Leicestershire Partnership NHS Trust

Security Policy

The Security Policy outlines the duties and arrangements for the security of staff within the organisation.

Key Words:	Security	
Version:	4	
Adopted by:	Quality Assurance Committee	
Date Adopted:	17 September 2019	
Name of Author:	Robert Lovegrove, Local Security Management Specialist	
Name of responsible committee:	Health and Safety Committee	
Date issued for publication:	September 2019	
Review date:	February 2022	
Expiry date:	1 September 2022	
Target audience:	All staff	
Type of Policy	Clinical	Non Clinical √
Which Relevant CQC Fundamental Standards?		

Leicestershire Partnership NHS
NHS Trust

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
Robert Lovegrove	Local Security Management Specialist

Circulated to the following individuals for comments

Name	Designation
Members of the Health and Safety Committee	Agreeing Committee
Members of the Directorate, Health, Safety and Security Action Groups	Sub-group of the Agreeing Committee

Contents

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
V1	March 2012	Harmonisation of three former policies
V2	October 2014	Minor amendments and updates to include requirements of NHS Protect Standards for Security Management.
V3	August 2016	Reviewed to reflect organisational changes
V4	July 2019	Minor amendments. Expanded section an access control and key security.

All LPT Policies can be provided in large print or Braille formats, if requested, and an interpreting service is available to individuals of different nationalities who require them.

Did you print this document yourself?
Please be advised that the Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version.

For further information contact:

Health and Safety Compliance Team
Leicestershire Partnership NHS Trust
Tel: 0116 295 1662

healthandsafety@leicspart.nhs.uk

Definitions that apply to this Policy

All procedural documents should have a definition of terms to ensure staff have clarity of purpose (refer to Policy for Policies for assistance)

Due Regard	Having due regard for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. • Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policies and practices that meet the diverse needs of our local population and workforce. It is about creating fair and equal access to goods, services, facilities and employment opportunities for all and reducing disadvantage experienced by some groups in comparison to others.

This policy takes into account the provisions of the Equality Act 2010 and the general and specific duties, ensuring as far as possible the Trust eliminates discrimination, advances equality of opportunity and fosters good relationships. It also ensures no one receives less favourable treatment on the grounds of age, disability, gender, reassignment, marriage and civil partnership, pregnancy and maternity, race, religion of belie, sex (gender) or sexual orientation.

In carrying out its functions, the Trust will take into account the different needs of different groups in their area. This applies to all the activities for which LPT is responsible, including policy development, review and implementation.

Due Regard

The Trusts commitment to equality means that this policy has been screened in relation to paying due regard to the Public Sector Equality Duty as set out in the Equality Act 2010 to eliminate unlawful discrimination, harassment, victimisation; advance equality of opportunity and foster good relations.

A due regard review found the activity outlined in the document to be equality neutral because this policy describes the arrangements in place for all staff across the Trust.

1 Summary

Security is essentially about risk management and has a bearing on the safety and welfare of patients, visitors and staff as well as having possible financial consequences for the Trust.

Effective security measures must be seen to be an essential feature in the delivery of quality healthcare to which the Trust is committed.

Like all other risks those affecting security need to be managed. This process requires the identification, evaluation and control of security risks as well as a commitment by every member of the Trust's staff to a safe and secure working environment.

Security can only be managed effectively when every member of staff is aware of and appreciates the risks involved, understands the importance of adhering to established procedures and feels he or she is an essential part of the overall security strategy.

Carefully planned and effectively managed procedures will ensure a safe environment for patients and for the staff that care for them as well as maximising the resources that are available for patient care.

2 Introduction

This Security Policy applies to all staff employed by Leicestershire Partnership NHS Trust.

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.

The fundamental problem facing most NHS premises today is 'striking the right balance' between security, safety and patient care. The aim of this Security Policy is to ensure that the optimum level of security is achieved and that accessibility to our services is reconciled with integrated security measures, designed to protect patients, visitors, staff, property and possessions. Maintaining discreet and effective security and safety enables staff, patients and visitors alike to be confident in the knowledge that the environment they are in is a safe and secure one.

In support of this policy the organisation has taken and follows guidance, as supplied by the NHS Security Manual.

3 Purpose

The aim of the Security Policy is to support the organisation in delivering high quality clinical services and the organisations commitment to providing a safe and secure environment for staff, patients and visitors. Security is the responsibility of all staff in not only safeguarding their own wellbeing and personal property but also that of patients, visitors and organisation property.

The organisation seeks to provide a safe environment for staff, patients and visitors by providing security measures across sites, training to deal with violence and aggression and to minimise security risk to all through continuous vigilance and improvement.

4 Strategy

The Security Strategy for the organisation attaches great importance to the security and safety of its staff, patients, visitors and property. The following measures are designed to deliver an environment for those who use or work in the NHS, which is properly secure so that the highest possible standard of clinical care can be made available.

Crime reduction must be the cornerstone of any security strategy. It means anticipating risks and taking action to remove, reduce or transfer them. To ensure compliance with the objectives expressed in the policy strategy. The

organisation has undertaken on a rolling programme crime reduction and security survey / risk assessments on the physical security of our building and the assets contained within and assets.

The security measures employed by the organisation are based upon the following principles:

- Developing a pro-security culture
- Deterring security incidents or breaches
- Preventing security incidents or breaches
- Detecting security incidents or breaches
- Investigating reported security incidents
- Taking appropriate sanctions against those responsible for security incidents or breaches
- Obtaining redress from those causing injury, loss or damage to Trust staff and property
- Learning lessons to ensure that identified risks and system weaknesses are appropriately dealt with.

The Security Policy seeks to ensure:

- The personal safety of staff, patients and visitors
- The protection of property against theft, damage and fraud
- The smooth and uninterrupted delivery of clinical services
- The incorporation of these objectives into building design

The Security Policy will meet the organisations objectives by ensuring that an annual security plan sets out the arrangements in place to support the framework to:

- Work towards full compliance with NHS standards for the management of security (there are currently no formal standards for NHS security following the lapse of standards in 2018; however, the Trust will continue to use the previous NHS Protect standards for security management as a guide for good practice)
- Undertake crime reduction and security surveys at each Trust site, ensuring that a survey is conducted at each site at least once every year
- Ensure that reported incidents of violence and aggression are appropriately investigated and risks identified
- Produce action plans to deal with identified security risks
- Undertake appropriate risk assessments regarding the physical security of staff, patients, premises and assets as identified in the action plan from surveys or any reported incidents
- To monitor the action plan and any outstanding actions from risk assessments in relation to the physical security of premises and assets as identified.
- Satisfy statutory requirements, e.g. NHSLA, CQC, Health and Safety.

5 Duties within the Organisation

5.1 Chief Executive

The Trust, through the Chief Executive and its management systems, shall ensure as far as it is reasonably practicable, good standards of security management that protect its staff and clients from risk. The Chief Executive has overall accountability for security and shall ensure:

- Appropriate action is taken to ensure compliance with any NHS standards for the management of security
- Responsibilities for security matters are properly assigned
- Requirements for additional resources to meet the objectives of the policy are brought to the attention of the Board
- Compliance with the policy is monitored by review reports provided to the Health, and Safety Committee
- Security is given adequate consideration prior to any major changes in the Trust's activities
- Staff receive appropriate training in security matters
- Appropriate security procedures are established and implemented
- Security risks are suitable assessed
- Where a criminal offence against Trust employees, contractors or property is suspected the Police are immediately informed, except in the case of a suspicion of fraud where the matter should be reported immediately to the Director of Finance in accordance with the Trust's Standing Finance Instructions.

5.2 Executive Director with responsibility for Security

The nominated executive director with responsibility for security management will control the formulation, implementation and monitoring of the organisations Security Policies and associated procedures.

The director is responsible for ensuring that corporate professional advice is available on matters relating to this policy and for establishing Trust-wide operating arrangements for security.

The director will ensure:

- The appointment of a Local Security Management Specialist (LSMS) who has undergone accredited training
- Implementation of a security strategy and promote effective security management based on NHS standards for the management of security
- The production of a written Annual Security Work Plan
- That the LSMS has the necessary support to carry out his responsibilities
- Subject to any contractual or legal constraints ensure all staff co-operate with the LSMS ensuring disclosure of information which arises in connection with any matter (including disciplinary matters) which may

have implications for the investigation and / or the prevention of breaches of security

5.3 Local Security Management Specialist

The Local Security Management Specialist will have responsibility to ensure that:

- Reports as appropriate are generated and presented to the Health and Safety Committee and Directorate Health and Safety Action Groups
- An annual written report is produced
- Accurate records of any breaches or suspected breaches of security are maintained
- Security management work is carried out in accordance with the NHS standards for the management of security
- Reports are made to the Trust's executive director with responsibility for security management on security-related issues
- Appropriate security incidents or breaches are notified to Health and Safety Committee
- Investigations into security matters are conducted where appropriate
- Advice is given to staff on key preventative and proactive measures to raise security awareness and reduce risk
- Advice is given on security for all capital and refurbishment work relating to the security of Trust premises
- Advice is given in relation to site security
- Advice is given in relation to personnel security.

5.4 Directorate Leads, Directors, Managers and Supervisory Staff

All Directors, Managers and Supervisory Staff are responsible for monitoring adherence to this policy. In particular they shall promote:

- That risk assessments are in place and where significant security risks exist local controls are in place mitigate risk to as low as is reasonably practicable
- That all staff are briefed with regard to their own personal security and local procedures, and where appropriate, are supported to attend security training
- That all staff are issued with staff identification badges
- That work areas under their control are operated in accordance with this policy and any associated procedures
- That all breaches of security arrangements are investigated and reported immediately in accordance with incident reporting policy and procedures
- That faults with Trust security systems are reported to Estates without delay
- That all staff upon leaving the organisation return their ID badges, uniforms, organisation issued keys, electronic passes and any issued security alarm system or personal protective equipment

- That confidential records are secured in line with Trust policy
- Advice is sought, as appropriate, from the LSMS and others where there is any doubt as to the standards that are to be applied in adhering to this policy
- Response is made at the earliest opportunity to any request from employees for advice on security concerns
- All security incidents are recorded using the Trust incident reporting system.

5.5 Head of Trust Health and Safety Compliance

The Head of Trust Health and Safety Compliance is responsible to the Chief Executive for the routine monitoring of adherence to this policy and in particular will promote:

- That any breaches of this policy are brought to the attention of the relevant manager and, as appropriate the executive director with responsibility of security management
- Advice is generally available to directors, managers and staff on matters relating to this policy
- Security risks are identified and assessed and recommendations for risk reduction are forwarded to relevant managers and, as appropriate the executive director with responsibility of security management
- The appropriate line management of the LSMS
- The LSMS maintains communication with the Police, security contractors and other external organisations on matters relating to this policy
- The monitoring of and completion of all actions relating to security risks through audit.

5.6 All Employees

All employees have a duty to co-operate with the implementation of this policy. In particular it should be ensured:

- That they bring to the attention of their immediate manager, or duty manager, as appropriate, any suspicious activity they observe on the organisations premises
- That they report all incidents of violence and aggression at the earliest opportunity
- That they attend appropriate security training or education
- That they adhere to all relevant departmental local procedures and make use of systems provided in identified areas
- That they wear their staff identification badges and identity cards at all times when on duty
- That they bring to the attention of their line manager any perceived shortcoming in security arrangements
- That they make full and proper use of personal lockers and take all reasonable care for their own property whilst at work

- That they report immediately to their departmental manager any loss, or malicious damage to, their own, patients or Trust property.
- That faults with Trust security systems are reported to Estates without delay.
- Where they are issued with staff personal safety alarms or other personal protective equipment that equipment is signed out in accordance with Trust policy and returned at the end of their shift or other continuous period of work.

6 General Security Arrangements

Departmental managers have responsibility for the securing their own departments and ensuring advice and local procedures are in place to manage security risk. All services, teams and wards must have a current security risk assessment. All premises shall be suitably secured to prevent unauthorised access during and outside of normal working hours or when core services are closed. Where sites are shared with other services local protocols are to be put in place to ensure collective responsibility for security. Advice from the LSMS should be sought on the adequacy of local security arrangements.

6.1 Access Control

Service managers at all Trust premises are to ensure that there are local written procedures detailing measures governing access to areas under their control. They should coordinate with service mangers in adjacent areas of the same building to ensure that security in these areas is not compromised.

It is particularly important that access is only granted to those who have a requirement to be in a particular area; therefore, access to staff-only, clinical, and other restricted areas, must be appropriately controlled.

Automated electronic access control systems must be appropriately managed and access fobs or cards only issued as part of a formal process which balances the operational needs of the service with the protection of Trust property and the health and safety of employees, contractors, patients and other legitimate visitors. Managers are to ensure that access cards and fobs are obtained in accordance with the local procedure for sites and are removed from members of staff when they no longer have a requirement for them.

Automated access control systems such as SALTO allow the use of fobs, cards or other tokens to release door locks electronically. Such systems are managed like networked computer systems and should be subject to the following administrative rules:

- Each system requires suitably trained system administrators
- There must be more than one administrator to allow for oversight and audit
- No access control card, fob or token should be issued unless specifically authorised by an appropriate manager.

- System administrators should maintain a list of authorising managers and provide managers with appropriate documentation to authorise access for employees.
- Managers should ensure that access control permissions are removed from staff when they leave or move to another team. Access control should be team and role specific and re-authorisation should occur when that role changes.
- Access control permissions should also be removed if an employee will not be using the access control system for some time. If an employee is on maternity leave or long-term sick leave but will be returning to work then access may be retained. If an employee is on detachment for a significant time, is suspended for disciplinary reasons or is still employed but not expected to return to work then access rights should be removed.
- System administrators should conduct routine audits to check that cards, fobs are still in use. If a card has not been used for a significant time (3 months) the authorising manager should be contacted to determine whether access is still required.

It is the responsibility of managers to ensure that they keep secure, accurate and up to date records of all organisation keys held by staff under their control. Staff should be aware of the need to immediately report any loss of keys and that periodic checks will be carried out to ensure that they maintain control of all keys issued to them.

Where members of staff require keys to complete their work, for example, nursing staff working in an inpatient environment, keys should be issued at the start of their shift and returned at the end. Supervisors, such as the nurse in charge of the shift, must ensure that all keys are signed for and accounted for at the end of the shift.

Where keys are held and managed by Estates and Facilities (internal or external provider) they must be held in a secure key safe in a secure area. All keys must be signed out in a key register and issuing staff must ensure that keys are returned by the end of the working day.

All keys held by external contractors shall be identified by only a unique site code and not the site address to maintain building security. All keys distributed shall be signed for by the individual, with routine audits being carried out at regular intervals to ensure that all keys and passes remain valid and within the individual's control. Any electronic pass not used for a period of three months shall be deactivated.

Contractor access is detailed in the Control of Contractors Policy.

Many sites use electronic or mechanical keypad locks which require a code. These locks are ideal in environments where a small number of people need access to a room or area but are less secure when traffic through the access/egress point is more frequent. Only staff requiring access to such an area should be notified of the code. However, it is easy for members of staff to

share codes which inevitably results in increased risk of unauthorised access through these doors. The following rules should apply to all keypad locks:

- Codes are to be changed at least twice annually. The best time being May and November as these are generally out of the holiday season
- Codes should be changed after a significant event, such as the suspension or dismissal of a member of staff, following contractors carrying out work at sites, following the reallocation of services to different sites and when recommended by the LSMS following a security incident or survey
- When the keypad is worn

6.2 Property (Patients)

Patients being admitted to hospital are to be advised not to bring valuables with them. In the event of patients having valuable items with them on admission, they are to be advised to hand them in for safekeeping. A documented system will be in place to record all such items placed in secure storage and subsequently returned to the patient when discharged. Patients should be made aware that the organisation cannot be held liable for their valuables if they are lost or stolen on our premises unless handed into staff for safe keeping.

6.3 Identity badges

A system is in place to issue all staff with personal identification badges and issue official visitors / contractors with passes for their period of visit. Members of staff will initially obtain their official identification badges as part of their induction within their first week of commencing employment. This is controlled by Workforce.

Members of staff are required to display their Identity badge at all times when on duty and managers are required to carry out random checks in this regard. Staff should be aware that security personnel and others are liable to challenge them whilst on the organisations premises and this is the interest of everyone's personal safety.

Badges should be kept safe at all times outside working hours. The employee's line manager should be informed immediately if identity badges are lost, so that the badge can be "locked out" and a replacement badge issued.

Lost identification badges must be reported using the organisation incident forms. New badges will only be reissued following organisation Identification Badge procedure.

Agency / temporary staff will be required to demonstrate upon arrival proof of identify and agency membership.

The responsibility for checking authenticity of agency membership will be vested in the appropriate senior manager on duty at the time of arrival.

6.4 Staff Property

Staff should be aware that the organisation cannot accept liability for loss or damage to staff property brought on to its premises. Reasonable arrangements for staff to secure personal items in lockers, etc., are however, generally available. Members of staff are advised not to bring valuable items into work whenever possible and to consider their own insurance arrangements, as appropriate.

6.5 Trust Property

Staff should take all reasonable steps to ensure that organisation property under their control remains secure and where appropriate the items are to be placed on the Asset Register (items valued at £5,000 or over). Managers should review organisation property held by their department on a regular basis to ensure that all items are security marked where appropriate. Valuable and attractive items of equipment, i.e. IT equipment will be marked by the IT provider (see Information Security Policy). Medical Devices are recorded on a separate register (see Medical Devices Policy).

6.6 Violence to Staff

The organisation has a policy on violence to staff (Prevention and Management of Aggression Policy) which outlines the arrangements to minimise risk, give general guidance and advises on reporting procedures. Copies of this policy are posted on the organisation's intranet site.

6.7 Reporting Security Incidents

Security incidents should be reported using the e-IRF system in accordance with the Trust's Incident Reporting Policy. In the event of any incident or if a member of staff has reason to believe a security breach or potential breach can or has occurred they should immediately report it to their line manager. In the event of a serious incident or obvious criminal behaviour then staff should inform the Police. The senior manager on-call is to be informed immediately if the incident occurred out of hours. All incidents must be reported using the organisations incident report process.

6.8 Medicines

Detailed guidance on the security of medicines is covered in the following policies:

- Medicines Management Policy
- Prescription Stationary – Secure Handling and Storage Policy.

7 Security Alarm Systems

Where a building or site has a security alarm system installed, appropriate staff should be trained to set and deactivate the alarm system. Site managers should be aware that members of staff who are in possession of alarm codes or fobs can potentially access the building out of hours so some form of audit of access should be available. This is possible with fob systems but may not be with manual keypad systems.

Prior to setting the alarm the appropriate key holder should check that the building is completely empty and all doors and windows have been secured.

Trust Headquarters and a number of other properties have a contract key holding service. Any contract performance issues associated with the contract key holder service should be reported in accordance with the Incident Reporting policy and to Estates and Facilities which manages the service.

8 Closed Circuit Television Systems (CCTV)

CCTV cameras are installed on many of the organisations sites. The use of CCTV is detailed in the Closed Circuit Television Policy.

9 Lone Workers

Detailed information is provided in the Working Alone in Safety Policy.

10 Information Systems Security

Detailed information is provided in the Information Security Policy.

11 Bomb Threats / Suspicious Packages

Detailed information is contained in the Business Continuity Plan.

12 Lockdown Procedure

Lockdown is the process of controlling the movement and access – both entry and exit – of people (NHS staff, patients and visitors) around the Trust's sites 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.

A lockdown risk profile and plan shall be developed for all sites, which shall include a local lockdown plan which will include a site specific risk assessment. The risk profile will be understood for the site based on the following criteria:

- Needs analysis
- Identification of critical assets
- Identification of potential threats and hazards
- Site vulnerability assessment

- Building vulnerability assessment
- Security vulnerability assessment
- Review personnel support to lockdown
- On-going review of the above.

The LSMS will be able to provide support and guidance on the development of a local lockdown procedure, but a stakeholder management team should be established to undertake the review and identify critical areas to be locked down.

The procedure will include key evaluation stages that will need to have individual procedure in place including:

- How the lockdown will be activated
- How the lockdown will be deployed
- How the lockdown will be maintained
- How the lockdown will be stood down
- How the lockdown will be reviewed.

For modern buildings with electronic security access a lockdown is relatively easy to initiate, however for older sites with limited internal security it will be often be difficult to implement a lockdown process, however, the method of implementing a lockdown and how it will be enforced will be based on the individual sites assessment of risks and site profile.

13 Training

All staff will receive induction and further mandatory training, as identified by a formal training needs analysis for their role, covering:

- How best to protect patients, staff, visitors and property
- How best to deal with violence and aggression, depending on the role of the individual and their work environment
- In understanding of the various elements that determine the organisations strategy for security and safety
- The scale of crime within an NHS and public sector setting
- The role of the Local Security Management Specialist and other support agencies.

A robust process managed within the Health, Safety and Compliance Team for the Health, Safety and Security Manager and Local Security Management Specialist to circulate further security and personal safety guidance to staff. This will be delivered by way of briefings and security publications.

14 Monitoring

The Health and Safety Committee will monitor compliance with this policy through:

- Reports received from the LSMS on a quarterly basis, Crime Reduction and Security Surveys and risk assessments on performance against agreed action plans and audits of practice and where appropriate escalate for further consideration to the Trust Board.
- Analysis, on a quarterly basis, of incidents and trend data received relating to the security of staff and property.
- The Health and Safety Risk Register and any entries pertaining to security.
- For clarification as to the monitoring of NHSLA criteria 4.1 please refer to appendix 1.

15 Review of Policy

The Trust will review the policy every three years to reflect any organisational changes, national guidance or changes in legislation.

16 Publicising this Policy

This Policy will be a document available electronically on the Trust's Intranet site.

17 References and Associated Documentation

CCTV Policy
Control of Contractors Policy
EPRR Policy
Prevention and Management of Aggression Policy
Lone Worker Policy
Incident Reporting Policy and Toolkit
Information Security Policy
Data Protection and Information Sharing Policy
Medical Devices Policy
Medicines Management Policy
Prescription Stationary – Secure Handling and Storage Policy

A Professional Approach to Managing Security in the NHS (NHS Protect 2003)
The NHS Standard Contract
NHS Security Management Standards (when issued)
Non-Physical Assault Explanatory Notes (NHS Protect 2003)
Tackling Violence Against Staff (NHS Protect 2007)
Not Alone – A Guide for Better Protection of Lone Workers in the NHS (NHS Protect 2005)
Conflict Resolution Training Implementing the National Syllabus (NHS Protect 2004)
The Health and Safety at work Act (1974)
The Management of Health and Safety at Work Regulations (1999)
The NHS Litigation Authority (NHSLA) Risk Management Standards
NHSLA Mental Health and Learning Disability Standards (2008)
Essential Standards of Quality and Safety (Care Quality Commission)

Monitoring Compliance and Effectiveness

Reference	Minimum Requirements	Self-assessment evidence	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
4.1 (b)	b) how the organisation risk assesses the physical security of premises and assets	4.0 Strategy LPT a rolling programme crime reduction and security survey / risk assessments on the physical security of our building and the assets contained within and assets. Reports received from the LSMS on a quarterly basis,	Trust Risk Assessment review process Reports received by the Health & Safety Committee	Local Security Management Specialists Local Security Management Specialists	As determined by individual risk assessments Quarterly

Policy Training Requirements

The purpose of this template is to provide assurance that any training implications have been considered

Training topic:	Security
Type of training:	Mandatory
Directorate(s) to which the training is applicable:	All Directorates
Staff groups who require the training:	All staff
Update requirement:	Attendance three yearly at Core Mandatory Training
Who is responsible for delivery of this training?	Learning and Development Team
Have resources been identified?	Yes
Has a training plan been agreed?	Yes
Where will completion of this training be recorded?	Trust learning management system
How is this training going to be monitored?	Quarterly report to Health and Safety Committee

*A full Due Regard (Equality Analysis) makes sure that any negative impacts have been considered and ways to minimize the impact are specified.

Due Regard Screening Template

Section 1	
Name of activity/proposal	Security Policy
Date Screening commenced	July 2019
Directorate / Service carrying out the assessment	Health and Safety Compliance Team
Name and role of person undertaking this Due Regard (Equality Analysis)	Robert Lovegrove, Local Security Management Specialist
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS:	
OBJECTIVES:	
PURPOSE:	

Section 2		
Protected Characteristic	**Could the proposal have a positive impact Yes or No (give details)**	**Could the proposal have a negative impact Yes or No (give details)**
Age	No	No
Disability	No	No
Gender reassignment	No	No
Marriage and Civil Partnership	No	No
Pregnancy and Maternity	No	No
Race	No	No
Religion and Belief	No	No
Sex	No	No
Sexual Orientation	No	No
Other equality groups?		

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.			
~~Yes~~		**No**	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	√

Section 4
It this proposal is low risk please give evidence or justification for how you reached this decision:

Sign off that this proposal is low risk and does not require a full Equality Analysis:
Head of Service Signed: Bernadette Keavney
Date: 29 August 2019

Leicestershire Partnership NHS
NHS Trust

The NHS Constitution

NHS Core Principles – Checklist

Please tick below those principles that apply to this policy

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	☐
Respond to different needs of different sectors of the population	√
Work continuously to improve quality services and to minimise errors	☐
Support and value its staff	√
Work together with others to ensure a seamless service for patients	☐
Help keep people healthy and work to reduce health inequalities	√
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	☐

PRIVACY IMPACT ASSESSMENT SCREENING

Privacy impact assessment (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individual's expectations of privacy. The first step in the PIA process is identifying the need for an assessment.

The following screening questions will help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise and requires senior management support, at this stage the Head of Data Privacy must be involved.

Name of Document:	Security Policy		
Completed by:	Robert Lovegrove		
Job title	Local Security Management Specialist	**Date**	29/08/19

	Yes / No
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	**No**
2. Will the process described in the document compel individuals to provide information about themselves? This is information in excess of what is required to carry out the process described within the document.	**No**
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	**No**
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**No**
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	**No**
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	**No**
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	**No**
8. Will the process require you to contact individuals in ways which they may find intrusive?	**No**

If the answer to any of these questions is 'Yes' please contact the Head of Data Privacy Tel: 0116 2950997 Mobile: 07825 947786
Lpt-dataprivacy@leicspart.secure.nhs.uk
In this case, adoption n of a procedural document will not take place until approved by the Head of Data Privacy.

IG Manager approval name:	
Date of approval	

Acknowledgement: Princess Alexandra Hospital NHS Trust