This policy is applicable to services provided by Heartlands, Good Hope and Solihull Hospitals Divisions

Heart of England NHS
NHS Foundation Trust

SECURITY POLICY

Key Points

The Heart of England NHS Foundation Trust is committed to raising the standards of Security Management within the Trust inline with the NHS Protect standards, which incorporates a risk based approach to both providing a safe and secure environment for patients, employees and visitors and to protecting NHS property and assets.

Anyone working in the NHS, receiving NHS treatment or visiting NHS premises has the right to feel safe and secure from violence and abuse, both physical and verbal. Keep safe at all times funds and assets belonging to the NHS or used to provide NHS services and care. A failure to do so can have a major impact on patient and employee welfare and the standard of care patients receive from the NHS.

This Policy is intended to provide a robust framework that ensures that the Trust provides the highest levels of personal and property security to protect patients, visitors, employees and the Trust from the risk of crime.

Paper Copies of this Document

- If you are reading a printed copy of this document, you should check the Trust's Policy website (**http://sharepoint/policies**) to ensure that you are using the most current version.

Ratified Date: February 2015
Ratified By: Director of Asset Management
Review Date: February 2018
Accountable Directorate: Asset Management
Corresponding Author: Head of Facilities

Heart of England NHS
NHS Foundation Trust

Meta Data

Document Title:	**Security Policy**
Status	RATIFIED
Document Author:	Chris Davies, Head of Facilities chris.davies@heartofengland.nhs.uk
Source Directorate:	Asset Management
Date Of Release:	February 2015
Ratification Date	February 2015
Ratified by:	Director of Asset Management
Review Date:	February 2018
Related documents	Bomb Threat Plan Emergency Planning Policies and Procedures Health and Safety Policy Incident Reporting Policy and Procedures Infant Abduction Procedure Lone Working Policy Medical Gases Policy Missing Patient Policy and Procedures Patient Confidentiality Policy Patient Property Policy Restraint (Clinical Holding) Policy; Adults and Children Risk Management Policy and Procedures Supporting Employees Policy Trust Lockdown Planning Manual Trust Security Strategy Violence and Aggression Policy Violent Marker Policy
Superseded documents	Security Policy v6.0
Relevant External Standards/ Legislation	Care Quality Commission NHS Litigation Authority NHS Protect Data Protection Act 1998 In The Picture: A data protection code of practice for surveillance cameras and personal information.
Key Words	Security, crime, violence, theft

Heart of England NHS
NHS Foundation Trust

Revision History

Version	Status	Date	Consultee	Comments	Action from Comment
1		15-06-07	Paul Quinsey	Introduction	
2		01-09-07	S Wright	Checks against criteria	
3		30-11-10	Paul Quinsey	Scheduled Revision	
4		26-05-11	Paul Quinsey	Inclusion of Lockdown Minor modifications in response to NHSLA & CQC requirements	
5	Ratified	July 12	Martin Long	Full review of policy - Consultation with Health and Safety and Security Contractor	
5.1	Addition	30-10-12	Martin Long	Inclusion of CCTV auditing tool (point 9.3 & attachment 4)	
6	Ratified	03/02/15	Chris Davies	Full review – consultation with members of the Security Committee	
6.1	Ratified	14/07/16	Phil Chambers/Chris Davies	Minor amendment – new Trust logo & requirement for inclusion of a standard relating to financial recovery	
6.2	Ratified	12/11/16	Phil Chambers/Chris Davies	Minor amendment to one job title.	

Heart of England NHS
NHS Foundation Trust

Table of Contents

Heart of England NHS
NHS Foundation Trust

1 Circulation

This Policy applies equally to employees in a permanent, temporary, voluntary, students, work placements or contractor role acting for or on behalf of HEFT.

2 Scope

2.1 Includes:

- **The policy covers all security management related activity within the Trust and should be read in conjunction with the Standard Operating Procedures. Together, they form the Trust Security Policy. The supporting documents are available in the procedures tab of the Trust policies and procedures SharePoint. http://sharepoint/policies/Procedures/Forms/AllItems.aspx**

  Policies relating to specific areas of security management (e.g. Health, Safety and Risk Management, Crime Reduction and Managing Security Incidents *et al*) will be drawn upon and referenced.

- This policy is applicable to ALL EMPLOYEES in their day-to-day work, on behalf of Heart of England NHS Foundation Trust. This policy also covers volunteers, students, those on work placements, and contractors. The policy applies to everyone who engages in activities on behalf of the Trust, not just those with a specific responsibility for security and crime reduction.

- **For the sake of brevity, all such people are included in the term "employees" in this policy.**

2.2 Excludes:

- Information Security

Heart of England NHS
NHS Foundation Trust

3 Definitions

Wherever the word 'Trust' appears in this document, it refers to Heart of England NHS Foundation Trust.

For the purpose of this Policy, the following definitions apply:

- **Violence:** The intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort (Physical Assault Definition contained within NHS Protect).
- **Aggression:** The use of inappropriate words or behaviour causing distress and/or constituting harassment. (Non-Physical Assault Definition contained within NHS Protect).
- **Theft:** A person shall be guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it (Theft Act 1968).
- **Fraud:** Whilst there is no strict definition of fraud in British Law, Section 1 of the Fraud Act 2006 created a new general offence of fraud and introduces three possible ways of committing it:
    - By false representation
    - By failure to disclose information when there is a legal duty to do so.
    - By abuse of position.

  To be considered fraudulent, conduct must be dishonest and with the intention to make a gain, cause a loss or the risk of a loss to another.
- **Hazard:** General definition is anything that has the potential to cause harm.
- **Risk:** The definition in the Risk Management Policy is: 'Anything which prevents an organisation from achieving its declared aims and objectives; this includes risk of injury or harm. Suggest including this'.

4 Reason for Development

Crime costs the NHS over £5 billion every year. The open access of hospital environments renders us particularly vulnerable to crime. Security measures are concerned with the provision of safeguards against crime, the loss of, or damage to, Trust property and protection of the interests of patients, visitors, employees and contractors in respect of offences against persons or property.

Anyone working in the NHS, receiving NHS treatment or visiting NHS premises has the right to feel safe and secure from violence and abuse, both physical and verbal. Funds and assets belonging to the NHS or used to provide NHS services and care should also be kept safe and secure at all times. A failure to do so can have a major impact on patient and employee welfare and the standard of care patients receive from the NHS.

Heart of England NHS
NHS Foundation Trust

This Policy is intended to provide a robust framework which ensures that the Trust provides the highest levels of personal and property security to protect patients, visitors, employees and the Trust from the risk of crime.

5 Aims and Objectives

5.1 The aims and objectives of this Policy are to:

- Establish a safe and secure environment that has systems policies and procedures in place to protect patients, visitors and Trust employees from violence, harassment and abuse.
- Safeguard NHS property and assets from theft, misappropriation or criminal damage.
- Protect resources from fraud bribery and corruption.
- Safeguard personal property and equipment against fraud, theft or damage.
- Deter criminal activity and provide an effective response to all security incidents including the provision of good order within the Trust's premises.
- Work with the Police to minimise crime and provide a safe environment in which to deliver healthcare services.
- Put procedures in place to affectively manage security and crime reduction (refer to FSM-SOP-001 List of Standard Operating Procedures); Available via the link to SharePoint:

  http://sharepoint/policies/Procedures/Forms/AllItems.aspx

5.2 **The key principles of the Published Standard Operating Procedures documents will be:**

- Access control
- CCTV
- ID Badge
- Managing Security Incidents
- Security response for protecting NHS assets

Heart of England NHS
NHS Foundation Trust

6 Standards

6.1 The Heart of England NHS Foundation Trust is committed to raising the standards of Security Management within the Trust inline with the NHS Protect standards, which incorporates a risk based approach to both providing a safe and secure environment for patients, employees and visitors and to protecting NHS property and assets.

6.2 This suite of documents are arranged in tiers aims to provide strategic governance, inform and involve, prevent and deter and hold to account:

- Security policy;
- Security Standard Operating Procedures (SOPs) are available on the Trust Intranet Policies and Procedures supporting documents available via this link.

  http://sharepoint/policies/Procedures/Forms/AllItems.aspx

  Security standard operating procedures are based on standards outlined in NHS Protect Strategy, Security Management, Fraud Bribery and Corruption.

6.3 **Financial Recovery;** The Trust is committed to the recovery of loss by holding to account those who cause loss to the Trust through criminal damage or theft.

The Trust will work closely with the Police, the Crown Prosecution Service or other agencies such as HM Revenue and Customs in order to achieve this.

In cases involving suspected fraudulent behaviour or alleged fraud, this should be reported either to the Local Counter Fraud Specialist, or by calling NHS Protects confidential Fraud and Corruption Reporting Line on 0800 028 40 60.

6.4 The section below sets out who is responsible within the Trust for particular aspects of the Trust's security management obligations.

Heart of England NHS
NHS Foundation Trust

7 Responsibilities

7.1 Chief Executive

The Chief Executive is the officer initially and ultimately responsible within the Trust for maintaining and achieving legal and policy outcomes and will;

- Delegate responsibility for Security to an Executive Director;
- Advise the Trust Board on resources and actions required to meet regulatory regimes affecting security and crime reduction;
- Provide adequate resources to improve and maintain standards in the form of the commitment of time and financial resources;
- Ensure that employees receive security and crime reduction training appropriate to their grade/position;
- Ensure all employees of the Trust are aware of their responsibilities in regards to security and crime reduction
- Promote a positive culture to continually improve safe working practices associated with waste management;

7.2 Nominated Security Management Director

The Nominated Security Management Director has lead responsibility for strategic management and support for all security management work within the organisation and will:

- Ensure that there is adequate strategic security management provision in the Trust, as specified in paragraphs 2 and 7 of the Secretary of State Directions 2004 (amended 2006).
- Ensure the security strategy is aligned to NHS Protect's strategy; the security strategy has been reviewed, evaluated, updated and approved by the Trust Board.
- Provide adequate resources to improve and maintain standards in the form of the commitment of time and financial resources inline with identified risks;
- Reports annually to the Trust Board on how the Trust has met the NHS Protect standards and
- Ensure the Trust Board are aware of the security management needs of the Trust, particularly in tackling violence and aggression.
- Has responsibility for the nomination and appointment of a Local Security Management Specialist (LSMS) and for subsequent liaison with and monitoring of the LSMS.
- Ensure procedures in place accurately record all relevant information relating to security incidents involving violence, aggression, theft, fraud, bribery, corruption and other security related crimes.

- Ensure employees know how to report a violent incident, theft, criminal damage or security breach by completing the Trust Incident Reporting Form and are encouraged to report all incidents.
- Ensure employees who have been a victim of a violent incident have access to support services should they require it.

7.3 **Executive Directors**

Directors will have delegated responsibility for the dissemination and operation of the Trust's Security Policy within their directorate and will:-

- Ensure all members of the Trust are aware of the Trust Board's expectations for carrying out their security responsibilities;
- Provide adequate resources to improve and maintain standards in the form of the commitment of time and financial resources;
- Manage the security process within the areas of their responsibility to ensure that a systematic approach is taken to identify and control compliance to an acceptable level;
- Ensure appropriate monitoring systems are in place to determine the effectiveness of risk reduction actions;
- Share lessons learnt with colleagues via agreed forums, i.e. Directors meetings.

7.4 **Director for Asset Management**

The Director for Asset Management has lead responsibility for operational security and will:-

- Ensure provision of adequate resources to ensure that legislative compliance is achieved and maintained;
- Ensure integration of security management plans into the Asset Management Directorate Strategic business plans for new builds or refurbishments of the Estate;
- Ensure liaison with Local Security Management Specialist (LSMS) during the briefing, design and planning stages of new builds or refurbishments. Consultation with the LSMS should be at each stage for advice of the local security issues and intelligence on areas prone to security breaches. These areas include incidents of violence and aggression against employees, lone workers, theft and vandalism.
- Ensure implementation and use of an asset management system to manage and monitor the use of assets and the use of security measures to prevent or deter their theft.
- Inform the Executive Medical Director/Chief Executive of significant risks in relation to security;

- Provide information to the Executive Medical Director/Chief Executive and the Trust Board on security management issues.
- Chair the Asset Management Statutory Compliance Group and monitor the effectiveness of the Committee by ensuring that it meets its agreed terms of reference;
- Ensure the Trust has an appropriate security management infrastructure and framework in place;
- Escalate security management issues through the appropriate committee structures as required;
- Ensure that when security management risks are identified they are managed as part of the Directorate's risk management process and when appropriate are escalated through the risk register process to the Trust Board.

7.5 **Clinical Leads/Matrons/Lead Nurses/General Managers/Operational Managers**

Clinical Leads/Matrons/Lead Nurses/General Managers/Operational Managers will:-

- Actively promote a positive security culture and ensure that appropriate resources are provided in terms of time and financial resources within their area of responsibility;
- Carry out incident investigation as required and ensure that actions are taken to reduce the risk of re-occurrence.
- Ensure that actions arising from security management audits are followed up and complete;
- Ensure that within their area of responsibility, patient valuables are registered and secured as directed in the Patient Property Policy; available via this link.

  http://sharepoint/policies/Office%20Documents/Forms/Nursing.aspx
- Report any defects or failures in the security management system to Directors;
- Ensure employees are aware of the Trust's Security Policy and SOP's;
- Ensure that personnel within their areas of responsibility have received up to date and appropriate security training;
- Participate in planned security management audits to monitor compliance against safe working practice.

7.6 **Managers and Heads of Department**

Managers and Heads of Department have day-to-day responsibility for the operational activities within their areas of control and will:-

- Promote a positive security culture and lead by example;
- Ensure that the security procedures set out in the SOPs are implemented;
- Ensure that the SOPs are adhered to and copies are available to employees. SOPs are available on SharePoint;

  http://sharepoint/policies/Procedures/Forms/AllItems.aspx
- As part of the department local induction programme ensure that new employees receive instruction on their roles and responsibilities with regard to security and crime reduction;
- Request confirmation from contractors that they have received authorisation from the relevant Estates Office to work in the area;
- Ensure that within their area of responsibility, patient valuables are registered and secured as directed in the Patient Property Policy; available via this link.

  http://sharepoint/policies/Office%20Documents/Forms/Nursing.aspx
- Manage identified security risks so far as is reasonably practicable in line with the Trust security management systems;
- Ensure that processes are in place to enable the completion of actions that arise as a result of the audits;
- Ensure that employees receive adequate security and crime reduction training appropriate to their role;
- Ensure that appropriate security monitoring is carried out to meet the requirements of this security policy;
- Report and manage incidents in line with the trust incident reporting policy;
- Escalate risks that cannot be managed locally by utilising the escalation process identified in the Trust risk management strategy/policy. (Guidance is available on the DATIX incident management system and in the incident reporting policy).

7.7 **Employees**

Heart of England NHS Foundation Trust is committed to promoting a safe environment for employees, visitors and patients that enter Trust premises. Employees have a duty under the Health and Safety at Work etc. Act 1974 to take responsibility for their own health and safety at work. Employees should-

- Operate inline with the security SOPs and the Trust's legal framework; Available on SharePoint via this link:

  http://sharepoint/policies/Procedures/Forms/AllItems.aspx
- Co-operate with supervisors and managers on security, crime reduction, health and safety matters;

Heart of England NHS
NHS Foundation Trust

- Report faults, defects and hazards to the employer;
- Participate in the security risk assessment process to ensure that significant risks within the organisation are identified and appropriate action is taken to reduce risks to an acceptable level;
- Not interfere with anything provided to safeguard their security or that of others;
- Take reasonable care of their own security;
- Comply with this policy and associated SOP's;
- Assist with compliance with health & safety, security and other crime reduction related legislation by adherence to best practice at all times;
- Ensure all adverse incidents are reported and documented in accordance with the Trust Incident Reporting Policy and Procedures available via this link;

  http://sharepoint/policies/default.aspx
- Attend security training appropriate to their role;
- Promote a positive security and crime reduction culture;
- Report security issues to their line manager in line with SOPs;

Heart of England NHS
NHS Foundation Trust

7.8 Head of Facilities

The Head of Facilities has responsibility for promoting understanding and compliance with the Security Policy and will:-

- Put in place an organisational security management framework (e.g. Auditing, Policy, SOPs, governance arrangements);
- Chair the Security Committee;
- Disseminate relevant security management information to appropriate personnel within the Trust;
- Report significant findings to the Director of Asset Management;
- In conjunction with other specialists within the Trust, contribute towards the development of Security SOP's;
- Promote close working relationships amongst employees both within the Directorate of Asset Management and outside who manage security processes on behalf of the Trust;
- Liaise with the Trust's Lead Local Security Management Specialist (LSMS) and members of the Governance and Risk team as required;
- Ensure that a programme of security audit is in place and the SOP's are utilised to escalate security issues and risks identified as a result of the audits;
- Ensure that the security management team complete a CCTV Privacy Impact Assessment to evaluate whether it is necessary and proportionate to continue using CCTV.
- Identify available training resources to support those employees within Facilities with specific duties for managing security at the Trust to fully discharge their duties;
- Ensure Facilities contractors receive relevant information on security whilst working at or on behalf of the Trust during their induction training.

7.9 Head of Capital Projects

The Programme Manager with responsibility for all new builds and refurbishments will:-

- Liaise with Local Security Management Specialist (LSMS) during the briefing, design and planning stages of new builds or refurbishments. Consultation with the LSMS should be at each stage for advice of the local security issues and intelligence on areas prone to security breaches. These areas include incidents of violence and aggression against employees, lone workers, theft and vandalism.
- Support and develop the existing pro-security culture in the Trust.
- Contribute through community safety partnerships to reduce crime and disorder in the local community.

- Consider crime reduction initiatives in NHS Car Parks where formal parking is provided.
- Consult the Secured by Design (SBD) core principles and the SBD Hospital Guidance to incorporate at the briefing, design and planning stages.

7.10 **Head of Estates**

The Head of Estates has responsibility for providing and managing access control and will:-

- Ensure the organisation has arrangements in place to manage access and control the movement of people within its premises, buildings and any associated grounds. Such arrangements should be based on guidance and risk assessments.
- Liaise with Local Security Management Specialist (LSMS) during the briefing, design and planning stages of new builds or refurbishments. Consultation with the LSMS should be at each stage for advice of the local security issues and intelligence on areas prone to security breaches. These areas include incidents of violence and aggression against employees, lone workers, theft and vandalism.
- Ensure Estates contractors receive relevant information on security whilst working at or on behalf of the Trust during their induction training.

7.11 **Trust Car Parking & Security Manager**

The Trust Car Parking & Security Manager has responsibility for managing the Car Parking & Security Contract and will:

- Under direction of the Deputy Head of Facilities, develop security auditing, Policy, SOPs, governance arrangements;
- Liaise with the Trust's Local Security Management Specialist (LSMS);
- Ensure the security contractor fulfils their duties as outlined in the 'Security and Car Parking' contract specification;
- Report significant security issues to the Deputy Head of Facilities;
- With the security management team complete a CCTV Privacy Impact Assessment to evaluate whether it is necessary and proportionate to continue using CCTV;
- Identify available training resources to support those employees within Facilities with specific duties for managing security at the Trust to fully discharge their duties;

7.12 **Security Contractor**

The Trust Security Contractor will:

- Protect patient visitors and employees as outlined in the 'Security and Car Parking' contract specification;
- Liaise with the Trust's Local Security Management Specialist (LSMS);
- Contribute to the crime risk assessment programme with the assistance of the LSMS to identify security requirements;
- Make recommendations for improvements to Trust security;
- Follow all Trust emergency and major incident procedures.
- Follow Trust Policy in relation to incident management, to include reporting and the investigation of incidents.

7.13 **Contract Security Officers**

Under the direction of the contracted Security and Parking Management Provider's local manager, Security officers are primarily responsible for:

- Protecting patients, visitors and employees.
- Securing Trust property.
- Working with law enforcement agencies in the detection of crime and the detention of criminals.

7.14 **Buildings operated and serviced by third party providers**

Those responsible for providing security services in buildings operated by third party providers (e.g. NHS Property Services Limited) will:

- Ensure that security of HEFT employees in leased and serviced buildings or areas (e.g. through an Service Level Agreement) is inline with NHS Protect, Trust policy and associated procedures;
- Provide assurance to HEFT that security management systems are compliant with legislation and statutory requirements;

7.15 **The Local Security Management Specialist (LSMS)**

The LSMS has responsibility for ensuring that the Trust complies with Secretary of State Directions and any further guidance from NHS Protect.

Specifically, the Local Security Management Specialist (LSMS) is responsible for:

- Completes the organisation crime profile. Failure to do so will result in the Trust being in breach of its obligations under Service Condition 24 of the standard contract.

- Maintain relationships with all the key stakeholders.
- Conduct a crime risk assessment with the assistance of the Trust's Security Contractor to identify security requirements.
- Raising employee's awareness and enhancing the pro-security culture within the Trust.
- Undertaking investigations in partnership with appropriate managers, providing recommendations for improvement.
- Ensuring appropriate action is taken on NHS Security Management alerts.
- Ensuring that reporting to NHS Protect takes place in a full and timely manner.
- Coordinating the risk assessment programme reporting progress and significant issues to the Security Committee.
- Report the following examples of security incidents to NHS Protect:
    - Any security incident involving physical assault of NHS employees
    - Non-physical assault of NHS employees (including verbal abuse, attempted assaults and harassment)
    - Theft of or criminal damage (including burglary, arson, and vandalism) to NHS property or equipment (including equipment issued to employees)
    - Theft of or criminal damage to employees or patient personal property arising from these types of security incident.
- Maintain good working relations with the local Architectural Liaison Officer/Crime Prevention Design Advisor who has direct links with ACPO Secured by Design.

7.16 **Local Counter Fraud Specialist (LCFS)**

The Trust has a dedicated Local Counter Specialists who can be contacted to discuss concerns of fraud. The LCFS can provide advice and guidance in relation to concerns; they will lead on investigations and can provide information and attend team meetings to help raise awareness of NHS Protect and the role of the Local Counter Fraud Specialist.

- **Where fraud, bribery and corruption is suspected or discovered follow the instructions in the Local Anti Fraud, Bribery and Corruption Policy available via this link;**

  http://sharepoint/policies/Office%20Documents/Forms/Finance.aspx

Heart of England NHS
NHS Foundation Trust

7.17 **Work and Wellbeing Service and Human Resources**

Work and Wellbeing Service and Human Resources will:

- The Work and Wellbeing Service will support those Departments and Functions involved in security activities through the provision, where required, of pre-employment health tests and ongoing health surveillance. Similarly, Human Resources will advise on issues relating to employment procedures and legal requirements in respect of such matters as social responsibility, discrimination, human rights, medical unsuitability, etc.
- Provide support services to employees who have been a victim of a violent incident should they require it.

7.18 **Contractors**

- All contractors are required to ensure they follow this policy and associated SOPs;
- Contractors are required to ensure their employees comply with the Trust's Security Policy and associated SOPs.

Heart of England NHS
NHS Foundation Trust

7.19 Board and Committee Responsibilities

Ratifying Board and Committee Responsibilities:

7.19..1 Safety Committee

For notification only.

7.19..2 Asset Management Statutory Compliance Group

The Head of Facilities will report any significant issues relating to security management to the Asset Management Statutory Compliance Group.

7.19..3 Security Group

The Security Group will oversee and coordinate the activities of security and crime reduction within the Trust ensuring that corrective action is taken to correct non conformities and any instance of non-compliance. The group will also receive reports from the Trust's security contractors and identify areas for improvement in respect of security management within their sites.

8 Training Requirements

- The Trust recognises the need for effective training of all employees to deal with security-related issues, including violence and aggression. Training and advice will be provided on Trust procedures and other matters at local induction and on-the-job training:
- The Health & Safety Team provide conflict resolution training, which all frontline employees working within the Trust are invited to complete, following the 10-point national syllabus indicated by NHS Protect.
- In addition to the above, all security officers must receive annual training in Control and Restraint.

Heart of England NHS
NHS Foundation Trust

9 Monitoring and Compliance

9.1 The Security Committee identifies Trust security issues, monitors security incidents and recommends improvements to improve the security of patients, visitors and employees, together with personal and Trust property.

9.2 The Security Committee will report to the Trust Safety Committee via the minutes and attendance of the Asset Management Compliance Manager. The implementation, effectiveness and application of this policy will be monitored in the following ways:

9.3 The Security Committee will monitor:

- Incident trends and an overview of associated risk reduction action identified to reduce the risk of violence.
- The status of Conflict Resolution training and Control and Restraint training.
- Overview of progress made against the security risk assessment plan.

Heart of England NHS
NHS Foundation Trust

9.4 Monitoring Compliance Schedule

Criteria	Monitoring Mechanism	Responsible	Committee	Frequency
Reports	LSMS	LSMS		Quarterly / Annual
Risk Assessments	LSMS and Quarterly Report	LSMS	Security Committee	Quarterly
Arrangements for ensuring action is taken as a result of Risk Assessments	Risk Assessment actions monitoring and escalation procedure	Security Contract Management Health and Safety Team All Departmental Managers	Security Committee	Quarterly
IR1's	Incident Trends	LSMS Report	Security Committee	Quarterly

Heart of England NHS
NHS Foundation Trust

10 References

NHS Protect.

11 Attachments

Attachment 1 – Consultation and Ratification Checklist
Attachment 2 – Equality Impact Assessment
Attachment 3 – Launch and Implementation Plan

Heart of England NHS
NHS Foundation Trust

Attachment 1: Consultation and Ratification Checklist

Title	**Policy and Procedures Framework v5.0**

	Ratification checklist	**Details**
1	Is this a: **Combined Policy & Procedure**	
2	Is this: **Revised**	
3*	Format matches Policies and Procedures Template (Organisation-wide)	**Yes**
4*	Consultation with range of internal /external groups/ individuals	**Safety and Governance Team, Corporate Nursing**
5*	Equality Impact Assessment completed	**Yes**
6	Are there any governance or risk implications? (e.g. patient safety, clinical effectiveness, compliance with or deviation from National guidance or legislation etc)	**No**
7	Are there any operational implications?	**No**
8	Are there any educational or training implications?	**No**
9	Are there any clinical implications?	**No**
10	Are there any nursing implications?	**No**
11	Does the document have financial implications?	**No**
12	Does the document have HR implications?	**No**
13*	Is there a launch/communication/implementation plan within the document?	**Yes**
14*	Is there a monitoring plan within the document?	**Yes**
15*	Does the document have a review date in line with the Policies and Procedures Framework?	**Yes**
16*	Is there a named Director responsible for review of the document?	**Yes**
17*	Is there a named committee with clearly stated responsibility for approval monitoring and review of the document?	**Governance and Risk for approval. Information Governance for ongoing monitoring**

Document Author / Sponsor	**Ratified** by
Signed	**Signed**
Title	**Title** -
Date	**Date** -

Heart of England NHS
NHS Foundation Trust

NHS | HEART of ENGLAND NHS Foundation Trust

Attachment 2: Equality and Diversity - Policy Screening Checklist

Policy/Service Title:	**Directorate:**
Name of person/s auditing/developing/authoring a policy/service:	
Aims/Objectives of policy/service:	

Policy Content:

- For each of the following check the policy/service is sensitive to people of different age, ethnicity, gender, disability, religion or belief, and sexual orientation?
- The checklists below will help you to see any strengths and/or highlight improvements required to ensure that the policy/service is compliant with equality legislation.

1. Check for DIRECT discrimination against any group of SERVICE USERS:

Question: Does your policy/service contain any statements/functions which may exclude people from using the services who otherwise meet the criteria under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
1.1	Age?		X		X		
1.2	Gender re-assignment?		X		X		
1.3	Disability?		X		X		
1.4	Race or Ethnicity?		X		X		
1.5	Religion or belief (including lack of belief)?		X		X		
1.6	Sex?		X		X		
1.7	Sexual Orientation?		X		X		
1.8	Marriage & Civil partnership?		X		X		
1.9	Pregnancy & Maternity?		X		X		

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

2. Check for INDIRECT discrimination against any group of SERVICE USERS:

Question: Does your policy/service contain any statements/functions which may exclude people from using the services under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
2.1	Age?		X		X		
2.2	Gender re-assignment?		X		X		
2.3	Disability?		X		X		
2.4	Race or Ethnicity?		X		X		
2.5	Religion or belief (including lack of belief)?		X		X		
2.6	Sex?		X		X		
2.7	Sexual Orientation?		X		X		
2.8	Marriage & Civil partnership?		X		X		
2.9	Pregnancy & Maternity?		X		X		

Heart of England NHS
NHS Foundation Trust

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING DIRECT DISCRIMINATION =							
3. Check for DIRECT discrimination against any group relating to EMPLOYEES:							
Question: Does your policy/service contain any statements which may exclude employees from implementing the service/policy under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
3.1	Age?		X		X		
3.2	Gender re-assignment?		X		X		
3.3	Disability?		X		X		
3.4	Race or Ethnicity?		X		X		
3.5	Religion or belief (including lack of belief)?		X		X		
3.6	Sex?		X		X		
3.7	Sexual Orientation?		X		X		
3.8	Marriage & Civil partnership?		X		X		
3.9	Pregnancy & Maternity?		X		X		
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
4. Check for INDIRECT discrimination against any group relating to EMPLOYEES:							
Question: Does your policy/service contain any conditions or requirements which are applied equally to everyone, but disadvantage particular persons' because they cannot comply due to:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
4.1	Age?		X		X		
4.2	Gender re-assignment?		X		X		
4.3	Disability?		X		X		
4.4	Race or Ethnicity?		X		X		
4.5	Religion or belief (including lack of belief)?		X		X		
4.6	Sex?		X		X		
4.7	Sexual Orientation?		X		X		
4.8	Marriage & Civil partnership?		X		X		
4.9	Pregnancy & Maternity?		X		X		
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING INDIRECT DISCRIMINATION =							

Signatures of authors / auditors: **Date of signing:**

Heart of England NHS
NHS Foundation Trust

Equality Action Plan/Report

Directorate:
Service/Policy:
Responsible Manager:
Name of Person Developing the Action Plan:
Consultation Group(s):
Review Date:

The above service/policy has been reviewed and the following actions identified and prioritised. All identified actions must be completed by the date:

Action:	**Lead:**	**Timescale:**
Rewriting policies or procedures		
Stopping or introducing a new policy or service		
Improve /increased consultation		
A different approach to how that service is managed or delivered		
Increase in partnership working		
Monitoring		
Training/Awareness Raising/Learning		
Positive action		
Reviewing supplier profiles/procurement Arrangements		
A rethink as to how things are publicised		
Review date of policy/service and EIA: this information will form part of the Governance Performance Reviews		
If risk identified, add to risk register. Complete an Incident Form where appropriate.		

When completed please return this action plan to the Trust Equality and Diversity Lead; Pamela Chandler or Jane Turvey. The plan will form part of the quarterly Governance Performance Reviews.

Signed by Responsible Manager: _____ Date: _____

Heart of England NHS
NHS Foundation Trust

Attachment 3: Launch and Implementation Plan

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Action	***Who***	***When***	***How***
Identify key users / policy writers		Prior to ratification	Through consultation of document identify key stakeholders and users.
Present Policy to key user groups		At time of ratification Following ratification	Via Security Committee. Via Asset Management Statutory Compliance Group.
Add to Policies and Procedures intranet page / document management system.		Following ratification	As per Gatekeeper process.
Offer awareness training / incorporate within existing training programmes		Following ratification	Initially provide 1:1 training / support as required via Safety & Governance team If demand requires more formalised training sessions, this will be arranged in collaboration with Diversity, Training and other training associated with Policy development
Circulation of document(electronic)		Following ratification	Via link to Microsoft SharePoint. Through Comm's bulletin