Security Policy

Department / Service:	Health and Safety
Originator:	Fiona Dwyer Local Security Management Specialist Julie Noble Head of Health & Safety
Accountable Director:	Scott Dickinson Director of Estates and Facilities
Approved by:	Health and Safety Committee
Approval Date:	15th August 2024
Review Date: **This is the most current document and should be used until a revised version is in place**	15th August 2027
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Purpose of this document:

Worcestershire Acute Hospitals NHS Trust (the Trust) is vulnerable to a number of threats including violence and aggression against another person, terrorism, unauthorised access, theft, burglary, criminal damage, fire and arson and the misuse of personal data and information.

This policy sets out the security objectives of the Trust to protect its sites and buildings and the personnel and property that they contain. Those objectives seek to provide a safe and secure environment for all staff, patients and visitors. This policy describes the process in place to manage security and provides guidance to staff in the prevention and management of security incidents on Trust premises.

Key amendments to this Document:

Date	Amendment	By:
July 11	Biennial review with changes to format and minor amendments due to changes in the Trust managerial structure	Paul Graham
July 12	Minor amendments made regarding managers duties and the risk assessment process to comply with NHSLA Standard	Paul Graham
Sept 12	Addition of Lockdown Plan as Appendix E	Paul Graham
June 13	Biennial review with minor changes	Paul Graham

June 14	Minor change to include use of mobile phone cameras	Paul Graham
Aug 16	Document extended for 12 months as per TMC paper approved on 22nd July 2015	TMC
June 18	Policy review with amendments made due to Governance structural changes and the decommissioning of NHS Protect	LSMS
Jan 20	Document extended for 12 months whilst in the process of appointing a new Health and Safety Manager.	Samantha Reid
February 2021	Document extended as per Trust agreement 11.02.2021	Niel Hodgekiss
June 21	Full review with reference to NHS standards for contract 2020/21 and changes to responsibilities	LSMS (CW Audits) H&S Manager
July2024	Full review with following additions: • Updated originator and director details • Update introduction as NHS Standards for Contract is no longer relevant. • Section 2 – Paragraph 1 & 2 new looking at scope. • Section 4 Definitions has been expanded, previously only Lockdown included • Section 5 – EMPR section updated • Section 6 – Security of People updated and security of property and premises combined • Updated name of V&A policy • Appendix A: QUICK GUIDE to REPORTING VIOLENCE AND AGGRESSION INCIDENTS – warning letters included • Appendix D: Suspect Package new • Removal of Lockdown cards	LSMS Fiona Dwyer and Head of H&S & Fire Safety Julie Noble

Contents page:

1. Introduction

Incidents of security breaches and offences of crime committed on hospital sites, divert valuable resources from their intended use of patient care and have a far-reaching effect on the ability of the NHS to meet the needs of the public. The Trust is vulnerable to a number of 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. Other recognised risks include:

- Violence and aggression against another person.
- Terrorism.
- Unauthorised access to secure areas.
- Areas left unsecure.
- Criminal Damage.
- Fire and Arson.
- Theft.
- Misuse of Information.
- Bribery.
- Corruption.
- Fraud

This list is not exhaustive.

2. Scope of Policy

This policy sets out the security objectives of the Trust which includes the protection of the Trust sites and its buildings, as well as the personnel and property they contain. The Trust is committed to providing an environment that is safe and secure for all staff, patients and visitors, which is essential to the provision of healthcare protecting them from violence and aggression, injury and accidents in line with statutory obligations. The Trust has robust systems and processes in place to manage security, it also provides guidance to all staff on the prevention and management of those incidents in the workplace.

Security is everyone's responsibility and as such the successful implementation of the policies and procedures referred to in this document will depend greatly on the manner in which individuals undertake their personal responsibilities and the way in which managers and senior employees enforce compliance.

In order to meet the requirements of the NHS Standards for Contract 2020/21 the Trust will strive to achieve the following objectives:

- to determine the size and cost of any existing security problem
- to provide protection to both staff and patients
- to provide protection of assets
- to determine priorities and establish a security conscious environment
- to identify problem areas and effect remedial action
- to protect the reputation of the Trust

The Trust Health and Safety Committee will ensure that an effective policy is introduced and maintained and in addition, will regularly monitor procedures to ensure that security and crime prevention initiatives designed to progress the policy meet the stated objectives.   A Trust security group will review and discuss operational security concerns and escalate to the H&S committee where not addressed.

Significant security risks will be identified via the normal risk assessment process and escalated to the Trust Leadership management Group who will where necessary inform the Board.

The Trust will ensure that contingency plans are established and implemented in the event of a security incident. Where necessary the Trust will initiate a lockdown procedure which will help to reduce the impact of any security incident (Refer to Lockdown plan / Evacuation and Shelter Plans (Emergency plans)

The Trust will not accept incidents of violence to members of staff and/or wilful damage to property. Notices to that effect will be displayed in work areas and appropriate action will be taken against the perpetrators of such acts. The Trust will endeavour to ensure that staff are provided with the appropriate skills to be able to effectively deal with site and/or personal security issues, as required.

Unauthorised possession, neglect or misuse of Trust property will warrant disciplinary action.

3. Audience

This policy applies to all staff in all work areas across the Trust. It will also apply to all contractors whilst working on site.
In the event of an infection outbreak, pandemic or major incident, the Trust recognises that it may not be possible to adhere to all aspects of this document. In such circumstances, staff should take advice from their manager and all possible action must be taken to maintain ongoing patient and staff safety.

4. Definitions

ALX	Alexandra Hospital, Redditch
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
KTC	Kidderminster Treatment Centre
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
Security Management	“The condition achieved when information, personnel, material, activities and installations are protected against accidental loss, theft, unauthorised disclosure and damage”.
Tailgaters	Accesses secure areas by following authorised personnel through the door
WRH	Worcester Royal Hospital

5. Responsibilities and Duties

5.1 Managing Director

The Managing Director has the ultimate management responsibility for security within the Trust, ensuring the Trust complies with security standards, direction and legislation and will ensure that the:

- Board, Directors and Executive Team understands and accepts its responsibilities and accountabilities for the implementation and monitoring of all relevant Security Policies.
- Requirements of security legislation are applied throughout the organisation.
- Matters of Health and Safety and Security are discussed and Monitored at Trust Board.
- Trust’s Policies and Codes of practice are observed.
- Appropriate resources are made available to meet these requirements.
- There is an identified Security Management Lead for the organisation.
- A qualified Security Management Specialist is employed by the organisation.

5.2 Director of Estates and Facilities

The Director of Estates and Facilities is the directorate lead for security management within the Trust. They will be accountable for overseeing all security matters, promoting a pro security culture and supporting the needs of the LSMS and in turn informing the Trust Board of any significant security risks.

5.3. Head of Health & Safety and Fire Safety

Operational responsibility for security is delegated by the Managing Director to the Head of Health & Safety and Fire Safety.

- The Head of Health & Safety and Fire Safety is responsible for ensuring that all aspects of security management are properly organised, co-ordinated and controlled and has nominated executive responsibilities for all aspects of security management matters, including the prevention of violence against NHS staff. They will ensure that: The board are informed of all relevant security matters that may have an impact on service delivery or the safety of employees.
- There is appropriate senior engagement throughout the divisions on all matters of security.
- Polices relating to security are fit for purpose and in line with current best practice and standards for Health, Safety and Security and will ensure that appropriate policies, procedures and controls are put in place to manage the risks.

5.4. Local Security Management Specialist (LSMS)

The Trust Local Security Management Specialists in conjunction with the Head of Health & Safety and Fire Safety are responsible for taking action in the following generic areas:

- Deterring offenders
- Preventing incidents
- Detecting incidents
- Investigating security incidents
- Progressing Sanctions against offenders
- Pursuing redress where appropriate

They will also be responsible for action in the following specific areas:

- Tackling violence
- Protecting property and assets
- Protecting paediatric and maternity units
- Protection of Drugs, prescription forms and hazardous materials

The LSMS will have responsibility for monitoring the Trust's security management of incidents and occurrences and the implementation of the requirements of this Policy along with:

- Strategic oversight for security management across the Trust.
- Carry out tasks to ensure compliance with the Violence Prevention and Reduction Standard.
- 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.
- Review all Datix entries categorised as Security and Violence and Aggression.
- Respond and investigate where appropriate instances of crime including physical assault, verbal abuse, theft and criminal damage.

The Trust with assistance from West Mercia Police will use legislation in pursuit of the prosecution of anyone who commits offences of assault on emergency workers as defined in the Assault against Emergency Workers Act 2018 and to utilise the powers of the Criminal Justice and Immigration Act offences of causing a nuisance on NHS Premises.

They will also be involved in dealing with security-related issues such as theft and criminal damage. On occasions, this may involve staff being suspected of such acts. It is important that where such suspicions or allegations involving staff occur that these are immediately referred to the LSMS for investigation, ahead of any disciplinary action that may be considered. It could be part of a wider problem, or the act may be so serious that a criminal prosecution may be required, along with action to recover any costs incurred by the health body.

The role of the LSMS does not extend to "staff on staff" issues, such as bullying or harassment. This is the responsibility of Trust's Chief People Officer.

5.5 Management duties

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. It is their responsibility to ensure:

- Correct policies, procedures and systems are in place.
- Any risks identified should be reported on an Incident Reporting Form or the local risk registers and escalated accordingly.

- Annual risk assessments are compiled, recorded on Datix and presented to the H&S committee.
- Arrange for safe custody of departmental keys.
- Keep records of those staff issued with keys in their ward/dept.
- Ensure setting of any security alarms fitted to protect the area.
- All staff wear visible Trust ID badges.
- Staff are aware of any security arrangements within the dept.
- Lone working risk assessments are carried for each member of lone working staff.
- Any change of Digi lock codes are carried out by Estates Team at ALX and KTC, and Equans at WRH.
- No additional keys for internal or external doors are cut, locks changed, Digi locks or alarm systems fitted without approval of the Estates and Facilities department at ALX and KTC, but by the PFI team at WRH.

5.6 Employee's duties

- Report breaches of security or any criminal act as soon as possible to their line manager.
- Report those incidents on the incident reporting system (Datix).
- Report any and all crime including physical assault, hate crime, theft and criminal damage to the police as soon as possible. This will enable necessary investigation to take place and capture any best evidence available.
- Protect and keep safe their own private property.
- Display their own Trust Identification and challenge anyone unknown or acting suspiciously (providing it is safe to do so).
- Ensure areas of work are secure when not in use.
- Follow Information Governance policy and keep from view any patient identifiable details, confidential information and unattended I.T. locked and secure.
- Not follow absconding patients who leave the Trust’s Hospital grounds.

5.7 ISS Security Department

The Security provider will maintain a 24/7 security presence on the Worcester Royal (WRH) and Alexandra Hospital sites to deal with security emergencies and carry out security functions. Qualified Security Industry Authority (SIA) licensed Security Officers will deliver a service in accordance with the Policies of the Trust and in compliance with ISS prepared working assignment instructions and the service level agreement (SLA). Functions include:

- Use of CCTV systems (at WRH).
- Maintain physical security measures and check infrastructure.
- Responding and dealing with reported security incidents in particular where there is a risk to staff from threatening or violent behaviour.
- Provide a visible presence as a deterrent to unlawful activity.

The Security Department can be contacted on Ext 39903 at WRH, Ext 44385 at ALX, at KTC Call porters
In the event of a serious incident or emergency, call Ext 2222.

5.8. Emergency Preparedness, Resilience and Response Team

This policy covers the day-to-day management of security and prevention of crime however there may be the rare occasion when (e.g. attempted act of Terrorism) with will result in the implementation of Lockdown processes. The Head of Emergency Preparedness, Resilience and Response will ensure there are emergency plans in place to cover such emergency reactive situations. The trust is a category one responder under the civil contingencies act 2004 (CCA 2004) as part of this the trust is an active member of the local resilience forum (LRF) including the risk assessment working group localising the national risk register 2023 edition. The trust has a comprehensive range of emergency policies and plans to support the management of incidents and recovery including business continuity plans at a department, directorate, divisional and corporate level. The trust emergency Planning resilience and response is assured on an annual basis with the NHSE core standards process in line with the NHSE EPRR framework of 2022.

6. Process

6.1 Identifying Security Risks

Managers will be responsible for carrying out risk assessments regarding the physical security of premises and other assets within their areas of responsibility using either the Personal Safety Risk Assessment Tool (Appendix F of the Management of Violence & Aggression Policy) or the Trusts Risk Assessment Template (refer to the Risk Management Policy). Risks identified as being low or moderate will be managed by the appropriate Divisional Team. Those identified as being particularly significant will be immediately escalated via the Management structure to the Trust Leadership Group who will consider the risk(s) and where reasonably practicable to do so support any necessary action.

The process of identifying security risks is a continuous process supported by incident reporting processes, feedback from teams and patients, audit and inspections and guidance from internal staff and external agencies.

Reports of significant risks will be monitored on a quarterly basis by the Trust Health and Safety Committee. These reports will provide the organisation with an overview of the risks associated with security. All security risks should be reviewed regularly or at any time if there has been a:

- Security incident.
- Change to security arrangements.
- Change to the security risk.

Where it is necessary to develop an action plan to effectively manage a risk these action plans will be drawn up by the local manager in consultation with staff and the LSMS.

6.2 Security Measures and Controls

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

- Physical measures. These are tangible objects installed and deployed to protect areas of business in particular to vulnerable areas.
- Security awareness and education. A vital aspect of security is to ensure that all staff, irrespective of status or professional position, understand the risks to the organisation and are aware of their responsibilities regarding security.
- Legislation, policy and procedures. These range from laws to Trust and departmental instructions and directives.

6.3 Security of People

The Trust will manage and mitigate security risks to employees, visitors and patients by ensuring adequate security is provided and:

- Adhering to the Violence Prevention Reduction and Management of Violence and Aggression Policy.
- Departmental risk assessments are completed and local arrangements for safety are agreed.
- Appropriate alerts and notifications are shared with employees about security risks, including terrorism.
- Adhering to Incident Response Plans.
- Providing all employees with photographic identification in the form of an ID card
- Developing a culture in which employees are able to challenge unknown people in their work area (as long as it is safe to do so) and deter tailgating.
- Compliance with the Lone Worker Policy and Guidance.
- Departments complete risk assessments for lone working where necessary and that there are locally agreed protocols for safe working.
- Providing adequate physical security (locks, key codes, electronic access control and management) to prevent entry to unauthorised visitors.
- Ensuring Digilock codes for restricted areas are only shared with authorised personnel.
- Ensuring Digilock codes are changed regularly (this should be scheduled) and when necessary following compromise of any code or change of use of the area/room.
- Ensuring compliance with the Child/Infant abduction and Missing Adult Patient Policy.
- Compliance with the Alcohol and Substance Misuse and Illicit Drugs Policies.
- Consideration of the guidance for those employees who encounter violence, aggression, weapons or firearms in the community.
- Training staff in conflict resolution (CR) to reduce the likelihood of assault. CR training is a mandatory requirement for all Trust employees.
- Promoting security awareness events throughout the organisation.
- Providing opportunity for Personal Safety training where required. Breakaway training can be requested through the Learning & Development Dept.
- Ensuring that body worn cameras are used by security officers and Trust staff (where applicable) when dealing with challenging behaviour and in high-risk areas of work.

Some high-risk areas/situations may include:

- Home visits to clients who are known to have aggressive tendencies.
- Working in health care premises when other staff are not usually present (Lone Working)
- Working with patients who have a history of aggressive behaviour against staff or who have the potential to display aggressive behaviour
- Patients who are intoxicated or under the influence of drugs.

6.4 Security of Property and Premises

The Trust will manage and minimise security risks to property by:

- Ensuring compliance with the Patient Property and Lost Property Policy.
- Limiting access to work areas to ensure that only those with authorisation can access the area or ward.
- Maintaining an Asset Register of expensive items and equipment and carrying out asset audits.
- Marking all I.T. equipment by the IT Department
- Utilising logging in/out processes for vulnerable assets.

- Use of Closed-Circuit Television (CCTV) as a prevention and detection measure.
- Encouraging staff to challenge and report unauthorised visitors or suspicious behaviour.
- Requiring all members of staff to wear their photographic identification at work.
- Ensuring physical security is effective in preventing entry to unauthorised visitors.
- Requiring Departments to report to the Health and Safety (H&S) committee any identified security hazards in the work area.
- Requiring Divisions to report quarterly to the Security Meeting any security risks.
- Working to the Trust's Medical Gas Policy.
- Developing a culture in which employees are able to challenge unknown people in their work area (as long as it is safe to do so) and deter tailgating.
- Providing, where possible, secure arrangements for storage of personal property.
- Drugs and Medicines to be stored in compliance with the Management of Medicines policy.
- Completing an annual review of the Fire Risk Assessment for all Trust sites to identify any significant fire/arson risks and agree arrangements to manage and minimise those risks.
- Ensuring the appropriate management of medical gases on site, working to the Medical Gas Policy.
- Stipulating 24/7 security response services (ISS) for WRH and ALX.

It is the responsibility of each member of staff to secure their personal property against loss.

6.5 Security of Information

The basic principle of document security is best summarised as "the need to know" in accordance with the recommendations of the Caldicott Committee (1997). This requires that the dissemination of classified information should be no wider than is needed for the efficient discharge of the business in hand and restricted to those who have authorised access. (Refer to the Code of Conduct in Respect of Confidentiality and the Information Security Policy) Any incidents relating to a breach in security of patient identifiable information must be referred to the Trust's Caldicott Guardian.

- The Trust will ensure that all staff comply with the Data Protection Act 2018, regarding the confidentiality of personal information and access to medical records. All Medical Records held in Trust premises will be securely stored in suitable areas. Access will be restricted to authorised personnel only.
- Staff are made aware of information security via the Information Governance Training Tool (IGTT).
- Patients will be reminded by staff that the use of mobile phones for recording video/audio footage or photographs in hospital premises without consent is strictly prohibited. Any breaches will be reported directly to the IG Manager.

6.6 Site Security

General site security is an issue for all staff and a general level of awareness is essential. Any untoward findings should be reported immediately to the manager responsible for the site and/or service.

- Under certain circumstances the Trust may need to consider a lockdown of premises in order to effectively control the movement and access of people around the Trust hospital sites.
- In certain areas of the Trust appropriately trained members of the Portering Team will be tasked with the role of responding to security incidents. They will offer support to the members of staff involved and assist in attempting to diffuse the situation. If the situation they are confronted with appears to be getting out of control or they feel that they are unable to

deal with it then they will immediately summon assistance from the local Police. (Refer to the Code of Practice for how to deal with incidents of violence and aggression please as documented within to the Violence Prevention Reduction and Management of Violence and Aggression Policy.

- All staff should ensure that their work areas are secured at the end of the working day (where applicable) and that departmental keys are held in a secure place at all times.
- The loss of any key(s) must be investigated and if not promptly found reported to the appropriate ward/departmental manager and to the appropriate Estates Department. It is important to avoid delay so as to ensure premises can be secured.
- The Estates Department will be responsible for the issue and holding of all spare keys associated with suited or security locks and on no account must replacements be cut without prior permission. The control of keys and their replacements in other areas is the responsibility of the local manager.
- Access to certain restricted areas is controlled via security locks. Access to these areas will be monitored and controlled by the manager designated responsible for the building. Security codes should be changed every 6 months or whenever it is felt that the code may have become compromised.
- All staff should be vigilant for unusual and unexplained packages. Any package discovered which cannot be identified should be reported immediately to a supervisor or line manager. Under no circumstances should a suspect package be handled. (See Suspect Package Appendix D for further details).
- All security incidents will be reported and recorded on the Trust's Incident Reporting System and forwarded, in the first instance, to your manager and then to the Trust's Local Security Management Specialist.

6.7. Involvement of Police

- In the event of theft or damage to Trust property, the line manager responsible for that particular building, ward or department will be responsible for informing the Police, if in the light of the circumstances, it is appropriate to do so.
- Where there is any suspicion of fraud the incident must be reported as soon as possible to the Director of Finance. They will decide, in conjunction with the Local Counter Fraud Officer, what action will be taken and whether to inform the Police.
- In the event of an assault the Police must be notified immediately by the person affected or a person authorised by the victim to do so. In parallel the incident must be Datixed. The LSMS will decide in conjunction with the Head of Health & Safety and Fire Safety, what action will be taken and whether any further investigation is required.

The Trust will cultivate good relationships with the local Police and in order to pursue the objectives of this policy will actively seek to prosecute any individual who wilfully damages Trust property or inflicts harm to any member of staff.

Where theft or damage is related to property belonging to other persons i.e. patients, visitors or contractors, than the victim needs to inform the Police who will normally be advised.

6.8. Patients Valuables/Cash

The Trust will not accept responsibility or liability for patients' property brought into hospital unless it is handed in for safe custody and a copy of an official patient's property receipt is obtained. For further information refer to the Trust's Standing Financial Instructions (Sec D, 28) and WAHT-CG-252 V6(2) Safe Keeping of Patient Monies and Personal Belongings Policy. All property accepted for safe custody must be placed in the ward security container or forwarded directly to the Cashier's Office. See Appendix C and D for instructions and procedures relating to patient's valuables/cash.

In the event of accidental damage by a member of staff to patient's property out in the community, i.e. in a patient's home, an Incident Report Form (Datix) should be completed giving full details of the damage caused and any action taken. The incident must be reported to the Director of Finance, as soon as possible.

6.9 Staff Property

All staff are responsible for the safe keeping of their own property. Any discovery of lost property or the loss of personal belongings must be reported immediately to your line manager. A Datix Incident Report Form must be completed for every loss/theft incident. A Loss/Damage Form must also be completed and forwarded via the line manager to the Finance Department where any claim for reimbursement will be assessed. (See SFI's, Sec D, 26) Please note that the Trust does not insure personal property.

6.10 Security of Drugs

Generally, the Pharmacy Departments will be the secure stock holding area for all drugs. Patient's drugs are the property of the patient and should be handled as any other personal belongings. During their stay in hospital patients will normally be supplied with drugs from the Pharmacy Department.

- The Registered Nurse in Charge of a ward or professionally qualified person in charge of a department such as an Operating Theatre, Radiology etc will be responsible for ensuring that all medicines are securely stored in appropriate containers.
- Midwives working out in the community now carry their own Prescription pads. Those individuals will be responsible for the security of such documents and for the safe storage of any drugs that they may carry with them.
- Medicine trolleys should be secured to a wall except during the medicine round. Keys to all medicine containers must be held on a separate ring from all other keys.
- Pharmacy boxes for the transportation of medicines must be secure at all times.

A Controlled Drug Register will be maintained for each stock of controlled drugs.

(Refer to Trust's relevant Medicines Policy (Policy on the Purchasing, Prescribing, Supply, Storage, Administration and Control of Medicines)

6.11 Trust Property

The Managing Director has overall responsibility for the maintenance of all Asset Registers. (See SFI's Sec D, 24)

- The Trust will maintain Asset Registers and will ensure the security of Assets, as per Standing Financial Instructions. All asset registers must be checked annually.
- Whilst each employee has a responsibility for the security of Trust property, it will be the responsibility of Directors and Senior Managers to apply such appropriate routine security

practices, in relation to Trust property, as may be determined by the Trust Board. (Refer to the Information Risk Management Policy)
- Any damage to the Trust's premises, vehicles and equipment, or any loss of equipment, stores or supplies must be reported by directors and employees, in accordance with the procedure for reporting losses.
- Where practicable, assets should be suitably marked as Trust property.

7. Reporting Security Incidents and Violence and Aggression

All incidents involving breaches of security and violence and aggression must be reported on the electronic incident reporting system - Datix. Any crime of assault, theft or criminal damage must also be reported to the police in the appropriate manner i.e. an emergency call on 999 for response or on the 101 reporting line.

All Datix reported incidents are reviewed by the LSMS and appropriate action considered. The Trust is firmly of the view that all those who work in or provide services to the NHS have the right to do so without fear of being subjected to unacceptable behaviour including violence, aggression or verbal abuse. Reports of violence and aggression will receive an appropriate response and may require further investigation by the LSMS.

Identified breaches of security will be notified to departments, allowing for an investigation to take place by the Department Manager with guidance and advice from the LSMS.

Trust employees working within sites not owned or controlled by the Trust must ensure that they understand the arrangements in place for their own safety and the safety of others and must comply with the site owners' security policies, procedures and/or guidelines.

8. Implementation Arrangements

This policy will be implemented by local managers in their respective areas of responsibility. The Trust's Head of Health & Safety and Fire Safety and LSMS will also ensure that the policy is implemented throughout all levels of the organisation.

The Security Policy will be made available on the Trust Intranet. It will also be communicated to managers and staff-side representatives via the Trust Health and Safety Committee.

The Trust will ensure that the appropriate members of staff are suitably trained in security measures particularly those associated with the management of violence and aggression as detailed in the Violence Prevention Reduction and Management of Violence an Aggression Policy. The specific training requirements are listed in the Trust's Mandatory Training Matrix.

All staff will be made aware of this policy via the Trust's local induction process.

9. Monitoring and compliance

Managers will be responsible for reviewing their own local security risk assessments and associated protocols and procedures.

The annual workplace health & safety risk assessment screening tool will also take into account security issues and will provide the Trust with a further overview report of the effectiveness of the security management system.

Section	Key Control	Evidence of compliance	Frequency	By whom	Reported to	Frequency
Sections 4.1 & 5	Security risks are considered as part of the annual workplace risk assessment	H&S Audit to check local records of assessments	Annually	LSMS	H&S Committee	Annually
Section 5.2	Local plan of action completed where there are outstanding risks	Records of action plans	As required	Local Manager	H&S Committee	Quarterly
Section 5	Reporting of any security related incidents	Datix record of incident	Quarterly	LSMS	H&S Committee	Quarterly

10. Policy Review

This policy will be reviewed as necessary by the Trust Health & Safety Committee every 3 years or more frequently, if indicated by any significant change.

11. References

References:

Health and Safety at Work, etc Act 1974	
Management of Health and Safety at Work Regulations 1999	
The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013	
Safety Representatives and Safety Committees Regulations 1977	
The Health and Safety (Consultation with Employees) Regulations 1996	
HSC 1999/226: Campaign to stop violence against staff working in the NHS – Zero tolerance zone	
HSC 1999/229 "Working Together, Securing a Quality Workforce for the NHS: Managing Violence, Accidents and Sickness Absence in the NHS.	
Risk Management Strategy	
Risk Assessment Policy	
Health and Safety Policy	
Incident Reporting Policy	

Violence Reduction Prevention and Management of Violence and Aggression Policy	
Lone Working Policy	
Medicines Policy	
Standing Financial Instructions (SFI's)	

12. Background

12.1 Equality requirements

An equality assessment has been performed. There are no equality issues presented by this policy.

12.2 Financial risk assessment

A financial risk assessment has been performed. Effecting change as a result of learning may have associated costs although these will be dealt with through individual business cases.

12.3 Consultation

The following were consulted in the production of the original policy:

- Chief People Officer
- Members of the Health and Safety Committee
- Members of the Trust Security Group
- Estates and Facilities Teams
- Pharmacy
- Finance
- Head of Emergency Preparedness, Resilience and Response

12.4 Approval process

The Trusts Key Document Approval Group will receive this policy for approval.

Changes to this document will be recorded and monitored in accordance with the Policy for Policies.

Appendix A: QUICK GUIDE to REPORTING VIOLENCE AND AGGRESSION INCIDENTS

Please refer to Violence Prevention Reduction and Management of Violence and Aggression Policy. Any person identified as being violent, aggressive or abusive, should be requested to refrain from such behaviour. If staff consider it an emergency then ring 2222 for security assistance at Worcester Royal and Alexandra Hospital, or for Porters at Kidderminster Treatment Centre, ring 0 for switchboard and bleep them on 3253.

Staff are reminded to challenge the behaviour by:

1. Addressing/Identifying the behaviour – “Please stop swearing/shouting/being abusive”
2. The reasons why – “Your language is degrading/rude/upsetting/threatening and making me feel unsafe/threatened/abused”

These steps are, on many occasions, what we fail to do at times of stress and vulnerability. Many situations can be defused if the culprit is informed of this at the time.

3. Inform them of the possible consequence of their continued behaviour – “If you continue to behave in this manner, I will be unable to deliver the care/service/answer your enquiry”
4. Staff will either then continue to deal with the person or state that they are withdrawing their service. “As you have continued to swear/shout/be abusive, I am not able to deal with you/your enquiry/your complaint”.
5. Call for support – “If your behaviour continues I will report this to our Security/Police”.

Staff are asked to record the circumstances on Datix as accurately and detailed as they can, within reason, including the name of the offender/culprit.
Quoting the language used may be difficult for some recipients to report, however it is imperative that the words used are recorded as evidence of the behaviour. When an offender/culprit is later reminded of the words they used it is very incisive, whether in a letter or possibly a court case.

Incidents of this nature should be reported on the Datix system. This enables the Trust to see the issues and be in a position to respond appropriately and proportionately.

Any crime including physical assault/theft/criminal damage should not only be reported on Datix but also reported to the police via the 101 system or the police report form online.

When completing the Datix report forms, it is important to be accurate with the Data. If there are any clinical issues such as brain injury trauma, dementia, delirium, alcohol or drug abuse, these conditions must be reported (under UNINTENTIONAL physical harm) and will be taken into consideration. Whether the assailant/offender has capacity is an important factor however capacity should be assumed until proven otherwise. If a complainant/victim wishes to have action taken against their abuser, a clinician will be asked to identify whether or not the assailant had capacity at the time. Whilst a lack of capacity does not prevent an assault being considered for investigation it may be mitigation in the circumstances.

Other parts of Datix are also important to complete. Entering the most accurate description of the incident whether security, restraint, anti-social behaviour etc. Also answering the questions, does the reporting person agree with Trust or police action being taken? Has the victim received conflict resolution training?

Outcomes

Operational Security guards / Porters will assist with many of these incidents in the initial stages, having been requested by a member of staff. If the abuser/aggressor is a patient, then the incident will be led by the clinician in charge and the outcome influenced by the clinician.
Staff should still report the incidents on Datix as the security team do not have access.
Events recorded as 'Security' or 'violence and aggression' on Datix, will be reviewed by the Security Management Specialist for the Trust.

A range of measures can be taken by NHS Trusts depending on the nature and severity of an incident, which may assist in the management of unacceptable behaviour by seeking to reduce the risks and demonstrate acceptable standards of behaviour, these may include:

- Verbal warnings
- Sanction Letters – Warning, Caution, Yellow and Red Card letters
- Acceptable Behaviour Agreement (ABA);
- Withholding treatment
- Civil injunctions, Community Protection Notice (CPN) or Criminal Behaviour Order (CBO)
- Civil prosecution

A Sanction Letter may be considered as an appropriate action and will be compiled and agreed with the investigating manager and the LSMS before being sent to an individual.

NB: Warning, Caution and Yellow Card Letters will be signed and sent by the LSMS (only). Red Card letters will be signed by the Managing Director or his deputy. See the Violence Prevention Reduce and Management of Violence and Aggression Policy to ensure compliance with issuing of sanctions.

Sanction Letters can be used in an attempt to control the behaviour of individuals when on hospital sites.

Although not pleasant, sometimes prosecution (Police) including caution, restorative justice or charge is the only way to endeavour to change behaviours. Injunctions or Non-molestation orders can be applied for to prevent "harassment, alarm, distress, nuisance and/or annoyance. Understandably used as the last option, the withdrawal of service or a change in the conditions of service/treatment delivery may be unavoidable.

Appendix B: QUICK GUIDE to REPORTING VIOLENCE AND AGGRESSION / SECURITY INCIDENTS IN THE COMMUNITY

Guidance for those employees who encounter Violence, Aggression, Weapons or Firearms in the Community.

✓ Don’t ask questions, try to observe as much detail as you can. Execute your exit strategy (professional excuse) as a priority.

✓ Once in a safe place (away from the property) call line manager/colleague/buddy to make them aware of the incident and to confirm you are in a safe place.

✓ As soon as practicable, contact the LSMS.

✓ Document in full and submit an incident reporting form (Datix).

✓ Consider putting an alert on any systems that can inform other employees of the hazard in the patient’s home. Discuss at team meetings and briefings to ensure colleagues are aware.

✓ Review any care plan immediately to protect employees from the hazard. Future visits may not be appropriate until all the highlighted risks are addressed.

✓ LSMS to liaise with the Police who will advise on any appropriate response they can take and future actions.

✓ Convene a meeting of the department team leader, the member of staff and the LSMS to discuss any appropriate action by the Trust and review any care plan for future treatment.

✓ In circumstances relating to firearms these should be reported immediately to the Police. The patient may then need to be informed of the need for compliance with legislation and license requirements and told to lock articles away (firearms, ammunition).

✓ The Lone working protocol should be discussed.

BE SAFE NOT SORRY

IF IN DOUBT, GET OUT!

INFORM OTHERS & REPORT IT

Appendix C: Security Risk Assessment

Department:	
Area:	
Location:	
Date of Assessment:	

PERSONAL PROPERTY & BUILDINGS	YES	NO	N/A	COMMENTS ACTION REQUIRED
Are appropriate locks fitted to all external doors and windows and where necessary internal doors?				
Are there lockable areas that provide for the safe storage of property and confidential material?				
Are locks fitted to office and equipment storage areas?				
Do all locks work adequately?				
Is there appropriate provision for the safe storage of staff belongings?				
Is there appropriate provision for the safe storage of patient property?				
Are local procedures for the safe storage of valuables in place in compliance with Trust Policy?				
Are staff aware of the procedures for the storage of patient's valuables?				

Is there a functioning burglar intruder alarm?				
Is there a safe?				
Does the area have any CCTV cameras in place?				
Are staff aware of how to report and record a security incident?				
Are all security incidents subject to formal local review?				
Where appropriate are amendments made to the directorate/Trust Risk Register following any security incident?				
Is there a procedure to ensure the safety of staff who work out of hours?				
Is any external lighting efficient and effective, providing adequate light for persons to safely enter and leave the premises while observing their surroundings?				

ACCESS	YES	NO	N/A	COMMENTS ACTION REQUIRED
Is there effective access control ensuring that security is maintained at all times and that staff and visitors are readily identifiable?				
Do all restricted areas have a secure physical barrier to prevent unauthorised people entering?				
Is there an effective procedure for the registration, security, monitoring and distribution of keys?				

Are keys kept in a secure/monitored location?				
Are keys issued against a Name, Date and Signature?				
Are keys checked a minimum of once per shift and at handover?				
Are the security codes for keypad door locks recorded and changed regularly?				
Are suitable procedures in place to ensure unidentified persons in restricted areas are challenged?				
Is there an effective procedure to record all persons present within the workplace?				

PROCEDURES	YES	NO	N/A	COMMENTS ACTION REQUIRED
Are staff aware of the procedure to follow when an incident occurs? (including how and who to call for help (2222))?				
Are staff reporting all incidents on the DATIX reporting system?				
Is the incident reporting system readily available to all staff?				
Is the department referring victims of violent or aggressive incidents to support counselling if required?				
If panic alarms are in place either fixed or personal, are staff aware of actions to take when the alarm sounds?				
If panic alarms are in place are they tested regularly?				

Does local practice ensure that people known to be violent/aggressive are identified? Is this covered by a local procedure?				
Are incidents of violence & aggression reviewed with those involved and the directorate management team?				
Where appropriate following any incident are amendments made to the directorate/Trust Risk Register?				

TRAINING	YES	NO	N/A	COMMENTS ACTION REQUIRED
Have the training needs been established for all staff?				
Is attendance of mandatory training monitored?				
Are all staff trained in Conflict Resolution?				
Are any staff trained in breakaway techniques?				

ENTRANCE & WAITING AREA	YES	NO	N/A	COMMENTS ACTION REQUIRED
Is the entrance monitored by CCTV?				
Is there sufficient seating for the number of people waiting?				
Are there sufficient, easily accessible and clearly marked facilities eg toilets, drinks machine for patients and visitors?				
Is there a system to ensure that facilities which are broken/out of order are reported and attended to promptly?				

Has a risk assessment taken place to identify potential hazards and where possible remove or secure objects which could be used as weapons?				

CLINICAL AREAS	YES	NO	N/A	COMMENTS ACTION REQUIRED
Is access controlled out of hours?				
Have all objects that could be used as a weapon been identified and actions taken to remove or secure them?				
Is the room and furniture organised to allow rapid escape if necessary?				
Is there a mechanism for communicating with other staff in an emergency (eg panic alarm)?				
Are local procedures in place to communicate and identify patients/service users who present an increased likelihood of violence to personnel?				

DIFFICULT & SENSITIVE DISCUSSIONS	YES	NO	N/A	COMMENTS ACTION REQUIRED
If difficult/sensitive issues need to be discussed, is there a private room/area for this?				
During difficult/sensitive discussions, is there a protocol for ensuring staff safety (eg escort, communication)?				

LONE WORKING	YES	NO	N/A	COMMENTS ACTION REQUIRED
Do you have any lone workers?				

Is the need for staff to work alone or in an isolated situation absolutely essential?				
Are additional measures in place to increase their security to an acceptable level (e.g. personal alarms locked doors, use of escorts, out of hour's arrangements)?				

COMMUNITY WORK	YES	NO	N/A	COMMENTS ACTION REQUIRED
Is there a system to ensure that managers are aware of the whereabouts of their community staff at all times?				
Is there a procedure informing managers/staff of the actions to be				
taken if there are concerns for the safety of staff in the community?				
Are there arrangements for additional staff to attend premises that have the potential for violence and aggression, or might pose other threats to personal security?				
Is there a system in place to alert staff to patients/relatives known to be violent or aggressive?				
Is there a protocol that allows for the service to be delivered on hospital premises where the identified risk of violence or aggression is too great to be provided in the community?				
Do staff have means of raising assistance whilst undertaking community work?				

HANDLING MONEY & VALUABLES	YES	NO	N/A	COMMENTS ACTION REQUIRED

Are procedures in place to ensure that the handling of money/valuables is kept to the minimum necessary?				
If handling of money/valuables is carried out regularly, is there a System to ensure the security and propriety of the system is in compliance with Trust policy?				

Assessor's Name (Block capitals)		**Assessor's Signature**		**Date**	
Managers Name (Block capitals)		**Manager's Signature**		**Date**	

Appendix D: SUSPECT PACKAGE

Physical Security Measures

The first line of defence against the common criminal may also deter and prevent the terrorist from gaining access to the Trust's premises. ALL staff should ensure that windows and doors are secured when work areas are not in use.

Access control is generally affected in the Trust's premises via personal identity badges. Please ensure that you wear these badges at ALL TIMES whilst at work. If you approach an individual who is not identifiable, then question his/her presence on site. Remember, be vigilant and report any persons acting suspiciously to your Supervisor/Line Manager.

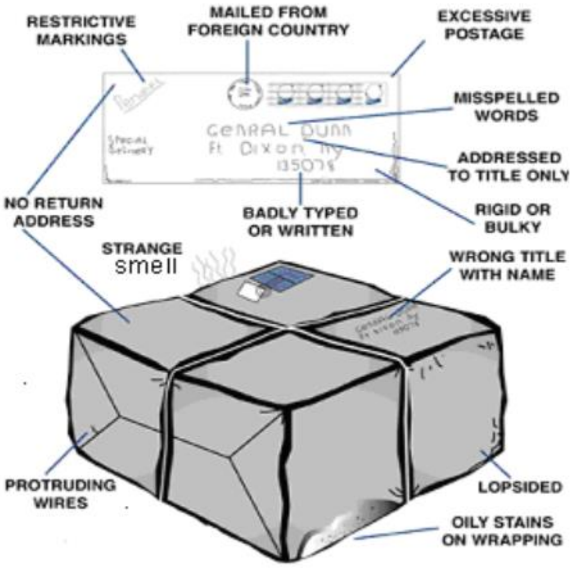
Procedure for Dealing with Suspicious Package or Letter

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 or 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: (Also see the diagram below).

Unexpected package or letter from an unknown source.	Badly Typed or Poorly Written
Mailed from a Foreign Country	Restrictive Delivery Markings
No Return Address	Excessive Postage
Lopsided/Protruding Item	Misspelled or Misused Words
Stains on Wrapping	Addressed to Title only
Wrong Title with Name	Rigid or Bulky
Possibly Oil stained or unusual Odour	Substance Leaking from the package



Examples of Dangerous Items that can be sent via Email.

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. Examples include but are not restricted to: explosives ('letter bombs'), chemical agents, radiological agents, biological agents (anthrax, botulism, other bacteria) and others such as illegal drugs.

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 SECURITY** or 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 or SECURITY ON SITE.**

SENIOR MANAGER / SECURITY ON SITE:

- Remember – No Radios or Mobile Phones near any suspect packages.
- **CONFIRM CONTACT** with the Police and stand by until relieved by them.

DO NOT handle any suspect package. Report its presence immediately to your Manager/supervisor or directly to the Estates Department via the Helpdesk. The person finding the object should be immediately available for interview by the police.

Responding to Incidents

The Local Security Management Specialist has the delegated responsibility for the day-to-day monitoring and co-ordination of security issues. They have both the responsibility and authorisation for implementing any security precautions necessary. In the event of the incident occurring outside of normal working hours then the Senior Manager on call will assume responsibility.

Staff must **NOT** speak to the media about incidents but pass all enquiries through to the Chief Executive's Office.

Welfare and counselling will be available to staff after any incident.

Good housekeeping will help reduce the areas in which a bomb or suspect package can be easily left undetected. Ensure that ALL work areas are kept litter free.

Appendix E: CHECKLIST RECEIPT OF BOMB THREAT

Whilst not common Switchboard operators most frequently will have to deal with telephone bomb warnings over the telephone; however, any member of staff may be confronted by such a message. The threat may also be received via email or a social media application. In these incidents:

- Do not reply to, forward or delete the message.
- Note the sender's email address or username/user ID for social media applications.
- Preserve all web log files for your organisation to help the police investigation (as a guide, police will require data from 7 days prior to the threat message and 48 hours after).

Any member of staff receiving a telephone threat call should Keep calm and Try to obtain as much information as possible from the call

LISTEN CAREFULLY!

Record the **EXACT** wording of the threat:
....
....
....

Was a 'Code-Word' given? .... Exact 'Code-Word was ....

(THIS DETAIL IS A CONFIDENTIAL MATTER IT MUST NOT BE FURTHER RECORDED OR REPEATED)

If possible ask **These** Questions:
Where is the bomb situated? ....

When is it due to explode? ....

What does the bomb look like? ....

What kind of bomb is it? ....

What will cause it to explode? ....

Did you place the bomb? .... Why? ....

Where are you calling from? Mobile ………................. Private Line ……………..........

What is your telephone number? ....

What is your name? ....

What is your address? ....

Time call completed: ....

Keep the telephone line open (even if the caller has disengaged). Do not use any facility on the telephone (i.e. call back) until Police have arrived.
If your telephone has Automatic Number Reveal note down the number ....

Using a separate telephone line........

NOW CONTACT THE POLICE USING 999 IMMEDIATELY
Once the Police and your immediate Supervisor/Manager has been informed please complete the questionnaire overleaf:

Time and Date of call .... Length of call ....

Your telephone number (that which the call came in on) ....
About the caller:

Male/Female
Caller's Age Group: Child. Youth. 20-30. 30-40. 40-50. 50-60. Elderly.

Language used:
Well spoken
Poorly Educated
Spontaneous
Foul
Taped
Incoherent

Callers voice:
Calm
Emotional
Deep
Angry
Stutter
Soft
Rational
Slow
Hostile
Deliberate
Rapid
Drunk

What accent? ....

Was the voice familiar? .... Who did it sound like? ....

Background sounds:
Traffic
Other voices
Music
Machinery

PA System
Static / Clear
Any other remarks ....
Your details:

Signature .... Print Name ....

Ward/Department ....

GIVE THIS CHECKLIST TO THE POLICE

Search Plan

The Local Security Management Specialist/Senior Manager on duty (or on call) or another designated manager may initiate a search. If a blanket search is required then individual areas within the hospital will be asked to conduct rapid searches, in order to eliminate them. Searchers should be looking for unidentified objects(s):

- that should not be there.
- that cannot be accounted for.
- that are out of place.

If a suspicious object is found then follow the golden rules:

- **DO NOT TOUCH OR MOVE THE OBJECT.**
- If possible leave a distinctive marker near (not touching) the device.
- Move away from the device to a designated control point.
- Inform search leader.
- The search leader should implement the evacuation plan, if required.
- Stay at the control point and draw an accurate plan of the location of the suspicious package or device.

In all cases where a bomb threat is received, the police should be informed immediately and kept advised as to what action is being taken.

Evacuation

The decision to evacuate premises will be taken by the search leader usually in consultation with the police. Evacuation will follow one of two patterns, either as quickly as possible using all available exits or via alternative route so that people can leave the building without being placed in danger by passing too close to the suspect device. Once an evacuation has been completed, the search leader will at some stage have to decide when the building can be reoccupied. Of course, where a suspect object has been found, the police (if not already present) will attend and assume control until the object is declared safe. Thereafter, control will revert to the search leader.

Recovery

Immediately following an incident staff and visitors must be prepared for a certain amount of disruption particularly in gaining access back into affected areas. Police may remain in situ and may well ask for identification prior to access. If a cordon is in place the police will ensure the security of premises within it. Once the cordon is lifted the responsibility reverts to the Trust and to the search leader/Senior Manager.

Remember all information obtained remains confidential.

Appendix F: INSTRUCTIONS AND PROCEDURES TO BE FOLLOWED FOR THE CARE OF VALUABLES AND CASH BELONGING TO PATIENTS.

1. It is the responsibility of the member of staff admitting the patient to inquire if they have any valuables with them.

2. Patients possessing valuables should be encouraged to get relatives to take the items home or to place them in safe custody with the member of staff.

3. If a patient insists that they wish to keep the property with them during their stay then that patient must be made aware of the fact that the management of the Trust will not accept any responsibility for the loss of such items. Disclaimer notices will be displayed worded as follows:

DISCLAIMER NOTICE:

> *'The Trust will not accept responsibility or liability for patient's property brought into Health Service premises, unless it is handed in for safe custody and a copy of an official patient's property record is obtained as a receipt'.*

4. The patient should also be asked to sign a disclaimer form, which should be witnessed by a senior member of staff. On completion this form should be retained in the patient's medical notes.

5. When receiving items for safe keeping the member of staff admitting the patient should itemise the valuables in a record i.e. the Custody of Patients Property (CPP) Sheet, with a second member of staff as a witness. Both members of staff and, if possible, the patient should sign the entry in the record.

6. CCP sheets are provided in a three-part NCR Book and each copy is noted as to whom it should be held by.

7. Cash and valuables must be kept in a secure place locally until they can be handed over to the official custodian.

8. In the case of patients who are unconscious, confused or under the influence of drugs or alcohol, their valuables should be removed and secured until they are in a position to have them returned. The senior member of staff at the time should ensure that details are recorded and witnessed, as above.

9. The official custodian or his/her representative will return valuables to the patient. Arrangements must be made for patients discharged outside of normal working hours or weekends.

10. Valuables must not be handed over to relatives unless written authority has been given by the official custodian.

11. When temporary custody of valuables occurs during such procedures as x-ray, minor operation etc, a member of staff (two members of staff if patient is unconscious, confused or under the influence of drugs or alcohol) should record and itemise the valuables. (A single sheet similar in design to the CPP sheet should be used and held in the department) Both members of staff should sign the record and again, if possible, the signature of the patient should be obtained. The patient should sign the receipt section of the record when the property is returned, and it should again be witnessed and signed by two members of staff.

12. Staff in outpatients' departments should not normally accept custody of patient's property. If a problem arises the manager should be informed so that arrangements may be made for the temporary custody of patient's valuables.

13. Dentures are normally the responsibility of the patient. However, if they are unable to care for them then a note must be made in the property record. (A single sheet similar in design to the CPP sheet should be used and held in the department) The dentures should then ideally be placed in safekeeping in a container clearly marked with the patient's name.

14. In the following circumstances patient's clothing will be itemised in a property record (as above) at the point in time:

- emergency admissions
- admissions of all children under 14 years, if unaccompanied by a parent or adult
- all internal and external transfers
- admissions of any confused or disorientated patient
- admissions of any unconscious patient
- any clothing received for custody and retained in wardrobes
- deceased patients

15. In the event of a death, clothing should be recorded by two members of staff who should place the articles into special cream plastic bags and attach a serial numbered property identification label to each one. All valuables should be listed on the CPP sheet, and any outstanding valuables not already accounted for should be included. The cash and valuables should be handed to the official custodian. The deceased's cash and valuables should only be surrendered to the next of kin on the written authority of the manager who has the responsibility for ensuring that it is done in strict accordance with instructions from the DOH concerning matters of probate. In no circumstances should staff hand over cash or valuables to other relatives or friends of the deceased person.

16. When a patient is being transferred, all miscellaneous property and clothing should be listed in the property record with a copy of the entry forwarded to the next person in charge, receiving the patient. If cash or valuables are held, then the official custodian should be informed of the transfer and arrange for the safe transfer of items. If the member of staff escorting the patient delivers any cash or valuables, he or she must obtain a receipt from the receiving unit. The receipt should then be returned to the official custodian of the original unit.

Herefordshire & Worcestershire STP - Equality Impact Assessment (EIA) Form
Please read EIA guidelines when completing this form

Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust	x	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

Name of Lead for Activity	Julie Noble

Details of individuals completing this assessment	**Name**	**Job title**	**e-mail contact**
	Fiona Dwyer	**Local Security Management Specialist**	Fiona.dwyer@nhs.net
Date assessment completed	5th June 2024		

Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	**Title:** Policy
What is the aim, purpose and/or intended outcomes of this Activity?	Ensure compliance

Who will be affected by the development & implementation of this activity?	□ x □ x	Service User Patient Carers Visitors	x □ □ □	Staff Communities Other ____________________
Is this:	X Review of an existing activity □ New activity □ Planning to withdraw or reduce a service, activity or presence?			
What information and evidence have you reviewed to help inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.				
Summary of engagement or consultation undertaken (e.g. who and how have you engaged with, or why do you believe this is not required)				
Summary of relevant findings				

Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group and explain your rationale**. Please note it is possible for the potential impact to be both positive and negative within the same equality group and this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	**Potential positive impact**	**Potential neutral impact**	**Potential negative impact**	**Please explain your reasons for any potential positive, neutral or negative impact identified**
Age		x		
Disability		x		
Gender Reassignment		x		
Marriage & Civil Partnerships		x		
Pregnancy & Maternity		x		

Race including Traveling Communities		x		
Religion & Belief		x		
Sex		x		
Sexual Orientation		x		
Equality Group	**Potential <u>positive</u> impact**	**Potential <u>neutral</u> impact**	**Potential <u>negative</u> impact**	**Please explain your reasons for any potential positive, neutral or negative impact identified**
Other Vulnerable and Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)		x		
Health Inequalities (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		x		

<u>Section 4</u>

What actions will you take to mitigate any potential negative impacts?	**Risk identified**	**Actions required to reduce / eliminate negative impact**	**Who will lead on the action?**	**Timeframe**
		.		
How will you monitor these actions?	**Regular monitoring of incidents**			

When will you review this EIA? (e.g in a service redesign, this EIA should be revisited regularly throughout the design & implementation)	**Next policy review**

Section 5 - Please read and agree to the following Equality Statement

1. Equality Statement

1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on the 9 protected characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation

1.2. Our Organisations will challenge discrimination, promote equality, respect human rights, and aims to design and implement services, policies and measures that meet the diverse needs of our service, and population, ensuring that none are placed at a disadvantage over others.

1.3. All staff are expected to deliver services and provide services and care in a manner which respects the individuality of service users, patients, carer's etc, and as such treat them and members of the workforce respectfully, paying due regard to the 9 protected characteristics.

Signature of person completing EIA	MDwyer
Date signed	5th June 2024
Comments:	
Signature of person the Leader Person for this activity	MDwyer
Date signed	5th June 2024
Comments:	

Supporting Document 2

Financial Risk Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	**Yes/No**
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments: Topical negative pressure or Vacuumed Assisted Closure has been used within the Trust for many years. Implementation of the guideline should contribute to ensuring cost-effective use	N/A

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the appropriate Operational Director before progressing to the relevant committee for approval