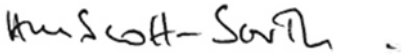
POLICY DOCUMENT

Burton Hospitals
NHS Foundation Trust

SAFE AND SECURE ENVIRONMENT POLICY

Approved by:	**Trust Executive Committee**
On:	**30 January 2018**
Review Date:	**December 2020**
Corporate / Directorate	**Corporate**
Clinical / Non Clinical	**Non Clinical**
Department Responsible for Review:	**Governance**
Distribution:	
• Essential Reading for:	**All Staff**
• Information for:	**Contractors and Volunteers**
Policy Number:	**69**
Version Number:	**9**
Signature:	 **Chief Executive**
Date:	**30 January 2018**

Burton Hospitals NHS Foundation Trust

POLICY INDEX SHEET

Title:	**Safe & Secure Environment Policy**
Original Issue Date:	**August 2006**
Date of Last Review:	**January 2018**
Responsibility:	**Security Management Director (SMD)/ Local Security Management Specialist (LSMS)**
Stored:	**Trust Intranet**
Linked Trust Policies:	**Health & Safety Policy** **Security Management Policy** **Risk Management Strategy** **Incident and Serious Incident Management Policy and Strategy** **Conflict Resolution Policy** **Lone Worker Policy** **Baby and Child Abduction Policy** **Fraud and Corruption Policy** **VIP and Official Visitor policy** **CCTV Policy** **Lockdown Policy** **Anti Fraud and Bribery Policy**
E & D Impact assessed?	**EIA 010**
Responsible Group / Committee	**Health & Safety Group**
Consulted	**Health & Safety Group** **Senior Managers** **Estates and Facilities Managers** **Staff Side** **Medical Records**

REVIEW AND AMENDMENT LOG

Version	Type of change	Date	Description of Change
7	NHSLA Standards	12.04.2012	Change to the monitoring standards
8	Review	16.12.2014	Regular review and update
9	Review and update	21/01/2018	Review and combination of Aggressive Behaviour Marker policy

SAFE AND SECURE ENVIRONMENT POLICY

CONTENTS PAGE

Burton Hospitals NHS Foundation Trust

SAFE AND SECURE ENVIRONMENT POLICY

1. INTRODUCTION

Burton Hospitals NHS Foundation Trust is committed, as far as is reasonably practicable, to ensuring the safety and welfare of its staff, patients, visitors, members of the public and the protection of Trust buildings and assets.

The Trust objectives to maintain security of the all premises and assets are based on Trust policies and Government security related legislation. The Management of Health and Safety Regulations 1999 places a specific duty on employers to carry out risk assessments of the hazards that employees and others may be exposed to and determine and implement suitable control measures to avoid or minimise the risk as far as is reasonably practicable.

This policy applies to all staff employed by the Trust, either directly or as part of a contracted service, and to any other person or organisation that uses Trust services or premises for any purpose. All staff have a core responsibility to ensure that local security measures and procedures are observed at all times. Security involves all groups and levels of staff. To be effective, it is important to establish at the outset, the support of everyone in the organisation.

The Policy directions shall be adopted Trust wide but it should be recognised that local procedures and protocols shall continue to be developed and implemented to support the Policy.

2. POLICY STATEMENT AND OBJECTIVES

The purpose of the Policy is to detail the Trust's responsibility for the effective management of security in relation to staff, patients, visitors and property and to support the aims of Burton Hospitals NHS Foundation Trust, in the delivery of high quality clinical services, through the provision of a safe and secure environment.

This policy seeks to:

- Develop a culture which recognises the importance of security.
- Ensure managers and staff are aware of their individual responsibilities in the implementation of security systems.
- Ensure the personal safety at all times of staff, patients and visitors, as well as other employees and contractors.
- Provide a working environment that is safe, secure and free from the dangers of crime for all people who may be affected by its activities.

- Ensure the protection of premises, property and assets against fraud, theft and damage.
- Support a safe environment in which the uninterrupted delivery of quality healthcare can be guaranteed.
- Establish a working partnership with local agencies, e.g. the police and local authority, for a safe and secure environment within all Burton Hospitals' locations.
- The smooth and uninterrupted delivery of the Trust's business.

3. DEFINITIONS

3.1 Physical Assault

The intentional application of force against another person without lawful justification; resulting in physical injury or personal discomfort.

3.2 Non-Physical Assault

Non-physical assault – the use of inappropriate words or behaviour causing distress and / or constituting harassment

3.3 Closed Circuit Television Cameras (CCTV)

Cameras placed in strategic areas of high risk to capture live motion and enable recording of an event where required.

3.4 Identified Front Line Staff

Staff who have been identified through risk assessment as working in high risk areas of verbal and /or physical abuse.

3.5 Lockdown

A lockdown is the process of preventing freedom of entry to, exit from or movement within the Trust (see separate Lockdown Policy).

4. BASIC PRINCIPLES

4.1 The Trust recognises that staff, patients and the public expect a safe and secure environment and they should not be put at risk directly or indirectly from the effects of crime or other threats. Crime is one of the most disturbing experiences, causing disruption and inconvenience to all concerned.

The security measures employed within the Trust are based upon the following principles:

To Deter Criminal activities where possible, by putting in place essential security control systems and other counter measures.

To Deny The criminal opportunity, not only through physical barriers, but by putting in place effective systems of loss prevention and

property control.

To Detect The criminal act. The earlier the criminal act is detected and reported, the greater the chances of preventing the offenders getting away. Raised awareness of security at all levels will both detect and reduce the risk of crime.

To Respond Effectively to security issues and problems, with workable counter-measures.

To Review The Policy, after additional counter measures have been put in place, to evaluate their effectiveness.

To Liaise With the local police and local authority to achieve partnership, working towards a safe and secure environment.

4.2 **The primary aims are:**

- To protect against criminal activity, other hazards and the preservation of good order within the Trust.
- The protection of staff from physical assault and/or verbal abuse.
- The prevention of the loss of patients', visitors' and Trust property / assets.
- The protection of the Trust's property, premises and assets against malicious acts, thefts, criminal damage, trespass etc.
- The detection and reporting of suspected offenders committing offences against patients, visitors, staff, the Trust, or private property within the Trust's premises.
- The provision of advice and assistance with all matters concerning security.
- The investigation of crime and security incidents within the Trust's premises. These investigations will, on occasions, be carried out in conjunction with the Trust's Auditors, the NHS Protect.
- The provision of appropriate training for staff.

5. DUTIES

5.1 **Chief Executive**

The Chief Executive has overall responsibility, on behalf of the Trust Board for;

- The organisation and management of security measures across the Trust.
- Monitoring the implementation of this Policy throughout the Trust.

5.2 **Director of Governance / Security Management Director is responsible for:**

- The formulation, implementation and maintenance of an effective Policy and supporting framework for the management of a safe and secure environment.
- Reviewing and amending this Policy to ensure compliance with any current guidance and legislation.
- Instituting regular campaigns to highlight the importance of security and the responsibilities of all Trust staff.
- Ensuring that full co-operation is given to the Local Security Management Specialist (LSMS) and Police, including access to personnel, premises and records (electronic or otherwise) considered relevant to security matters.
- Ensuring that details of incidents are recorded on the Trust's incident reporting system to comply with Health and Safety legislation.
- Ensuring that managers review any significantly violent incident and that it is used to evaluate Policy guidelines and skills to avoid further incidents.

5.3 **Directors:**
It is the responsibility of the Directors to:

- Disseminate and ensure compliance with this Policy within their area of responsibility and ensure that staff are appropriately trained and supported.
- Co-ordinate security issues with other organisations and employers who share the worksite of Burton Hospitals NHS Foundation Trust.

5.4 **Head of Health & Safety / Local Security Management Specialist (LSMS)**

The Head of Health & Safety/ LSMS has specific responsibility for promoting staff security within the Trust under the Secretary of State's Directions and will:

- Provide advice to managers at all levels on security measures, dealing with violence, aggression, nuisance or disturbance behaviour, including new legislation and government initiatives relating to security.
- Act as the Trust's lead with external bodies such as the local police, crime prevention officers, Crime and Disorder Partnership Scheme and the Community Safety Partnership Scheme.
- Liaise with the police, NHS Protect and their Legal Protection Unit in prosecuting offenders to ensure that where appropriate, redress is sought from those who commit security incidents.
- Investigate instances of crime and security breaches, interview and record statements in accordance with NHS Protect requirements and provide assistance to managers implementing risk reduction measures and post-incident management.

- Facilitate the provision of appropriate training in conjunction with the Learning & Development Department by assisting managers to identify training needs and provide/make available appropriate courses.
- Report to the Security Management Director on key security management issues. Analyse security incidents and report them to the designated Trust Board Committee, SMS and other appropriate bodies.
- Monitor the effectiveness of implementing this Policy by means of the Adverse Incident Reporting Procedures and audits.
- Collate and report incidents and actions to the Quality Committee.

- Provide assistance to managers undertaking violence at work, risk assessments and report to the Health and Safety Group on the implementation of risk assessments by directorates.
- Refer staff to Occupational Health, as necessary.

5.5 Head of Estates

The Head of Estates has responsibility for matters relating to the security of Trust property and premises and for the maintenance of CCTV.

5.6 Health and Safety Group

The Health and Safety Group is accountable to the Quality Committee and will provide assurance on health, safety and security performance to the Board.

5.7 Managers/Heads of Department

Security is the responsibility of all Managers; they must undertake preventative measures for the safety of staff, patients, visitors and property.

All managers carry a responsibility for security. It is their job to see that the right policies, procedures and systems are in place in their local areas and that such policies are kept under constant review. They need to carry out risk assessments and ensure staff are trained and receive relevant instruction and training.

The manager is responsible for the completion of a security risk assessment for the department and any identified additional control measures required must be entered onto an action plan and managed until all actions are completed.

It is the individual manager's responsibility to see that safe and secure environments are maintained and that all incidents are fully reported by means of the Trust's incident reporting system, Datix and that action is taken as and when necessary and the incident investigated.

Guidelines are available for Managers and Staff at Appendix A. In addition Managers should:

- Implement a procedure to record details i.e. make, model, serial number, value etc. of all valuable or important property within their department/directorate, except where asset registers are held centrally e.g. computer & electrical equipment. The Estates Department or the Head of Health & Safety/ LSMS can advise on methods to secure property.

- Ensure that arrangements are made to secure the department/ business unit out of working hours, together with the safe custody of keys and the setting of any security alarms or devices to protect the property.

- Ensure records are kept of all keys issued to staff in their department/ business unit and report all losses of keys to the Estates Department.

- Advise the Estates Department of any changes within their department/ business unit that may adversely affect the security of the premises.

- Ensure that all staff employed by the Trust, and staff from other organisations working within Burton Hospitals NHS Foundation Trust, contractors and official visitors, wear an ID badge at all times.

- Ensure that all staff are made aware of this Policy and fully understand its content and their responsibilities.

- Ensure that all staff ID access cards are correctly coded to permit access to areas of the Trust appropriate to their role.

5.8 **Staff**

Employees have a legal obligation to co-operate with management to achieve the aims, objectives and principles of this Policy. Great emphasis is placed on the importance of the co-operation of all staff in observing security and combating crime and ensuring their own and colleagues' safety in accordance with the Lone Worker and Conflict Resolution Policies.

5.8.1 Every member of staff has a responsibility to familiarise themselves with (additional information in Appendix A):

- Any special security requirements relating to their place of work or work practices.
- The action to take in the event of a security incident.
- To safeguard themselves, colleagues, visitors, patients, so far as is reasonably practicable and ensure that neither equipment nor property are put in jeopardy by their actions, either by instruction, example or behaviour.

- To follow prescribed working methods and security procedures at all times.
- To comply with all training requirements concerning security issues.
- To ensure the Trust identity badge is worn and visible whenever on Trust premises.
- To ensure that their security access card is safely stored and reserved specifically for their use only. Staff must not make their security access card available to any other person – staff, patients or visitors.

- Ensure staff do not permit tailgating into swipe access areas.

Additionally, staff should be aware of their responsibilities in protecting at all times, the assets/property of patients, visitors and that of the Trust. Where staff know or suspect a breach in security, they must report it immediately to their manager, the Estates Department if it is a breach of premises' security, the Governance Department if it concerns staff safety (or both if in doubt) and complete an incident form on Datix.

Staff are responsible at all times for the protection and safe keeping of their private property. If requested, the Estates Department and/or Governance Department will advise staff on the security of their property. Any loss of private property must be reported to their manager and Head of Health & Safety / LSMS without delay and comply with the Trust's **Incident and Serious Incident Management Policy and Procedure** If private property has been stolen, then it is the owner's responsibility, not the Trust's responsibility, to contact the police. However, the Trust will provide necessary assistance to the individual(s) affected.

All security related incidents must be reported on the Trust Datix system. These include, but are not limited to: thefts, damage to property, suspicious persons on site, insecure areas of the hospital and aggressive and violent incidents. **In addition deliberate physical assaults must be reported to the police immediately and to the Security Management Director or Head of Health & Safety/ LSMS at the earliest opportunity.**

5.9 Security Guards

Security Guards employees and contracted out will provide security assistance to all departments/staff as required.

Security Guards will periodically patrol the whole site, varying routes and complete a daily log.

5.10 Medical Records Manager

The Medical Records Manager or nominated person will be responsible for annotating paper records once an application for a marker has been approved by

the panel, and entering the relevant information into the VIP field. They will also ensure that it is entered into the medical alerts field by a clinical member of staff.

6. PERSONAL SAFETY AND PHYSICAL SECURITY OF PREMISES AND ASSETS

6.1 PERSONAL SAFETY AND SECURITY

6.1.1 The Trust recognises the problem of violence and aggression to staff as a major priority. The Trust is committed to providing a safe environment for staff and in addition has a Policy for the withdrawal of treatment in cases where violence is perpetrated by patients and members of the public, as specified in the Conflict Resolution Policy.

All staff must follow the existing Health and Safety policies and guidelines, and should be aware of all potential dangers.

6.1.2 Lone Worker Devices (LWD)

The Trust issues LWDs to members of staff that have been assessed as a lone worker and where they face the risk of violence.

All staff issued with a device are trained by contractors of the LWD who monitor all alarms initiated by staff.

Staff are advised to read and comply with the Lone Worker Policy available on the Trust Intranet.

6.1.3 Name Badge/Security I.D. Pass

The Trust has adopted a combined name badge/security pass, which is an integral part of the security arrangements within the Trust and will be worn and clearly displayed by **all** Trust staff. In addition non-Trust staff working on site, e.g. contractors, will be issued with temporary passes. For visitors the VIP and Official Visitor policy should be followed on the Trust intranet.

Agency/temporary staff will be required to demonstrate proof of identity on arrival. The responsibility for checking authenticity of agency membership will rest with the appropriate senior manager on duty at the time of arrival.

Estates contractors will be issued with a visitor's pass and a temporary access card by the Estates Department. Visitors to other departments should be issued with a visitor's pass by the relevant department. Passes should be returned to the issuing department prior to leaving the site.

Name badges **MUST NOT** be given to anyone else allowing them access through security doors, as this action is a security breach and may have disciplinary consequences.

All managers must ensure that all personnel have only got access to their required areas, specifically any "**CRASH TEAM MEMBERS**".

NOTE: IF ANY MEMBER OF STAFF FEELS THREATENED BY ANY PERSON, AND/OR FEEL THEY OR ANOTHER STAFF/ PATIENT IS AT ANY IMMEDIATE RISK OF HARM, THEY MUST PHONE FOR POLICE ASSISTANCE BY DIALING 999

6.2 SECURITY OF PREMISES AND ASSETS

6.2.1 Where possible, all departments should be secured when not in use. Risk assessments will be undertaken in accordance with section 10 of this policy. Only authorised personnel, who must complete the key register and sign their entry, should remove keys. Records should be auditable in cases where an investigation is subsequently required.

6.2.2 Closed Circuit Camera System (CCTV)

An integral component in providing the Trust with a secure environment is the installation of a closed circuit security camera system.

The use of cameras enables greater security coverage within hospital premises, thereby increasing safety. The Trust has external and internal cameras designed to deter and detect crime and safeguard staff, patients and visitors to the hospital.

All internal cameras are constantly recording onto media and reviewed accordingly.

Whilst crime within the Trust's premises in most instances is perpetrated by outside individuals, on rare occasions crimes are committed by members of staff. The anger and distress that is caused by these actions to staff can be very disconcerting, resulting in loss of confidence and in some instances disruption of services to patients. Whilst the Trust has not installed covert CCTV, it reserves the right to do so in conjunction with the police, when it would be beneficial not just to deter but, in rare selected instances, to catch offenders in the act, so that more appropriate action can then be taken.

Accordingly, the use of covert surveillance cameras in very special situations, in conjunction with the police, may be undertaken.

Look at the CCTV Policy of the intranet site for further information.

6.2.3 Lockdown Profiles for Trust Sites

Lockdown is the process of controlling the movement, access and egress of people around NHS property, or other specific building/area in response to an identified risk, threat or hazard that might impact on the safety and security of people and assets or, indeed the capacity of that facility to continue to operate.

A lockdown may be implemented by the Trust as part of a security incident or the major incident plan. This may be in partnership with other organisations both NHS and external e.g. due to Police intelligence.

Ward / Departmental managers may also need to be able to lockdown their own area e.g. in the event of a missing patient or a possible incident of violence and aggression within their area or department, where the manager decides to lockdown the area for safety and security of patients, staff, visitors, contractors and members of the public.

The Trust will produce a Lockdown plan for each of its hospital sites as follows:-

- Queen's Hospital Site
- Samuel Johnson
- Sir Robert Peel

This requires the Trust to ensure that a Risk Profile and Lockdown Plan is undertaken at each location to ensure that in the event of a decision to "lockdown" this can be implemented for all or part of a site. For further information see the Trust Lockdown Policy.

7. BREACHES OF SECURITY

Breaches of security will cause an unwanted disruption to clinical and operational services provided by the Trust, due to any loss or damage to Trust property, assets or injury to staff. Intentional breaches of security may have disciplinary implications towards members of staff. Breaches of security may include:

- Fraud
- Theft
- Vandalism

or

- Not reporting an act of fraud committed by another person
- Not reporting an act of theft committed by another person
- Not reporting an act of vandalism committed by another person
- Allowing unauthorised use of your, or somebody else's, swipe card
- A Trust member being in an unauthorised area

For more information on Fraud, refer to the Trust Anti-Fraud and Bribery Policy.

8. REPORTING OF CRIME/SECURITY INCIDENTS

8.1 Crime prevention/reduction must be the cornerstone of any security Policy. This entails:

- The systematic review of incidents to identify appropriate responses.
- The collective responsibility by all staff in ensuring their own and others' safety.

Incident reporting is the first step in the process:

- To establish the facts.
- To provide the basis of preventative measures.
- To ensure the basis and success of prosecution.
- To support the victim/s of crime.

This enables the development of a secure environment in which to meet the health needs of patients.

Where staff become aware of a breach of security, they must report the incident immediately to their respective manager and also the Head of Health & Safety/ LSMS.

Where a crime/security incident is of a serious nature, or is happening there and then, the **Police should be called immediately on 999.**

Any security incident, whether be reported on the Datix System as a matter of priority actual or perceived, should. Deliberate physical assault must be reported to the police immediately and to the Head of Health & Safety/ LSMS at the earliest opportunity.

Thefts or criminal incidents should also be reported to the police.

All department managers are responsible for ensuring all security related incidents are reported to the Trust's Head of Health & Safety/ LSMS at the earliest opportunity.

9. TRAINING

All appropriate front line staff **MUST** complete Conflict Resolution Training. (Refer to the Learning and Development intranet site).

Burton Hospitals NHS Foundation Trust has systems in place to ensure an appropriate response to incidents:

- Whereby trends are identified and risks assessed by recording all incidents on a dedicated security database.
- By audit review reports, indicating trends and the action to be taken to ensure compliance with all relevant security Policies.

Various courses are run by the Learning and Development Department to assist staff in dealing with various security issues e.g. Conflict Resolution.

All employee's MUST read all health and safety/security related policies and the appropriate health and safety/security risk assessments applicable to an individual's role.

10. PROCESS FOR CARRYING OUT RISK ASSESSMENTS

The Trust wide risk assessment process will be used to undertake risk assessments of the physical security of premises and assets. The risk assessments will be reviewed after an incident has occurred or when there is a change to the environment or a process. Where high risks are identified an action plan must be drawn up to address any gaps in the existing control measures. The plan must indicate who is responsible for what action and the timeframe to achieve this.

The Head of Health & Safety/ LSMS is available to provide advice to staff in the identification, assessment and management of security risks. Line Managers/ Heads of Departments/ Matrons must oversee this process and ensure that these are carried out at Ward/departmental level by competent persons. Generic risk assessments are generally not appropriate for different areas/departments but may be where services/functions are the same.

The department manager, on behalf of the Head of Health & Safety/ LSMS and the SMD, will collate all completed risk assessments. Any identified trends that highlight gaps in control measures to manage risks will be reported to the Risk & Compliance Group at quarterly meetings.

All appropriate assessments will be subjected to an audit in accordance to the Trust Health and Safety Self Inspection Process.

Risk assessor training is provided by the Head of Health & Safety and all assessors receive refresher training every 3 years.

11. AGGRESSIVE BEHAVIOUR MARKER

11.1 If there is an immediate threat, staff should follow local protocols to contact the internal security service or call the police.

11.2 The incident should be investigated by the department and the Manager who will liaise with the Head of Health & Safety/ LSMS to decide on an aggressive behaviour marker on the V6 system.

11.3 The following risk factors should be considered when determining whether a record should be marked:

- nature of the incident (i.e. physical or non-physical)
- degree of violence used or threatened by the individual
- injuries sustained by the victim
- the level of risk of violence that the individual poses
- whether an urgent response is required to alert staff
- impact on staff and others who were victims of, or witnessed, the incident
- impact on the provision of services
- likelihood that the incident will be repeated
- any time delay since the incident occurred
- the individual has an appointment scheduled in the near future
- staff are due to visit a location where the individual may be present in the near future
- the individual is a frequent or daily attendee (e.g. to a clinic or out-patients)
- the individual is an in-patient
- the incident, while not serious itself, is part of an escalating pattern of behaviour
- the medical condition and medication of the individual at the time of the incident

11.4 The CEO/SMD will be responsible for making the final recommendation on the need for a marker, based on incident reports, the nature and severity of the incident and consultations by the LSMS with the victim as soon as reasonably practicable after an incident.

See Appendix C for the Aggressive Behaviour marker flow chart and guidance.

11.5 For yellow or red warning for a patient, follow the Conflict Resolution Policy.

12. EFFECTIVE MONITORING

12.1 The table at Appendix B highlights the minimum requirement as evidence of compliance for the NHSLS Standards.

13. EQUALITY AND DIVERSITY

13.1 There will be no discrimination against any member of staff.

14. STAFF SUPPORT

Staff who feel traumatized by an incident which may have affected them can obtain support from local management.

Additional support will be offered by the Occupational Health Department.

Appendix A

GUIDELINES FOR MANAGERS AND STAFF

HOW TO MEET YOUR RESPONSIBILITIES UNDER THIS POLICY

1. What will my manager do to meet his/her responsibility?

- Communicate the Policy and related safety and security information to you, providing instruction and training as appropriate.
- Consult with you, other staff and Health and Safety representatives to ensure that appropriate risk assessments are undertaken, taking account of the risks inherent in your job and the environment.
- Regularly review risk assessments in light of changing working practice. Consultation with Health and Safety representatives is essential whenever changes in workplaces or new workplaces are under discussion.
- Establish pro-active safe systems of work that either eliminate, or where this is not feasible, minimise particular risks that arise from your job.
- Demonstrate through the production of risk assessments and safe systems of work that he/she has acted upon the requirements of the Policy.
- Demonstrate that you and other staff have received and understood information and instruction regarding the risk assessments and safe systems of work, so that you are aware of local security protocols and working practices.
- Ensure that emergency procedures are established and that you are adequately trained and informed and have appropriate access to first aid provisions, and means of communication, so that you can respond correctly in emergency situations.
- Ensure that incidents are correctly reported, contacting other professionals (e.g. Head of Health & Safety / LSMS where appropriate.
- Ensure that incidents are fully investigated and that actions are taken, where possible, to prevent a recurrence.
- Ensure that you are given the necessary time to attend relevant training events on this subject.

2. What must I do to meet my responsibilities?

- Read this Policy and co-operate with its principles.
- Take reasonable care of your own health and safety and that of others, which might be affected by your acts or omissions.
- Not knowingly put yourself or others in “at risk” situations.
- Take part only in those activities for which you are trained and authorised to act.
- Ensure that management are kept informed of any change in your health which may affect your ability to work safely.
- Assist with, or initiate the risk assessment process as appropriate, including any changes in risk.
- Co-operate with any safe systems of work that arise from risk assessments being carried out.
- Ensure that you are available for any necessary training in order to lessen the hazards associated with your job, including risk assessment.
- Keep informed of emergency procedures established by management.
- Report any incidents, concerns or dangerous occurrences with regard to security to your manager and on the Datix incident reporting system.
- Be available to co-operate with any investigation of an incident and comply with actions taken from the outcome.
- Report the failure of equipment/safe systems etc.

3. I am concerned about my safety and security - what should I do?

- Report your specific concern to your manager, or their next in line senior manager, in the first instance. Also refer back to the other policies and procedures available to report incidents or safety issues.
- Contact the Trust Head of Health & Safety/ LSMS.

APPENDIX B

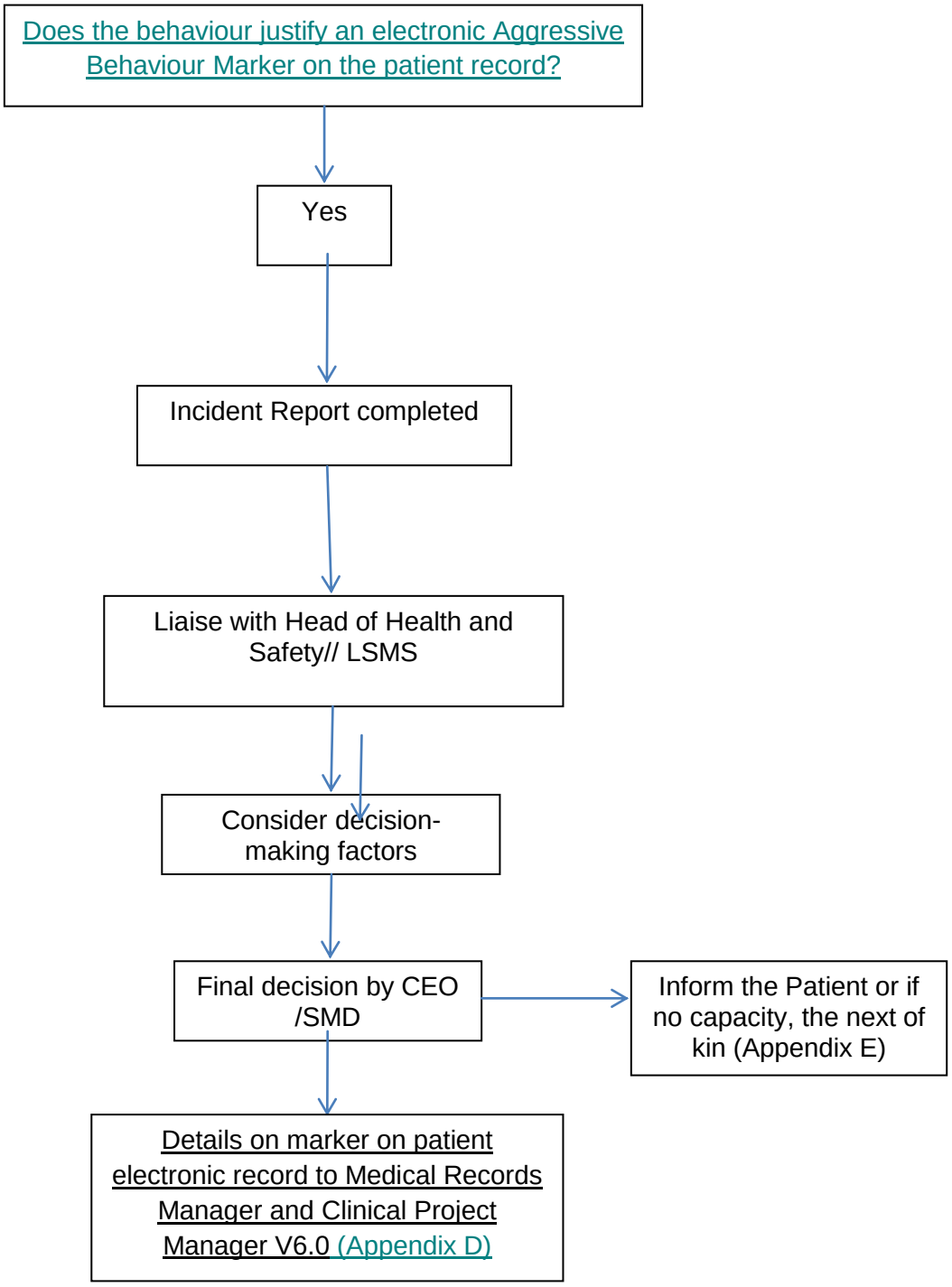
Monitoring Matrix

Minimum policy requirements to be monitored	Process for monitoring e.g. audit	Responsible Individual/ Committee/Group	Frequency	Responsible Individual/ Committee/Group for review of results	Responsible Individual/ Committee/Group for development of the action plan	Responsible Individual/ Committee/Group for monitoring of the action plan
How the Trust risk assesses the physical security of premises and assets	Every department risk assessor completes a security risk assessment. H&S Self Inspection with policy and risk assessment compliance procedure	Head of Health &S afety	Initial compliance audit followed by a 6 month review then annual reviews. Health & Safety Group quarterly	Health and Safety Group (HSG)	Department Managers	Department Managers
How action plans are developed as a result of risk assessments	Every department manager is responsible for completing an action plan following the risk assessment	Head of Health & Safety	Initial compliance audit then annual reviews. HSG quarterly	Health and Safety Group (HSG)	Department Managers	Department Managers

	process (where applicable). H&S Self Inspection with policy and risk assessment compliance procedure					
How action plans are followed up	All action plans (where applicable) are managed by department managers. H&S Self Inspection with policy and risk assessment compliance procedure	Head of Health & Safety	Initial compliance audit then annual reviews. HSG quarterly	Health and Safety Group (HSG)	Department Managers	Department Managers

APPENDIX C

Aggressive Behaviour Marker procedure



APPENDIX D

BURTON HOSPITALS NHS FOUNDATION TRUST

AGGRESSIVE BEHAVIOUR MARKER APPLICATION FORM

Patient or associate's Name		
Patient or associate's address		
Hospital number:		**Date of Birth:**
Nature of incidents	**Physical: Deliberate / Non Deliberate**	
	Verbal: Deliberate / Non Deliberate	
No of previous incidents		
Description of incident		
Nature of underlying clinical condition		
Severity of incident(s)	**Low - 1 – 2 – 3 – 4 – 5 – High**	
Signature LSMS	**Approved**	**Refused**
Signature of MD	**Approved**	**Refused**
	Notification Letter	**YES / NO**
Signature CEO	**Approved**	**Refused**
	Notification Letter	**YES / NO**
Date marker applied __/__/____		**Date of Review** __/__/____

APPENDIX E

Aggressive Behaviour Marker Notification Letter

Dear (patient or associate's name)

Notification of an aggressive behaviour marker is being placed on your NHS patient record

I am writing to you from Queen's Hospital, Burton upon Trent where I am the Head of Health & Safety/ Local Security Management Specialist (LSMS). Part of my role is to protect the Trust staff from abusive and violent behaviour and it is in connection with this that I am contacting you.

(Insert summary of behaviour complained of, include dates, effect on staff/services and any police/court action if known)

Behaviour such as this is unacceptable and will not be tolerated. Queen's Hospital, Burton upon Trent is firmly of the view that all those who work in or provide services to the NHS have the right to do so without fear of violence, threats or abuse.

The NHS Constitution makes it clear that just as the NHS has a responsibility to NHS service users, so service users have a responsibility to treat staff with respect and in an appropriate way.

All employers have a legal obligation to inform staff of any potential risks to their health and safety. One of the ways this is done is by marking the records of individuals who have in the past behaved in a violent, threatening or abusive manner and therefore may pose a risk of similar behaviour in the future. Such a marker may also be placed to warn of risks from those associated with service users (e.g. relatives, friends, animals, etc).

I have carefully considered the reports of the behaviour referred to above and have decided that a risk of aggressive behaviour/violence marker will be placed on your records.

This information may be shared with other NHS providers we jointly provide services with (e.g. ambulance trusts, social services and NHS pharmacies) for the purpose of their health and safety.

This decision will be reviewed in 12 months' time from the date of this letter and if your behaviour gives no further cause for concern this risk marker will be removed from your records. Any other provider we have shared this information with will be advised of our decision.

Yours sincerely,

Head of Health & Safety/ LSMS
Rasila Sarda