SECURITY POLICY

Version Number	4.4	Version Date	March 2018
Policy Owner	Chief Financial and Commercial Officer		
Author	Fire, Health & Safety Manager		
First approval or date last reviewed	Aug 2009, October 2011(Version 4); October 2017 reviewed and updated version in December 17 included links around Restraint outlined in the Interventions policy (section 4.8). Reviewed at the Patient Safety Steering Group March 2018 including Body Worn Video.		
Staff/Groups Consulted	Security Committee Health and Safety Committee Local Security Management Specialist Trust Risk Manager Heads of Departments Chief Pharmacist IT Officer		
Approved by Security Committee	October 2011, Version 4.3 Approved last in Oct 2017 and May 2018 for version 4.4		
Next Review Due	March 2021		
Equality Impact Assessment Completed	March 2018		

Table of Contents

1. RATIONALE

Security on the Yeovil District Hospital NHS Foundation Trust sites including wholly owned subsidiaries and joint ventures premises affects both staff, patients, visitors and property. Striking the right balance between security, safety and patient care is achievable through measures taken in line with the security standards. Alongside the Security policy will be a number of operating procedures designed to enhance this policy to provide guidance to staff and direction in maintaining safe and secure premises.

2. POLICY STATEMENT

The purpose of the Security Policy is to establish and maintain robust structures and processes to manage the security of patients, visitors, staff, premises and assets. The Trust acknowledges that it has a duty of care to ensure the security and safety of its staff, patients and visitors and will achieve this with the provision of safeguards to protect its property and the safety of those who work in and use its premises. This includes the right of staff and others to work in a safe & respectful environment without fear of violence, aggression, abuse or harassment from patients & relatives.

Crime reduction through anticipating risks and taking action to remove, reduce or transfer them will be the focus of the security management team working alongside external agencies as necessary. Adopting a pro-security culture the Trust follows the NHS Security standards for commissioners, security management as part of the NHS Standard Contract under the following headings:

- Strategic Governance
- Inform and Involve
- Prevent and Deter
- Hold to Account

3. APPLICABILITY

This Policy applies to all permanent and temporary staff, and Contractors employed by Yeovil District Hospital NHS Foundation Trust, Simply Serve Ltd and Day Case UK. Failure to follow this policy by staff may result in action under either the disciplinary or capability policies. Other persons may be subject to other action by the Trust.

4. POLICY PROVISIONS

4.1 Risk Assessment

Risk assessment related to security risks will be identified through proactive work of audits and inspections carried out by the Local Security Management Specialist (LSMS) in coordination with key stakeholders and managers of departments. Ultimately risk assessment is the responsibility of the department manager and the risk register should be

used to record risks and mitigating actions in line with the Risk Management Policy adopting the 5 steps to risk assessment approach.

4.1.1 Risk Assessment monitoring

The LSMS will maintain an overall central register of security risks assessments conducted and actions identified and progress on implementation. A report will be submitted to the Security Committee on a quarterly basis with actions in place. Progress on actions to mitigate risk will be monitored by the committee using these quarterly reports.

4.2 Incident Reporting

All Trust staff are to report security incidents including violence and aggression incidents in line with the Incident Reporting and management policy. Utilising data from incidents allows the LSMS and managers to monitor trends for risks, thereby identifying intervention and prioritisation.

Investigations will be carried out by the LSMS which will be reported back through the appropriate management teams and committees with findings.

Security incident reporting and trends are to be reviewed through Security Committee with the LSMS action plan identifying and documenting areas of improvement aimed at minimising risk.

4.3 Major Incidents, Contingency Planning and Lockdown Procedure

The Trust has a Major Incident Response Plan and a Business Continuity Policy. As part of these plans the Trust is required to have a Lockdown Risk Profile and procedures in place. A lockdown may be required in response to a specific incident, or as a proactive measure in response to receiving specific intelligence data, for example in connection with a terrorist threat.

A lockdown is achieved when access/egress into a department or building is controlled and restricted, this is achieved through a combination of physical security measures and the deployment of security personnel. The lockdown procedures on the YDH Intranet should be referred to for further detail for YDH.

4.4 Security Management

The Security Management will be managed through the Estates and Facilities management structure under Simply Serve Ltd (SSL) who will ensure arrangements are in place for the security of persons, premises and assets at all times. A 24/7 physical security guarding presence will be maintained on the main YDH site whilst appropriate security measures will

be managed on other sites. The effectiveness and value of these arrangements will be subject to review by the Security Committee.

In addition to this, Estates and Facilities will provide a specialised management service to the Trust that will include the following:

- The effective management of CCTV & Body Worn Video (BWV) (and other technical security methods) in accordance with current legislation and best practice.
- The delivery of security awareness training to all staff as part of the Induction and Mandatory Training programme.
- Investigating and reporting on criminal activities throughout the Trust.
- Providing advice and guidance on security matters and lone working.
- Assessing security risks within departments and wards, and producing Security Risk Assessments, and action plans to mitigate the risks.
- Liaising with local police on crime reduction measures and with other relevant agencies on security/policing matters.
- Conducting security visits and inspections to review department security to support risk assessment findings.

4.5 Closed Circuit Television (CCTV) and Body Worn Video (BWV)

The overall purpose of CCTV schemes is to help reduce the fear of crime for the Trust staff and service users / carers (particularly those who are entering and leaving the Trust premises during the hours of darkness) and to protect the Trust premises from criminal activities. CCTV will be used:

- To assist in the prevention and detection of crime against both persons and property.
- To facilitate the identification, apprehension and prosecution of offenders in relation to crime.
- To ensure the security of property belonging to Trust and to employees and visitors of the Trust.

The CCTV code of practice provides further information on the use and safeguarding information in line with the Data Protection Act.

4.5.1 Body worn video cameras will be used on YDH premises managed by Simply Serve Ltd (SSL), worn by security guards employed by SSL. The use of BWV cameras is in line with the CCTV & Surveillance Systems Code of Practice. The use of BWV is to deter and to protect staff and services users from acts of violence and aggression and will be used as evidence for prosecution purposes. There is no intention to use BWV on Symphony Healthcare sites.

4.6 Bomb Threats (Improvised Explosive Devices (IEDs)) and Suspicious Packages

In the event of a threat to the hospital buildings and persons through receiving a warning, or through the identification of a suspicious package or vehicle, IED, the Trust will respond following the procedures detailed in the **Bomb Threat / Suspicious Package procedures**. Initial assessment is to be made by the security team to validate information following the flowchart in the procedures in order to identify the nature and threat before reporting the situation to the Police. This process is not intended to deter from calling the police but aims to implement checks that highlights the risk level to avoid disruption of services.

Initial assessment may take the form of validating the nature of threat, taking details from telephone calls, or messages received. Identifying suspicious activity through reporting to the security team and using a combination of CCTV and confirmation checks on any article, bags or other suspicious packages received.

4.7 Access Control and Identity Badges

All managers are responsible for ensuring staff are authorised to access areas of the building in line with their job role. Members of staff and all contractors are to display their identity badge at all times when on duty, staff should refer to the dress and appearance section of the Yeovil District Hospital and Simply Serve Ltd HR Manual for information. Lost identification badges should be reported using the incident reporting system. HR and Facilities must be informed as soon as possible to cancel / suspend security access to restricted areas which have electronic door control access systems fitted.

Contractor access is detailed in the Estates and Facilities Contractors Induction and procedural document. This document is to be provided to all contractors who are responsible for compliance with their sub-contractors. All contractors working on Trust buildings and premises are to book in and out through EFM with allocation of ID badges.

Challenge Culture: Staff require to challenge people who are entering restricted areas, for example ask them for identification, or if they can assist them if they are lost. If staff have any concerns or suspicions about any person’s behaviour they are to contact security immediately. All staff members are responsible for the collective security of everyone at the Trust.

Electronic access systems are managed through Facilities. ID badge security access application can be found on YCloud (trust Intranet) under the Security site.

Access control to areas of the building is also managed under the Trust lockdown procedures (Sect 4.3) to isolate areas and secure departments for security purposes. This is carried out through a combination of physical locks and electronic locking systems.

4.8 Safeguarding Patients

4.8.1 Restricting Physical Access

Restrictions on access to patient areas and hazardous areas will be implemented as necessary whether permanent or temporary to safeguard the patients on the ward and protect patients when wandering. Arrangements and options for restricting access are included in the Protecting Wandering Patients policy. The Missing Persons procedure provides guidance on assessing the risk level and decision making processes when escalating risk and communicating internally and with external authorities i.e. Police.

4.8.2 Physical Restraint

Staff including security guards may assist to restrain patients for their safety on request of the Ward Manager and/or Matron and Clinical Site Manager in line with the Safeguarding Policy on Restrictive Interventions.

The Mental Capacity Act allows restrictions and restraint to be used in a patient clinical support situation, but only if they are in the best interests of a person who lacks capacity to make the decision themselves. All incidents of restraint are to be reported in line with the Incident Reporting and Management policy.

4.8.3 Assessing Safety of Patient Environments for Ligatures

Specific risk assessment following the 'Manchester Ligature Audit Tool' guidance should be carried out in departments that have inpatient facilities for patients who have Mental Health conditions, and/or who may present as a suicide risk. When placing patients assessed as at risk of suicide, or may cause harm to themselves or others then steps should be taken by the clinical team to make the environment as safe as possible. The Ligature and Patient Safety Environment Risk Management procedures should be followed.

4.9 Staff Property

Staff should be aware that the Trust cannot accept liability for loss or damage to staff property brought onto its premises, this includes vehicles and other forms of transport. Reasonable arrangements for staff to secure personal items in lockers etc. are available, but not necessarily directly in their work area. Where there are hygiene and infection control standards to be applied for changing uniform or work clothes, lockers and secure facilities may be provided.

Staff property brought onto trust premises should not introduce hazards that affect safety, i.e. introducing incompatible electrical charging equipment for mobile phones and other devices. Smoking materials and e-cigarette (vape devices), refills and any other hazardous substances should be stored securely if brought on site. The Smoke Free Policy identifies the YDH site is smoke free.

4.10 Trust Property

Staff should undertake to take all responsible steps to ensure that Trust property under their control remains secure and where appropriate the items are to be placed on the Asset register in line with Standing Financial Instructions (SFIs) for capital purchases. Other asset registers held by departments are the responsibility of the Head of Service and local manager to maintain up to date.

4.11 Patients Property

Patients being admitted should be discouraged from bringing in valuables with them. Patient property is managed in line with the Patient Property policy with a system of recording and securing of valuables following the policy procedures. Property brought onto trust premises is ultimately the responsibility of the owner.

4.12 Violence to Staff

The Prevention and Management of Violence, Aggression and Abuse in the workplace procedures outlines the arrangements to minimise risk, gives general guidance and advises on reporting procedures. Violence against staff in the workplace from patients and visitors is covered in these procedures. Provision of Conflict Resolution Training (CRT) for staff is a key part of making staff aware of how to reduce threats and prevent escalation of situations. This provision will be focussed on higher risk groups of staff in clinical areas.

4.13 Removal of Persons from Trust Premises

Trespass is a civil offence committed when somebody enters property where he/she has no right to be and refuses to leave when requested to do so by the owner, or his/her representative. In law, if a trespasser refuses to leave the property when asked, the owner/representative is entitled to use ‘reasonable force’ to evict him/her.

‘Reasonable Force’ in Common Law

No attempt should be made to remove a trespasser unless he/she has first been asked to leave and has been given to do so. If he/she then refuses to leave voluntarily, ‘reasonable force’ may be used. What would count as ‘reasonable force’ is dependent upon the circumstances and unique to the situation but essentially requires deploying the absolute minimum force necessary. Any violence over and above what is absolutely necessary could leave the individual liable to prosecution for assault

4.14 Medicines Security

Detailed guidance on the security of medicines is covered in the Medicines Management Policy.

4.15 Information Security

Security of IT and patient records are included in the Information Governance policies. Access to IT is managed through the systems and procedures of HR and IT not detailed here.

4.16 Lone Working

Lone workers may be at risk due to their work routine, equipment used, isolation, or location of work. Lone working can be defined as any situation in which someone works without a colleague nearby, or when someone is working out of sight or earshot of a colleague. The Lone Working procedures identify the risk assessment approach and arrangements for identifying appropriate controls.

4.17 Training

All staff joining the Trust are required to attend Induction and regular mandatory training. This training includes Security and Conflict Resolution awareness.

For all areas where the risk assessment process has identified a greater risk of conflict occurring staff are required to attend Conflict Resolution Training which follows the NHS Protect National Syllabus. Courses are arranged through the Yeovil Academy.

Specific security awareness training will be provided through the LSMS as training needs are identified.

5. ASSOCIATED PROCEDURES

Links with other Trust policies and procedures relating to aspects of security are made in this policy to accurately reflect the aim of maintaining secure premises, safe and secure areas for patients safeguarding and providing safe and secure environments for all. The Major Incident Plan details the processes that are followed when an external or internal major incident is declared. A security incident may lead to a major incident being declared. The Major Incident Plan can be accessed on the Trust's intranet site.

6. IMPLEMENTATION, MONITORING AND EVALUATION

Responsibility for implementation, monitoring and evaluation is identified in the Trust's Policy on Procedural Documents. The policy will be monitored by the Security Committee who will review all incidents and actions resulting from the incidents, review security risk assessments including lone worker arrangements and monitor the completion of the required actions to mitigate risk through annual audit by the LSMS. The audit will include the review of arrangements put in place to manage physical security, premises and assets, including the risk assessments for the prevention and management of violence and aggression. The Security Committee will receive quarterly reports from the LSMS with the key findings and recommendations.

7. DEFINITIONS

7.1 NHS Protect

NHS Protect leads on work to protect NHS staff and resources from crime, dealing with a wide range of issues, including violence against NHS staff and theft of NHS property. It is part of the NHS Business Services Authority. **Note**: At the time of publishing (Oct 2017) NHS Protect may be superseded with other organisation of arrangements for Security (refer to NHS England).

7.2 Lockdown

Lockdown is the process of controlling the movement and access – both entry and exit – of people to all or part of the premises in response to an identified risk, threat or hazard that might impact upon the security of patients, staff and assets or indeed the capacity of that facility to continue to operate.

7.3 Lockdown risk profile

A Lockdown Risk Profile is a risk assessment of each site to determine its potential vulnerability to threat and its capability of either partial or full lockdown.

7.4 Bomb (Improvised Explosive Devices)

For the purposes of this policy these two terms are synonymous and refer to any actual or suspected explosive device. The popular term Bomb will be used in this policy.

7.5 Security Incident

Circumstance is which some or all of the processes referred to in this policy are activated to protect those present or near the Trusts premises. All such incidents should be reported in accordance with the Trust's Incident Reports and Investigation Policy and Procedure.

7.6 Assets

Irrespective of their value, assets can be defined as the materials and equipment used to deliver NHS healthcare. In respect of staff, professionals and service users it can also mean the personal possessions they retain whilst working in or providing services to the NHS.

7.7 Premises / Buildings

The physical buildings in which staff work, where service users are treated and from where the business of the NHS is delivered.

7.8 Closed-circuit Television

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted.

7.9 Restraint

Restraint is an intervention that prevents a person from behaving in ways that threaten to cause harm to themselves, to others, or to Trust property and/or equipment.

8. TABLE OF ROLES AND RESPONSIBILITIES

Role	Responsibility
Chief Executive	The Chief Executive of Yeovil District Hospital NHS Foundation Trust has ultimate responsibility for ensuring the provision of a safe and secure environment for all staff, patients, visitors and contractors. The Chief Executive is responsible for nominating a Security Management Director (SMD).
Security Management Director	The SMD is the nominated Board lead for Yeovil District Hospital NHS Foundation Trust. The SMD is responsible for reporting on security matter to the YDH Board of Directors and for ensuring the implementation of this policy and meeting the NHS Security Management Standards
Simply Serve Ltd (Estates and Facilities Director)	The Estates and Facilities Director under Simply Serve Ltd is responsible for the operational implementation of the security policy relating to the physical guarding, security and access arrangements.
Local Security Management Specialist (LSMS)	The Trust appoints an accredited Local Security Management Specialist, reporting to the Fire Health & Safety Manager (SSL) to the SMD to act as the Trust security advisor. The role of LSMS is to work on behalf of the Trust to deliver an environment that is safe and secure so that the highest standards of clinical care can be made available to patients. The LSMS will report through the Security Committee detailing the work that has been carried out the previous year. They submit an annual assessment against NHS Security standards. Each year an annual work plan will be developed by the LSMS to identify what actions the LSMS will employ to reduce security risks for the forthcoming year.
Security Committee	The membership of the Security Committee will be a wide representative group from members of Yeovil District Hospital NHS Foundation Trust and Simply Serve Ltd management. The Chair (SMD) is the reporting lead to the Hospital Management Team and Board of Directors. Refer to the Terms of Reference for the Security Committee.
Heads of Departments and Managers	Heads of Departments and Managers are responsible for the security of their workplaces, their staff and of any patients, visitors and contractors within their department. They must ensure:

	• All unoccupied areas are secured when not in use • Expensive equipment or hazardous materials are secured when not in use • Confidential documents are secured when not in use • Breaches of security including criminal activity are reported through the Trust's incident reporting procedure. • Security risk assessments are completed when risks identified and mitigating actions put in place
All staff	All staff are responsible for: • Maintaining a secure environment and ensuring security arrangements are followed • Being responsible for the security of their own personal property whilst at work. • Challenging anyone that should not have access to an area of the premises without authorisation • Wearing identity badges whilst at work. • Ensuring security of access codes and keys in their possession. • Reporting all security incidents through the incident reporting procedure.

9. REFERENCE TO OTHER POLICIES

This policy should be read in conjunction with the Risk Management Policy, the Incident Reporting and Investigation Policy and the Health and Safety Policy.

10. SOURCE REFERENCES AND ACKNOWLEDGEMENTS

- Data Protection Act 1998
- Health and Safety at Work Act 1974
- Human Rights Act 1998
- Regulation Investigatory Powers Act 2000
- NHS Protect Standards for Commissioners 2016-17, Security management
- NHS Protect A Professional Approach to Managing Security in the NHS (2003)
- Secretary of State for Health's Directions on NHS Security Management Measures (2003)
- Secretary of State for Health's Directions on work to tackle violence against staff and professionals who work to provide services for the NHS (2003)
- NHS Protect Non-Physical Assault Explanatory Notes (2004)
- NHS Protect Tackling Violence Against Staff: Explanatory notes for reporting procedures introduced by Secretary of State Directions in November 2003 (2007)
- NHS Protect Not Alone – A Guide for the Better Protection of Lone Workers in the NHS (2005)
- NHS Protect Conflict Resolution Training Implementing the National Syllabus (2004)

ANNEX A – EQUALITY IMPACT ASSESSMENT TOOL

Security Management Policy

		Yes / No / N/A	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	Yes	Access control for protecting wandering patients is in line with safeguarding requirements
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	N/A	
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Trust's lead for Equality & Diversity, together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the Trust's lead for Equality & Diversity.

Signed – Adrian Pickles (Fire, Health & Safety Manager) Date: 15 March 2018