civil protection in the UK and sets out clear expectations and responsibilities for front-line responders at local level, to ensure that they are prepared to deal effectively with the full range of emergencies from localised incidents to full-scale emergencies.

The Civil Contingencies Act 2004 and accompanying regulations and guidance provides a single framework for civil protection across the United Kingdom. The Act is divided into two parts

Part 1 – focuses on local arrangements for civil protection, establishing a statutory framework of roles and responsibilities for local responders.

Part 2 – focuses on emergency powers, establishing a modern framework for the use of special legislative measures that might be necessary to deal with the effects of the most serious emergencies.

RESPONDERS

Two types of responders have been identified, these are:

Category 1 Responders are those organisations at the core of any emergency response; for example local authorities, the emergency services, NHS Trusts.

Category 2 Responders are those organisations likely to be heavily involved in an emergency response, for example utility companies, rail companies, airport operators, the Highways Agency.

5.10 Suspect Packages / Suspicious behaviour

Dealing with suspicious packages or letter is covered in Appendix I.

Any suspicious behaviour should be reported appropriately, this could be to your line manager, or call switchboard to inform or call security, or if appropriate, call the police.

5.11 PREVENT (Counter Terrorism)

The UK's Counter-Terrorism Strategy (CONTEST), aims to reduce the risk to the United Kingdom from terrorism, so that people can go about their lives freely and with confidence.

CONTEST is organised around four principal work streams:

- Pursue: - to stop terrorist attacks
- Prevent: - to stop people from becoming terrorists or supporting terrorism
- Protect: - to strengthen our protection against terrorist attacks
- Prepare: - where an attack cannot be stopped, to mitigate its impact

The Trust's contribution to the Prevent work stream is to categorise Prevent Awareness as Mandatory, therefore all staff will receive Workshop to Raise Awareness of Prevent (WRAP) Training on induction and three yearly update through safeguarding training.

The Trust has arrangements with the Police Counter Terrorism department to deliver training in Counter Terrorism, staff at all levels are encouraged to attend.

6. MONITORING COMPLIANCE AND EFFECTIVENESS

A review of this policy will take place every 3 years.

Monitoring of any risk assessments including action plans and follow up for the physical security of premises and assets will be undertaken annually by Department/ Ward managers by the Health, Safety and Security Inspection which will be feedback to the Head of Health and Safety/ LSMS and reported to the Health and Safety Group.

7. REFERENCES

- Tackling crime against the NHS – a strategic approach
- Standards for Providers – Security Management
- Tackling violence and anti-social behaviour in the NHS Joint Working Agreement between the Association of Chief Police Officers and the Crown Prosecution Service
- A Professional Approach to managing security in the NHS
- Health and Safety at Work etc. Act 1974

Appendix I

Guidance from Staffordshire Civil Contingencies Unit

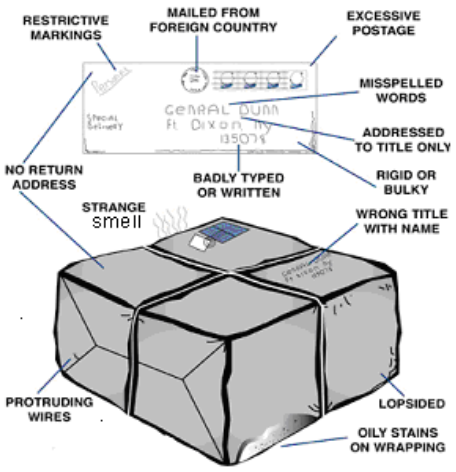
PROCEDURE FOR DEALING WITH SUSPICIOUS PACKAGES OR LETTER

What is a Suspicious Package or Letter?

A suspicious package is just that – a package or envelope found or received, normally by mail or courier or delivered in person, which arouses the suspicion of the receiver because of some indicator or indicators. It may or may not be preceded by letter or telephone threats or warnings. It may simply be poorly addressed, or it may be a hoax.

The likelihood of receiving a package or letter containing suspicious substances is remote. However, it is important for staff to be aware of characteristics that are common to suspicious packages. Some indicators include, but are not limited to, the following.

- Unexpected package or letter from an unknown source
- Mailed from a Foreign Country
- Excessive Postage
- Misspelled or Misused Words
- Addressed to Title Only
- Wrong Title with Name
- Rigid or Bulky
- Badly Typed or Poorly Written
- Restrictive Delivery Markings
- No Return Address
- Lopsided / Protruding item
- Stains on Wrapping
- Possibly oil stained or unusual odour
- Substance leaking from the package



Examples of Dangerous items that can be sent via mail

There is a wide range of dangerous items that can be sent by post, it may be an explosive device, a chemical, a biological agent or a radioactive substance. Each type of suspicious package poses separate difficulties.

What to Do If You Find or Identify A Suspicious Package or Letter

If a package or letter arouses suspicion and you cannot verify the contents with either the addressee or the sender:

LEAVE IT ALONE! – If you are holding it, gently put it down on a hard, flat surface. **Do not place it in water or sand.**

- **TELL YOUR SUPERVISOR – BUT DO NOT USE RADIOS OR MOBILE PHONES** anywhere near a suspicious package.

- **ENSURE** no one else comes in contact with it.

- **EVACUATE** the immediate area to a safe distance. Put a solid wall between you and it.

- **TURN OFF** any fans, heaters, or air conditioning equipment in the immediate area.

- **ADVISE** colleagues not to brush any powder or liquid off of their clothing or person, keep their hands away from their face and wash their hands, if possible, without leaving the area. (Make a list of these people).

- **SECURE** all doors and access points (inc. stairs, lifts & hallways) that lead to the area.

- **WASH** your hands with soap and water immediately if you have been in contact with a suspicious package or its contents (avoid touching anything else, especially your face).

- **REMAIN ON SITE IN A SAFE LOCATION** – all persons who have had contact with the package / letter or who were in the immediate area **must remain** until contacted by a **SENIOR MANAGER ON SITE**.

SENIOR MANAGER ON SITE:

- **Remember –** ***No Radios or Mobile Phones near any suspect packages.***

- **CONFIRM CONTACT** with the Police and **stand by** until relieved by them.