Trust-wide Document

NHS
Great Western Hospitals
NHS Foundation Trust

Security Policy

Document No	HR - 00010	**Version No**	3.0
Approved by	Policy Governance Group	**Date Approved**	11/02/2020
Ratified by	Security Advisory Group	**Date Ratified**	04/02/2020
Date implemented (made live for use)	21/04/2020	**Next Review Date**	04/02/2023
Status	LIVE		

Target Audience- who does the document apply to and who should be using it. - The target audience has the responsibility to ensure their compliance with this document by: • Ensuring any training required is attended and kept up to date. • Ensuring any competencies required are maintained. • Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.	All employees directly employed by the Trust whether permanent, part-time or temporary (including fixed-term contract). It applies equally to all others working for the Trust, including private-sector, voluntary-sector, bank, agency, locum, and secondees. For simplicity, they are referred to as ‘employees’ throughout this policy
Special Cases	None
Accountable Director	Director of Strategy & Community Services
Author/originator – Any Comments on this document should be addressed to the author	Head of Health & Safety, Fire and Security.
Division and Department	Corporate Division. Estates Health & Safety,
Implementation Lead	Head of Health & Safety, Fire and Security
If developed in partnership with another agency ratification details of the relevant agency	N/A
Regulatory Position	Health and Safety at Work etc. Act 1974 (HSW ACT) (Ref 13) The Management of Health and Safety at Work Regulations 1999 (Ref 14) Occupiers Liability Acts 1957 (Ref 15) Occupiers Liability Act 1984 (Ref 16) The Children Act 1989 (Ref 17) The Theft Act 1968 (Ref 18) The Data Protection Act 2018 / GDPR (Ref 19)
Review period. This document will be fully reviewed every three years in accordance with the Trust’s agreed process for reviewing Trust -wide documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.	

Contents

1 Introduction & Purpose

1.1 Introduction & Purpose

This policy sets out the security objectives of Great Western Hospitals NHS Foundation Trust (the Trust). Security includes the protection of sites and the buildings and the personnel and property that they contain.

1.2 Glossary/Definitions

The following terms and acronyms are used within the document:

BWV	Body Worn Video
CCTV	Closed Circuit Television
CQC	Care Quality Commission
DBS	Disclosure Barring Checks
DPO	Data Protection Officer
EIA	Equality Impact Assessment
GDPR	General Data Protection Regulation
H&S	Health and Safety
HSW	Health and Safety at Work
IP&C	Infection Prevention and Control
IT	Information Technology
Lockdown	The process of controlling the movement and access – both entry and exit – of people (NHS employees, patients and visitors) around a Trust site or other specific Trust building/area in response to an identified risk, threat or hazard that might impact upon the security of patients, employees and assets or indeed the capacity of that facility to continue to operate. A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.
Lockdown risk profile	A risk assessment of each site to determine its potential vulnerability to threat and its capability of either partial or full lockdown
LSMS	Local Security Management Specialist
NHS	National Health Service
SAG	Security Advisory Group
Security	The protection of people, information, material activities, reputation and facilities against harm, loss or unauthorised disclosure.
Security Management	"The condition achieved when information, personnel, material, activities and installations are protected against accidental loss, theft, unauthorised disclosure and damage".
SRT	Security Review Tool
Tailgaters	Accesses secure areas by following authorised personnel through the door

2 Main Document Requirements

2.1 Foreword by the Chief Executive

Great Western Hospitals NHS Foundation Trust regards the security of its employees, patients, visitors, Trust assets and information as a prime responsibility, both as an employer and as a health care provider.

The purpose of this Policy is to ensure that the guiding principles and legislation, which govern the management of security risks within the Trust, are clearly stated for the use of all employees.

The Trust is vulnerable to several threats, two of the most important being the safety and welfare of employees, patients and visitors and the security of confidential information held by the Trust in any format, including paper medical notes.

The successful implementation of the policies and procedures contained within this document will depend greatly on the manner in which individuals undertake their personal responsibility and in which managers and senior employees enforce compliance. The Trust will therefore, in support of this Policy, provide relevant training and updates to keep all parties informed and raise awareness.

The Security Advisory Group (SAG) will meet at not less than quarterly intervals in order to oversee the implementation, monitoring and review of this policy. For membership and Terms of Reference of SAG contact the Head of Health, Safety, Security and Fire.

2.2 Security Management Objectives

The safeguarding of Trust property and resources against crime, loss, damage, misplacement and insecurity is of paramount importance.

The Trust's security management objectives are to:

- Ensure the personal safety and welfare of patients, employees and visitors.
- Offer measures to protect the property of patients, employees and visitors.
- Secure hospital property, premises and buildings.
- Protect Trust information and property against theft, fraud, damage and other types of criminal activity.
- Promote a pro-security culture.

2.3 Identifying Security Risks

The Trust recognises that security risks include:

- Terrorism (Ref 10);
- Vandalism of property;
- Theft (Ref 20);
- Fire & arson (Ref 7) ;
- Criminal damage;
- Fraud (Ref 21);
- Inappropriate access to or Misuse of Information (Ref 3);
- Violence against individuals (Ref 5);
- Misconduct by employees/ Bank/agency/locum and students (Ref 21);

Identification of significant security risks will happen at organisational, division and departmental levels.

Managers and their employees are responsible for identifying, assessing and managing the security risks in their work areas and those risks arising from their work activities.

The identification of security risks is a continuous process supported by incident reporting processes; feedback from teams and patients; audit and inspections and guidance from external agencies including the Care Quality Commission and others.

2.4 Security Risk Assessments

All departments are responsible for completing and reviewing any Department specific security risk assessments. These should be current, contain a review date and risk owners name and role.

The security risk assessment will identify site specific security risks and describe agreed actions to minimise and manage those risks. The LSMS is available to advise on request.

The LSMS will complete a Site Security Risk Assessment which will be shared with Site Co-ordinators and with the Security Advisory Group on completion.

The site security risk assessment will be reviewed at least annually or at any time if there has been:-

- A security incident on the site.
- A change to security arrangements.
- A change to the security risk.
- There is any other reason to believe that the assessment is no longer valid.

Department Managers are responsible for identifying, assessing and managing any Department specific risks and will complete the Trust Risk Assessment Template to document the assessment and agreed local arrangements for safety (Ref 4 & 6).

2.5 Security Measures and Controls

The Trust will use the following measures and controls to manage and minimise security risks:

- **Physical measures**. These are physical obstacles planted to protect security interests. A system of surveys, inspections, audits and checks is necessary to ensure the physical measures achieve their original aim.

- **Security education and training**. A vital aspect of security is to ensure all Trust employees, irrespective of status and profession, understand the risks for the Trust and are sufficiently aware of their responsibilities as regards security.

- **Laws, executive letters and instructions**. These range from legislation to Trust and departmental instructions.

2.6 Security of People

The Trust will manage and minimise security risks to employees, visitors and patients by:-

- Working to the Minimising Violence and Aggression in the Workplace Policy (Ref 5).
- Ensuring that Department Violence and Aggression Risk assessments are completed and local arrangements for safety are agreed (Ref 5).

- Ensuring that where risks are identified from an individual, a risk assessment is completed and a strategy is agreed for working safely with the individual (Ref 5).
- Ensuring appropriate alerts are shared with employees about terrorist and other security risks.
- Working to the Incidents Response Plan (Ref 10).
- Providing all employees with photographic identification.
- Developing a culture in which employees feel able to challenge unknown people in their work area (as long as it is safe to do so).
- Working to the Trust's Lone Worker Policy and Guidance (Ref 27).
- Ensuring Departments complete risk assessments for Lone Working and that there are locally agreed protocols for safe working.
- Providing adequate physical security (locks, key codes, electronic entry management) to prevent entry to unauthorised visitors.
- Ensuring key codes for work areas/access passes are only shared with those with authority to access areas.
- Ensuring key codes are changed regularly.
- Working to the Trust's New-born Baby Security (Including the Prevention and Management of Baby/Child Abduction) Policy (Ref 23)
- Complying with the Trust's Alcohol, Drugs and Substance Misuse Policy (Appendix D)
- Following the Protocol for Firearms and Weaponry in Patient's Home (Appendix E)
- Following the Trust's Missing Patient Policy (Ref 26)
- Ensuring that Body Worn Cameras are used by employees in high risk areas of work [currently Car Parking and Security Officers (Ref 25).

2.7 Security of Property

The Trust will manage and minimise security risks to property owned by employees, visitors and patients by:-

- Providing employees with somewhere secure to store their personal belongings whilst at work.
- Following the Trust Patient Property and Lost Property Policy (Ref 20).
- Limiting access to work areas to ensure that only those with authorisation can access the area or ward.
- Having a Trust Asset Register and carrying out asset audits.
- Use of Closed-Circuit Television (CCTV) as a preventative and protective measure (Ref 25)
- Where possible securing valuable assets in restricted areas.
- Encouraging employees, agency/locum and students to be vigilant and to report unauthorised visitors or suspicious behaviour.
- Requiring employees, agency/locum and students to wear their photographic identification at work (Ref 22).
- Ensuring physical security is effective in preventing entry to unauthorised visitors.
- Requiring Departments to complete a monthly Fire and Health and Safety (H&S) Checklist (Ref 12) to identify any security hazards in the work area (Ref 6).
- Working to the Trust's Medical Gas Cylinder (Handling, Storage and Use) Policy (Ref 8).
- Completing an annual Security Risk analysis of all reported incidents to identify trends and determine any Trust assets that may be vulnerable to theft and confirming existing measures to mitigate risks are sufficient.
- Developing a culture in which employees, agency/locum and students feel able to challenge 'tailgaters'.
- Ensuring that portable Information Technology (IT) equipment and equipment in insecure areas is encrypted to make it unusable by unauthorised users, or in the event of loss or theft (Ref 18).

2.8 Security of Premises

The Trust will manage and minimise security risks to premises by:-

- Completing an annual Site Security Risk Assessment to identify security risks.
- Developing a partnership approach (Site Co-ordinators, Estates & Facilities; Managers and the LSMS) to managing and minimising security risks.
- Completing an annual review of the Fire Risk Assessment for all Trust sites to identify any significant (Ref 7) fire/arson risks and agree arrangements to manage and minimise those risks
- Ensuring that appropriate management of waste on sites, working to the Trust's Waste Policy (Ref 9)
- Ensuring that appropriate management of medical gases on site, working to the Trust's Medical Gas Cylinder (Handling, Storage and Use) Policy (Ref 8).
- Providing out-of-hours security response services for the Trust.
- Using Closed Circuit Television (CCTV) (Ref 27) and following the Code of Practice for the Operation of Closed Circuit Televisions (Ref 25)
- Agreeing security response arrangements for all Trust sites.
- Maintaining existing security measures and testing them regularly.
- Ensuring that all sites have clear lockdown procedures for the end of the working day (Ref 1).
- Ensuring that all sites have appropriate lockdown procedures for areas not in use overnight.
- Ensuring that employees entering Trust premises are informed of local security arrangements

2.9 Security of Information

The Trust will manage and minimise security of information risks by:-

- Compliance with the Data Security and Protection Policy (Ref 3)
- Compliance with the Information Governance Policy (Ref 11)

2.10 Reporting Incidents, Accidents and Near Misses

All accidents, incidents and near misses involving violence and aggression will be reported on an Incident Notification Form (Ref 2).

Investigations into breaches of security will be completed by the Department Manager working with the LSMS.

2.11 Employees Working in Non-Trust Premises

Trust employees working within sites not owned by the Trust must ensure that they know what they need to do for their own safety and the safety of others and must comply with the site owners' security policies, procedures and/or guidelines.

3 Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below: -

Measurable policy objectives	**Monitoring or audit method**	**Monitoring responsibility (individual, group or committee)**	**Frequency of monitoring**	**Reporting arrangements (committee or group the monitoring results is presented to)**	**What action will be taken if gaps are identified**
Arrangements (including timescales) for producing a *lockdown risk profile* for each organisational site or other specific building/area	Will be reviewed as part of the update of the policy and will take account of changing roles, organisational structure and tasks	Security Advisory Group	Minimum two yearly or when changes to the policy are made due to guidance or organisational changes	Security Advisory Group	Appropriate action will be agreed and followed up
Requirement to undertake appropriate risk assessments regarding the *physical security* of *premises* and *assets*	Part of health and safety audit (Violence & Aggression Risk Assessment Section)	Health and Safety Group	Annually	Health and Safety Committee	Any gaps will be drawn to the attention of the Security Advisory Group for action.
Compliance with requirement of policy looking at variable elements e.g. tail gating	Mystery Shopper audit Site assessment by professional security consultant	Security Advisory Group	Bi-annual	Security Advisory Group	Any gaps will inform the work planner for the Security Advisory Group
Ensuring that action is taken as a result of risk assessments	Review health and safety audit report	Security Advisory Group to review	Annually	SAG/Health and Safety Committee	Depending on gap, any issues will be flagged back to the relevant department for action. If a Trust wide issue it would be entered on risk register and action plan drawn up by SAG.

4 Duties and Responsibilities of Individuals and Groups

4.1 Chief Executive

The Chief Executive is ultimately responsible for the implementation of this document.

4.2 Ward Managers, Matrons and Managers for Non Clinical Services

All Ward Managers, Matrons and Managers for Non Clinical Services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

4.3 Document Author and Document Implementation Lead

The document Author and the document Implementation Lead are responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

4.4 Security Management Director

The Director of Strategy and Community Services is nominated as the Board Member with particular responsibility for the strategic direction of security risk management and is responsible to the Chief Executive for ensuring that all aspects of security risk management are properly organised, co-ordinated and controlled.

4.5 Director of Estates and Facilities

The Director of Estates and Facilities has specific responsibility for physical security matters across the Trust. This will ensure that a consistent Trust wide approach is adopted towards the provision of security advice and monitoring.

4.6 Trust Security Advisory Group

The Trust's Security Advisory Group (SAG) is responsible for the implementation, monitoring and review of the Trust's Security Policy and for the provision of advice on how best to secure continuous improvement in security risk management throughout the Trust. The Terms of Reference for SAG are available from the Head of Health, Safety, Security and Fire.

4.7 Head if Health, Safety, Security and Fire

The Head of Health, Safety, Security and Fire:

- Has operational responsibility for the security management system across the Trust.
- Will ensure LSMS provision is available in accordance with NHS requirements.
- Will chair the Security Advisory Group.

4.8 Local Security Management Specialist (LSMS)

The Local Security Management Specialist will have day-to-day responsibility for monitoring the Trust's security and the implementation of the requirements of this Policy.

In addition the LSMS will:-

- The LSMS will complete an SRT (Security Review Tool) which will inform the Trust work plan

- The LSMS will complete a quarterly report, this will inform the annual report and will be a working document
- Work with Site Co-ordinators to agree actions to manage and minimise security risks on site
- Act as a source of advice and support to Managers

4.9 Director of Facilities Management (Serco)

The Director of Facilities Management (employed directly by Serco is responsible for the day-to-day operational management of the security personnel employed by Serco as part of the Concession Agreement. The post holder must also ensure that any breaches of security are fully investigated, that appropriate action is taken to reduce the risk of recurrence and that, where there is criminal activity, or suspected criminal activity, the police are informed. **Director of Facilities Management (SERCO),** with close liaison with **The Hospital Company** is also responsible for the support, installation and maintenance of technological and physical security systems and equipment needed to support the Trust Security Policy [with the exception of the Keri security access control system which the Trust retains responsibility for]. The Director of Facilities management also ensures the principle of “Secure by Design” is incorporated into all Trust building and refurbishment programmes.

4.10 Director of Human Resources

The Director of Human Resources is responsible for all recruitment procedures including that appropriate security checks are carried out and to advise on this Policy’s effectiveness in meeting the requirements of the NHS Human Resources Strategy (Ref 28) in particular the targets for reducing incidence of violence and aggression.

4.11 Director of Information Technology (IT)

The Director of IT is responsible for formulating policies, procedures and guidelines relating to the security of all information imported into, stored and disseminated from the Trust. This includes drawing up a disaster recovery plan to counter the loss of computerised information.

4.12 Divisional Directors

Divisional Directors are responsible for the dissemination and implementation of Trust security policies within their areas of responsibility. They also have a responsibility to ensure that all their employees are trained and made aware of the security measures required within their own Division.

4.13 Line Managers

Line Managers have the responsibility to review their local security arrangements routinely in order to confirm any local and Trust-wide physical security risks to premises or assets are adequately managed. Any risks identified should be reported on an Incident Reporting Form or the local risk registers and escalated accordingly.

4.14 Employee Responsibilities

Every employee and member of temporary or agency worker has a responsibility for their own safety and should report any concerns to their Line Manager immediately, in the first instance. Employees and temporary or agency workers are also expected to be aware of the Trust’s Security Policy (Ref 29), standards, procedures and guidelines and their implementation as it affects them.

5 Further Reading, Consultation and Glossary

5.1 References, Further Reading and Links to Other Policies

The following is a list of other policies, procedural documents or guidance documents (internal or external) which employees should refer to for further details:

Ref. No.	Document Title	Document Location
1	Lockdown Risk Profiles	Security Manager
2	Incident Management Policy	T:\Trust-wide Documents
3	Data Security and Protection Policy	T:\Trust-wide Documents
4	Risk Management Strategy	T:\Trust-wide Documents
5	Minimising Violence & Aggression in the Workplace Policy	T:\Trust-wide Documents
6	How to Assess Risk Policy and Procedure	T:\Trust-wide Documents
7	Fire Safety Protocol	T:\Trust-wide Documents
8	Medical Gas Cylinder (Handling, Storage and Use) Policy	T:\Trust-wide Documents
9	Waste Policy	T:\Trust-wide Documents
10	Incidents Response Plan	Intranet/Resilience Manager
11	Information Governance Policy	T:\Trust-wide Documents
12	Monthly Health & Safety & Fire Checklist	T:\Trust-wide Documents
13	Health and Safety at Work etc. Act 1974 (HSW ACT)	www.legislation.gov.uk
14	The Management of Health and Safety at Work Regulations 1999	www.legislation.gov.uk
15	Occupiers Liability Acts 1957	www.legislation.gov.uk
16	Occupiers Liability Act 1984	www.legislation.gov.uk
17	The Children Act 1989	www.legislation.gov.uk
18	The Theft Act 1968	www.legislation.gov.uk
19	The Data Protection Act 2018	www.legislation.gov.uk
20	Patients' Property (including valuables) & Lost Property (including valuables) Policy	T:\Trust-wide Documents
21	Fraud and Corruption Policy	T:\Trust-wide Documents
22	Conduct Management Policy	T:\Trust-wide Documents
23	New Born Baby Security (including the prevention & management of baby/child abduction) Policy	T:\Trust-wide Documents
24	Information Commissioners Office: In the picture: A data protection code of practice for surveillance cameras and personal information	https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Ref. No.	Document Title	Document Location
25	Management, Operation & Use of Close Circuit Television (CCTV) Policy	T:\Trust-wide Documents
26	Missing Patient Policy	T:\Trust-wide Documents
27	Lone Working Policy & Guidelines	T:\Trust-wide Documents
28	NHS Human Resources Strategy	https://improvement.nhs.uk
29	Security Policy	T:\Trust-wide Documents
30	Misuse of Drugs Act 1971	www.legislation.gov.uk

5.2 Consultation Process

The following is a list of consultees in formulating this document and the date that they approved the document:

Job Title / Department	Date Consultee Agreed Document Contents
Local Security Management Specialist	03 January 2020
SERCO Representative	07 January 2020
Head of Information Governance and DPO	22 January 2020
Head of Patient Advice and Liaison Service	15 January 2020
Pharmacy Operations Manager	17 January 2020
Academy Representative	07 January 2020

6 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been completed for this document and can be found at Appendix A.

Appendix A - STAGE 1: Initial Screening For Equality Impact Assessment

At this stage, the following questions need to be considered:			
1	What is the name of the policy, strategy or project? Security Policy		
2.	Briefly describe the aim of the policy, strategy, and project. What needs or duty is it designed to meet? This policy sets out the security objectives of Great Western Hospitals NHS Foundation Trust		
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any of the nine protected characteristics (as per Appendix A)?		**No**
4.	Is there evidence or other reason to believe that anyone with one or more of the nine protected characteristics have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?		**No**
5.	Has prior consultation taken place with organisations or groups of persons with one or more of the nine protected characteristics of which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?		**No**

Signed by the manager undertaking the assessment	Mark Hemphill
Date completed	03/02/2020
Job Title	Head of H&S, Fire and Security

On completion of Stage 1 required if you have answered YES to one or more of questions 3, 4 and 5 above you need to complete a STAGE 2 - Full Equality Impact Assessment

Equality Impact Assessment

Are we Treating Everyone Equally?

Define the document. What is the document about? What outcomes are expected?

Consider if your document/proposal affects any persons (Patients, Employees, Carers, Visitors, Volunteers and Members) with protected characteristics? Back up your considerations by local or national data, service information, audits, complaints and compliments, Friends & Family Test results, Staff Survey, etc.

If an adverse impact is identified what can be done to change this? Are there any barriers? Focus on outcomes and improvements. Plan and create actions that will mitigate against any identified inequalities.

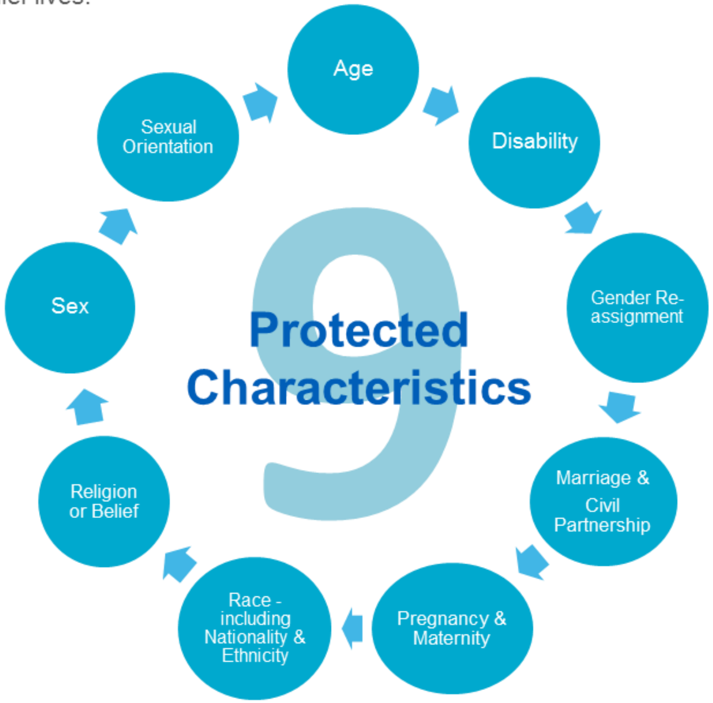
If the document upon assessment is identified as having a positive impact, how can this be shared to maximise the benefits universally?

Trust Equality and Diversity Objectives

Better health outcomes for all	Improved patient access & experience	Empowered engaged & included staff	Inclusive leadership at all levels

Our Vision

Working together with our partners in health and social care, we will deliver accessible, personalised and integrated services for local people whether at home, in the community or in hospital empowering people to lead independent and healthier lives.



9 Protected Characteristics

Age

Disability

Gender Re-assignment

Marriage & Civil Partnership

Pregnancy & Maternity

Race - including Nationality & Ethnicity

Religion or Belief

Sex

Sexual Orientation

Appendix B – The Law and Healthcare

Degree of Responsibility

The Trust, as with all employers, has responsibility for the acts of its employees if they are "committed during their employment ". This is known as vicarious liability. However when it comes to criminal activity by employees, liability and accountability passes from the Trust to the individual because the employee was not employed to commit a crime.

The Trust can be held liable where insufficient measures have been taken to safeguard against criminal activity by its employees, or indeed anyone who enters Trust property. This gives victims the opportunity to pursue the Trust by litigation for negligence and failing to prevent a criminal act.

The Trust through the Human Resources Department must therefore take great care in the selection; training and supervision of its employees to ensure that people, who are unsuitable because they have a criminal history, lack the relevant qualification or have an inappropriate temperament are not employed. The Careful vetting of all applicants against pre-determined criteria is essential.

Health and Safety at Work etc Act 1974 (HSW ACT) (Ref 13)

Crown immunity for hospitals was removed in April 1991 and Trusts are expected to provide a "safe system at work". While the perception is that this applies to areas traditionally covered by health and safety, such as injury and accident prevention, the Act also expects that a safe working environment is provided by means of safe systems of work. This implies a secure environment for patients, employees and visitors.

So far as security is concerned, this includes:

- The identification of the risk.
- A written security policy.
- Adequate training and education to ensure employees are aware of their responsibilities for security.

The Management of Health and Safety at Work Regulations 1999 (Ref 14)

The requirements of the HSW Act were expanded by the Management Regulations and required the Trust to assess the risks and threats in the workplace and to document any significant risks.

Both pieces of legislation demand a positive and proactive response to reduce the risks and to continually monitor and audit to ensure that policies are being enforced. This is covered in a separate policy.

Occupiers Liability Acts 1957 (Ref 15)

The occupier of a premises or facility owes a "common duty of care" to visitors, which in this context includes patients, to ensure they are reasonably safe. Occupier includes employees. This duty of care extends to the activities of third party criminal activity. Failure to provide that duty of care by adequate security measures can lead to substantial damage settlements.

In the event that a duty of care cannot be provided, a warning must be given so that the visitor is aware of the risk.

Occupiers Liability Act 1984 (Ref 16)

Under this Act, Occupiers are also expected to provide a duty of care to trespassers that is those persons on site and using Trust facilities without the permission of the Occupier.

It is the policy of Great Western Hospitals NHS Foundation Trust to challenge suspected trespassers and persuade them it is not in their best interest to remain on site or use Trust facilities of any sort (including those with public access) without permission.

The Children Act 1989 (Ref 17)

The Children's Act was brought into force to govern the welfare of child patients while they are in hospital. The removal of a child by someone without Parental Responsibility amounts to Child Stealing is therefore kidnap and is an arrestable offence.

Provided adults have "Parental Responsibility", as defined in the Children's Act, they may take any decision affecting that child. Therefore to prevent a parent removing a child from hospital irrespective of the state of that child's health could lead to court proceedings. In cases where removal will have a seriously detrimental effect of the child's health, the court may choose not to proceed. This does not mean that clinical and medical employees can make arbitrary decisions about a child without full consultation with those with parental responsibility.

All employees, irrespective of status, involved in the provision of care for children are to be checked with a Disclosure Barring Checks.

The Theft Act 1968 (Ref 18)

The basic definition of the Theft Act 1968 is that a person is guilty of theft if that person "dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it". It is immaterial whether the appropriation took place for personal gain or personal benefit.

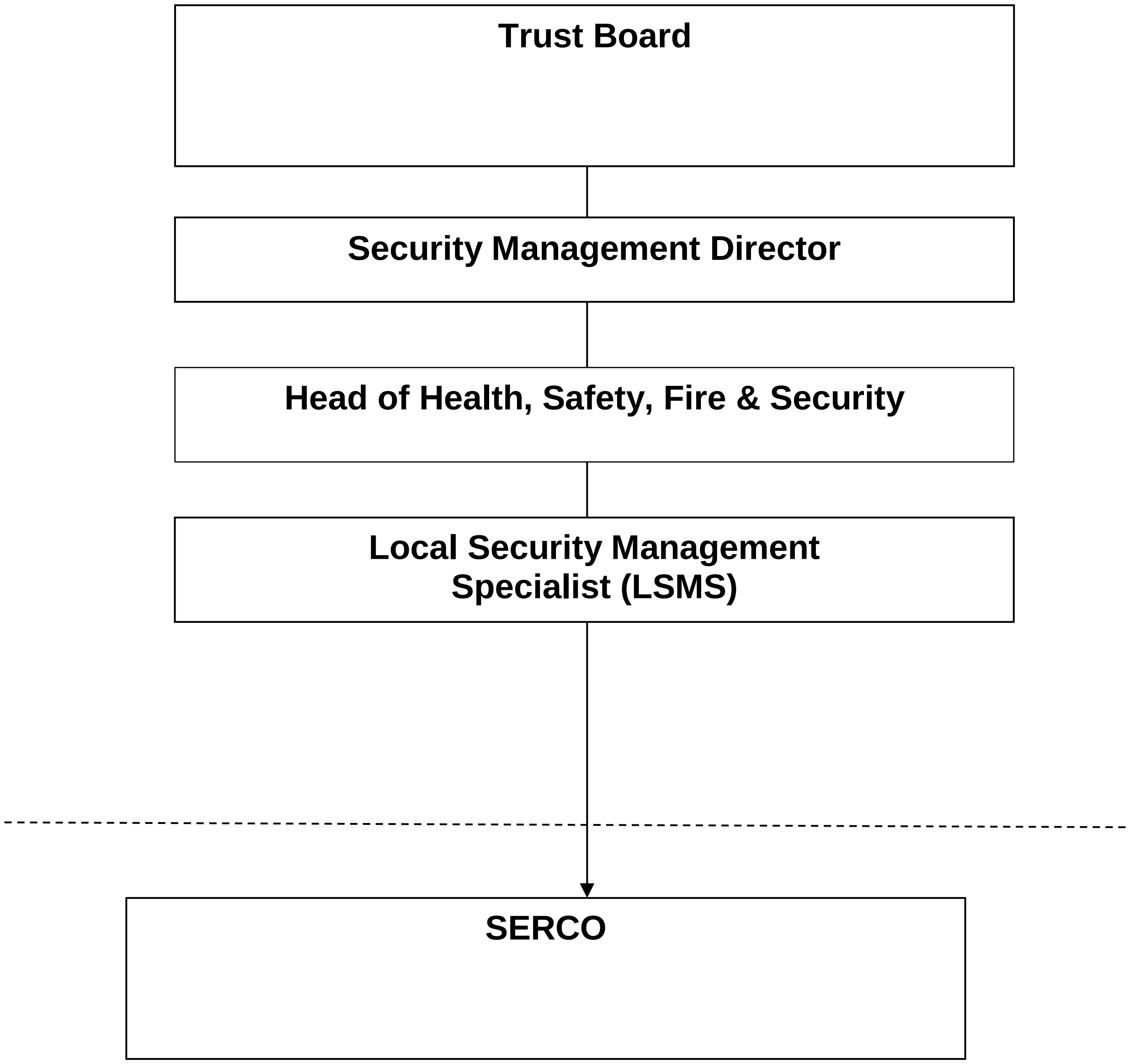
Also included within the provisions of the Theft Act are:

Section	13	Abstracting electricity without due authority
Section	15	Obtaining property by deception
Section	16	Obtaining pecuniary advantage by deception
Section	17	False accounting
Section	21	Blackmail
Section	22	Handling stolen goods

The Data Protection Act 2018 (Ref 19)

The Data Protection Act 2018 / GDPR covers both digital and manual information about living persons that can be accessed by reference to the individual. This is covered separately in the Data Security and Protection Policy (Ref 3).

Appendix C – Structure showing the Security Management Provision



Trust Board

Security Management Director

Head of Health, Safety, Fire & Security

Local Security Management Specialist (LSMS)

SERCO

Contracted Service GWH Site Only

Appendix D - Illicit Substances Procedure

Introduction

Under the Misuse of Drugs Act 1971 it is an offence to allow the Trust's premises to be used for the illegal supply or possession of any controlled drug or illicit substance.

Suspicion of Illicit Drugs being Used

There should be a good cause for suspicion e.g.: the smell of the drug being smoked or information given by other patients, visitors or employees.

Any suspicion should be reported first to Department Manager, then to the Trust LSMS.

Procedures at GWH Site

The Department Manager is responsible for making the decision to escalate the incident to the Security Department.

The Security Department are responsible for managing the incident and taking decisions about how to proceed in accordance with the Misuse of Drugs Act 1971 (Ref 30).

Security will offer the person under suspicion the choice of handing over any illicit substances in their possession to them for authorised disposal, or having the Police called to attend.

Unless the patient is present and has given permission, and another employees witnesses the procedure, it is illegal to search a patient or his/her property. This may be construed as an infringement of the patient's rights (and their confidentiality, including their right to privacy). A search of a person without that person's permission could lead to the searcher being charged with assault. Notification of permission to be searched should be recorded in the patient's clinical record.

This does not preclude nursing and medical employees from searching a patient in order to establish the possible causes of their medical condition, so that appropriate treatment may be administered, in accordance with standard clinical practice.

The reasons for the suspicion and the advice given to the patient should be recorded in the clinical record.

The patient should be advised that if drugs are subsequently found the procedure detailed below will be instigated.

Procedure at Community Sites

The Department Manager is responsible for making the decision to escalate the incident to the Police Department and reported to the Trust LSMS.

Confiscating Illegal Substances

Procedure at GWH Site

An employee who finds an illicit substance in the possession of a patient/visitor or has reasonable grounds to suspect the presence of an illicit substance must contact Security. The Security Department are responsible for managing the incident and taking decisions about how to proceed in accordance with the Misuse of Drugs Act 1971.

Small amount = for personal use follow this:

- Confiscate the suspected illicit substance and pass on to the ward co-ordinator for signing into the patient's own CD register. Illicit medicines should be held in the CD cupboard.
- Call the police If suspected to be an illicit substance and if the person refuses to hand it over.
- If illicit drugs are taken from a patient/visitor this confiscation must be verbally explained to them and recorded in patients notes and on an Incident Notificaiton Form.
- The substance should be sealed in an envelope and labelled "suspected illicit substance".
- Contact Pharmacy [Ward Pharmacy Bleep] at the earliest opportunity to arrange for collection and safe storage Hand over to pharmacy ward pharmacist who is to return to the pharmacy and write in to the 'ward stock for destruction register, number and store the suspected illicit substance in the quarantine basket'. This must be held in pharmacy for 30 days after possession then destroy in line with normal stock destruction (destruction must be witnessed by an authorised external witness as per CD policy)
- Employees do have the right to detain the person pending the arrival of the police, however this should only be done in circumstances where there is a clear and present danger to employees, visitors or other patients

Large Volume = more than for personal use

Call police and put in CD reg / cupboard until police arrive, then sign out and hand over to police.

Methadone Mixture

Methadone mixture will be treated as an illegal substance if it is not in the prescribed container with the correct patient details.

Procedure at Community Sites

An employee who finds an illegal substance in the possession of a patient/visitor, or has reasonable grounds to suspect the presence of an illicit substance, should contact the Police Department.

UNDER NO CIRCUMSTANCES MAY ANY SUSPECTED ILLICIT SUBSTANCE BE RETURNED TO THE PATIENT. ANY EMPLOYEE DOING SO COULD BE COMMITTING A CRIMINAL OFFENCE.

Appendix E - Protocol for Employees encountering any sort of weaponry/firearms in a Patient's Home

Firearms in a service-users home - What you should know

On occasion, community employees visiting service-users at home have reported the presence of firearms clearly visible in the home. This guidance will help you to take appropriate action in such circumstances.

The law regarding firearms is complex, but in simple terms:
A firearm, including a shotgun, is "a lethal barrelled weapon of any description from which any shot, bullet or other missile can be discharged”.

- It is offence to possess a firearm or shotgun without a certificate, which is issued by the police.
- It is also an offence to openly possess an imitation firearm in public, and these are defined as "anything which has the appearance of being a firearm (whether or not it is capable of discharging any shot, bullet or other missile").
- Under some circumstances antique weapons are also included, but guns that can be proved to be antiques can be possessed without a certificate.
- When on private premises there are no restrictions around the possession of air soft (paint ball), low powered air rifles / pistols and other imitation firearms (sometimes referred to as BB guns). It can be very difficult to tell realistic imitations apart from the “real thing” – if in doubt, treat as real.

A rifle is a Section 1 firearm for which a licence is required, with restrictions around possession of ammunition for firearms (generally bullets).
A shotgun is a Section 2 firearm for which a certificate is required, but there are generally no restrictions around the possession of shotgun ammunition (generally cartridges).
A pistol or revolver is a Section 5 prohibited weapon, and possession of these is generally unlawful, although some are held as part of a collection.
Any firearm or shotgun must be stored securely and in a way that has been approved by the police. The law says that they "must be stored securely at all times so as to prevent, so far as is reasonably practicable, access to the guns by unauthorised persons".
Broadly speaking, if you enter someone’s home you should not see any firearms or shotguns.
If they are lawfully present they be kept secure and ideally out of sight. Antiques should still be securely fixed to a wall or mantelpiece, but there is no such requirement for imitations, so it is important to bear in mind the difficulty in distinguishing the difference between real and imitation – if in doubt, treat as real.
You are not expected to be able to identify different types of firearm or whether they are lawfully held. If you see a firearm that is not safely stored away - first and foremost – keep yourself safe.
If you feel in any way threatened or fear for your own or another’s immediate safety - leave the premises and phone the police on 999.

If you do not perceive immediate danger discuss with your line manager and safeguarding lead as soon as possible. Remember that unsecured firearms, even if lawfully held, may be a serious risk to children who live in or visit the home. It may be necessary to carry out a risk assessment and report the matter to the police and other agencies.
Any incident involving a potential firearm needs to be treated with the utmost seriousness until we have assurance from the relevant authorities that our teams, the service-user and wider public are not at risk. For advice please contact your Security Management Specialist.