AGENDA ITEM NO:

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 22 DECEMBER 2011

Title:	**APPROVAL OF POLICIES**
Responsible Director:	David Burbridge, Director of Corporate Affairs
Contact:	Louisa Bailey, Senior Manager Corporate Affairs

Purpose:	To seek the Board of Directors approval for the following policies: • Risk Management Policy (appendix A) • Security Policy (including The Prevention and Control of Violence & Aggression) (appendix B) • Policy for the Development and Management of Controlled Documents (appendix C)
Confidentiality Level & Reason:	None
Medium Term Plan Ref:	N/A
Key Issues Summary:	The Policies have been reviewed by the Policy Review Group considered them compliant with the Policy for the Development and Management of Controlled Documents, and recommends that it be approved. The approved policy will be notified to all relevant stakeholders by e-mail and will be put onto the Intranet.
Recommendations:	The Board of Directors is asked to consider and if thought fit, approve the following policies: • Risk Management Policy (appendix A) • Security Policy (including The Prevention and Control of Violence & Aggression) (appendix B) • Policy for the Development and Management of Controlled Documents (appendix C)

Signed:	**Date:** 16 December 2011

APPENDIX A

University Hospitals Birmingham NHS

NHS Foundation Trust

CONTROLLED DOCUMENT

Risk Management Policy

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE:	To set out the principles and framework for the management of risk with University Hospitals Birmingham NHS Foundation Trust.
Controlled Document Number:	**120**
Version Number:	**Draft 9 Version 3**
Controlled Document Sponsor:	Director of Corporate Affairs
Controlled Document Lead:	Risk Management Advisor
Approved By:	Board of Directors
On:	
Review Date:	
Distribution: • **Essential Reading for:** • **Information for:**	 All Directors, Senior Managers and Department Heads All Staff

Risk Management Policy

Contents

1 Policy Statement

1.1 Risk Management is essentially the process where an organisation adopts a proactive approach to the management of future uncertainty and facilitates the evaluation and control of risk.

1.2 The Trust recognises that the provision of healthcare and the activities associated with the treatment and care of patients, employment of staff, maintenance of premises and managing finances, by their nature, incur risks. The Trust accepts its corporate responsibility to provide the highest standards of patient care and staff safety, and as such, the process of Risk Management is viewed as an essential component in maintaining and improving standards at the Trust.

1.3 The objective of this policy is to ensure that the Trust has an effective system for identifying and managing risks with the aim of:

1.3.1 achieving its objectives;

1.3.2 protecting patients, staff and members of the public; and

1.3.3 protecting assets.

2 Scope

This policy applies to all areas and activities of the Trust and to all individuals employed by the Trust including contractors, volunteers, students, locum and agency staff and staff employed on honorary contracts.

3 Framework

3.1 This section describes the broad framework for the management of risk. Operational instructions for risk management, investigation of incidents, and learning from incidents are detailed in separate procedural documents which are approved by the Director of Corporate Affairs

3.2 Definitions

3.2.1 **Risk** is the likelihood of a hazard resulting in an incident set against the severity of that incident if it does occur. In terms of the healthcare environment risk means the possibility of injury, harm or loss to patients, staff, visitors or the structural/financial integrity of the organisation.

3.2.2 **Control** is the mitigating action put in place to reduce the risk.

3.2.3 **Hazard -** A hazard is something (e.g. an object, a property of a substance, a phenomenon or an activity) that can cause adverse effects

3.3 Risk Management Structure

3.3.1 Appendix 2 provides the Risk Management Reporting Framework; this framework identifies the reporting mechanism within the Trust to ensure that the Board is assured that Risk Management processes are in place and effective.

3.3.2 The Board of Directors shall conduct an annual review of the effectiveness of the Trust's system of internal controls, which shall be reflected in the Annual Governance Statement (AGS) that is published in the Annual Report. The Board will receive the Audit Committee minutes and an Audit Committee annual report which provides assurance to the Board on the risk management process in the Trust.

3.3.3 The Board has delegated authority to the Audit Committee to oversee risk management on its behalf. The Audit Committee will receive quarterly Risk Management Reports which include trends data in relation to incidents including Serious Incidents Requiring Investigation; as well as results of the quarterly Risk Register compliance audit.

3.3.4 The Terms of Reference for the Audit Committee identify the role of the Audit Committee and its responsibility for risk management within the organisation.

3.4 Managing Risks within the Trust

3.4.1 The risks in a health care environment are significant and ever changing. Risk must be managed through the systematic analysis of actual and potential risks and the development and implementation of measures to counteract those risks.

3.4.2 There are corporate risks inherent in the financial and contractual stability of the Trust; the Trust must seek to manage risks that threaten its ability to achieve its business objectives.

3.5 Risk Management is made up of three stages:

3.5.1 Risk identification

3.5.2 Risk analysis

3.5.3 Risk control

3.6 Risk identification

3.6.1 Risks can be identified from a number of the following sources (this list is not exhaustive):

a) Incidents;

b) Complaints;

c) Claims; and

d) General observations

3.6.2 Once a risk has been identified the risk must be assessed and reviewed in accordance with the Procedure for the Development and Management of Risk Registers and Risk Assessments (see section 3.7 below).

3.6.3 Appropriate risk assessments must be carried out when new activities are contemplated by the person responsible for that activity.

3.6.4 All identified risks must be recorded by the Risk Register owner on the appropriate risk register in accordance with the procedure for the Development and Management of Risk Registers. The hierarchy of risk registers within the Trust is as follows (see Appendix 3):

a) Board Assurance Framework

b) Executive Director Risk Registers

c) Divisional Risk Registers

d) Speciality and Corporate Area Risk Registers

e) Ward/Department Risk Registers

The Procedure for the Development and Management of Risks Registers provides details on how these are to be populated and what type of risks should be on each risk register.

3.6.5 All risks will be escalated from the relevant risk register in accordance with the Procedure for the Development and Risk Management of Risk Registers.

3.7 Risk analysis

3.7.1 For each risk identified, a reasonable estimate must be made of its likely occurrence and its likely consequences[1] with no controls in place. This analysis will identify the “Initial Risk”.

3.7.2 Risks to Trust objectives, structural or financial integrity or Trust assets must be assessed to identify the likely consequences for the Trust.

3.7.3 Risks to patients, staff or visitors must be assessed both in terms of the consequences for those patients, staff or visitors and the consequences to the Trust. Analysis of consequence and likelihood provides the risk significance enabling a list of prioritised risks to be developed. The Procedure for the Development and Management of Risk Registers and Risk Assessments provide further detail.

3.8 Risk Control

3.8.1 The Board of Directors shall determine the level of risk tolerance that is deemed to be acceptable to the Trust and review this as required, but no less often than every three years.

3.8.2 The level of acceptable risk is set out in the Procedure for the Development and Risk Management of Risk Registers.

3.8.3 All risks above this level must either have controls set up that will eliminate the risk or reduce the risk to or below that level or the Trust must consider whether the activity associated with that risk should be continued. Divisional Management Teams must also ensure that any risks quantified as high should have controls and action plans in place. Any high level risks that cannot be controlled within the Divisional/Specialty structure should be escalated to the relevant Executive Directors for consideration of actions to be taken; that may be to accept the risk; to allocate resource mitigate the risk or to discontinue the activity to negate the risk.

3.8.4 The Risk Management Team will identify high and significant level risks to the relevant Divisional Management Team for them to decide whether this risk should be escalated to an Executive Director.

3.8.5 Existing controls must be reviewed on a quarterly basis as a minimum for speciality/divisional risk registers and

[1] The method of analysing risk is based on an adaptation of the Australian/New Zealand Risk Management Standard AS/NZ 4360:1999.

bi-annually for ward/departmental risk registers to ensure that they remain effective or can be discontinued if no longer required. Where existing controls are considered not to be effective the existing action plan should be developed further to implement new or enhanced controls in order to reduce the level of risk over an appropriate time scale.

3.9 Incident Reporting

3.9.1 For Risk Management to be effective, staff must report all adverse incidents and near misses that they have been involved in or witnessed. If all incidents including near misses are reported, areas of potential risk can be identified and any trends analysed.

3.9.2 The Policy for the Reporting and Management of incidents including Serious Incidents Requiring Investigation, the Procedure for the Development and Management of Risk Registers and the Procedure for the Reporting and Investigation of Incidents provide further details.

3.10 **Training**

3.10.1 All Board members, including Non-Executive Directors, and Senior Managers (which, for the purpose of this policy means those directors reporting directly to the Chief Executive and their deputies, Divisional Directors, Directors of Operations and Associate Directors of Nursing) will be provided with risk awareness training within 6 months of the commencement of their role. An individual who has undergone this training before is not required to repeat it on a move to a new role.

3.10.2 The process for ensuring compliance with this training requirement, including recording of attendance and following up of non-attendance is set out in the Procedure for Board/Senior Manager Risk Awareness Training.

3.10.3 Risk awareness training for all other staff shall be provided as set out in the Trust’s Training Needs Analysis document.

3.10.4 Where there are changes to risk management standards further refresher training will provided if necessary.

4 **Duties**

4.1 **Director of Corporate Affairs**

The Director of Corporate Affairs is responsible for ensuring that the Trust's obligations for Risk Management are discharged accordingly and that Risk Management principles are embedded throughout the Trust. This includes compliance with the NHS Litigation Authority Risk Management Standards and UK law.

4.2 **Director of Finance**

The Director of Finance is responsible for ensuring the effective operational management and strategic development of all financial risks. This includes the Standing Financial Instructions.

4.3 **Chief Operating Officer**

The Chief Operating Officer is responsible for ensuring that effective operational arrangements are in place throughout the Trust and across both sites. This includes the management of operational risks.

4.4 **Director of Delivery**

The Director of Delivery has responsibility for ensuring the effective operational management of all Human Resources and Health and Safety Risks. This includes compliance with Health and Safety Executive (HSE) guidance and UK legislation.

4.5 **Medical Director**

The Medical Director has responsibility for ensuring the effective operational management of all relevant professional risks.

4.6 **Chief Nurse**

The Chief Nurse has responsibility for ensuring the effective operational management of all relevant professional risks. The Chief Nurse also has responsibility for the management of infection control, patient involvement, and the Patient Advice and Liaison Service.

4.7 **New Hospital Project Director**

The New Hospital Project Director has responsibility for the risks associated with the real estate, new hospital and retained estate.

4.8 All the above directors are responsible for ensuring that the members of the Board of Directors are informed of the appropriate risks.

4.9 **The Clinical Governance Support Unit**

4.9.1 The Clinical Governance Support Unit is responsible for ensuring collation of evidence to demonstrate compliance with the Essential Standards of Quality and Safety and the NHS Litigation Authority Risk Management Standards.

4.9.2 The Risk Management Team as part of the Clinical Governance Support Unit has responsibility for supporting the implementation of risk management activities throughout the Trust providing a support role to Divisional management. They also provide support for other committees within the Trust as required.

4.9.3 The Risk Management Team undertakes an audit of compliance with the Risk Register process on a quarterly basis.

4.10 All managers

4.10.1 All managers/directors must:

a) Ensure all necessary risk assessments are carried out within the Division/Group/Department and appropriate control measures are implemented and monitored.

b) Ensure all employees are aware of the risks within their work environment and of their personal responsibilities. They must also be given the necessary information, instruction, supervision and training to enable them to work safely. These responsibilities extend to anyone affected by the Trust's operations including sub-contractors, members of the public, visitors etc.

c) Ensure that inspection, testing and maintenance of equipment used within their areas of managerial control is carried out in accordance with legislative requirement and are responsible for ensuring all risks identified are minimised as far as is reasonably practicable.

d) Ensuring risks identified are populated within the relevant risk register according to the management level. See the Procedure for the Development and Management of Risk Registers.

4.11 Head of Governance

The Head of Governance has responsibility for implementation of all aspects of governance, clinical effectiveness and risk management, through the management of the Governance and Risk Management Teams.

4.12 Risk Management Advisor

The Risk Management Advisor has responsibility to achieve high standards of risk management for the Trust, including the implementation of the Trust's Risk Management Policy. They are responsible for the continuing development of a proactive risk management culture and practice throughout the Trust; actively promoting and ensuring good risk management practices, an open, just and fair culture and the achievement of national risk management standards and performance indicators.

4.13 All Employees

4.13.1 All employees must:

a) comply with all Trust rules, regulations and instructions;

b) work in a manner which is safe and secure for themselves, colleagues, patients and visitors.

c) take reasonable care for their own safety and the safety of others who may be affected by their acts or omissions;

d) undertake safe clinical practice in diagnosis and treatment;

e) comply with Divisional/Group/ Departmental clinical procedures; and

f) neither intentionally or recklessly interfere with or misuse any equipment provided for the protection of health and safety.

4.13.2 Any employee who fails to comply with the Trust or local policies or guidelines on risk, or recklessly interferes with or misuses any equipment, provided for the protection of health and safety, will be subject to disciplinary action.

5 Implementation and Monitoring

5.1 The Policy and the associated procedural documents will be available on the Trust intranet. The policy will also be disseminated through the management structure within the Trust.

5.2 The Risk Management Team and the Health and Safety Team will provide consistent advice and guidance to managers and staff on the application of this policy and its procedures.

5.3 See Appendix 1 for details of monitoring

6 References

6.1 Australian/New Zealand Risk Management Standard AS/NZ 4360:1999

6.2 NHSLA Risk Management Standards

6.3 Care Quality Commission Essential Standards of Quality and Safety

7 Associated Policy and Documentation

7.1 Policy for the Reporting and Management of incidents including Serious Incidents Requiring Investigation

7.2 Procedure for the Development and Management of Risk Registers and Risk Assessments

7.3 Procedure for the Reporting and Investigation of Incidents

7.4 Procedure for the Management of Serious Incidents Requiring Investigation

7.5 Health and Safety Policy

7.6 Procedure for Board/Senior Manager Risk Awareness Training

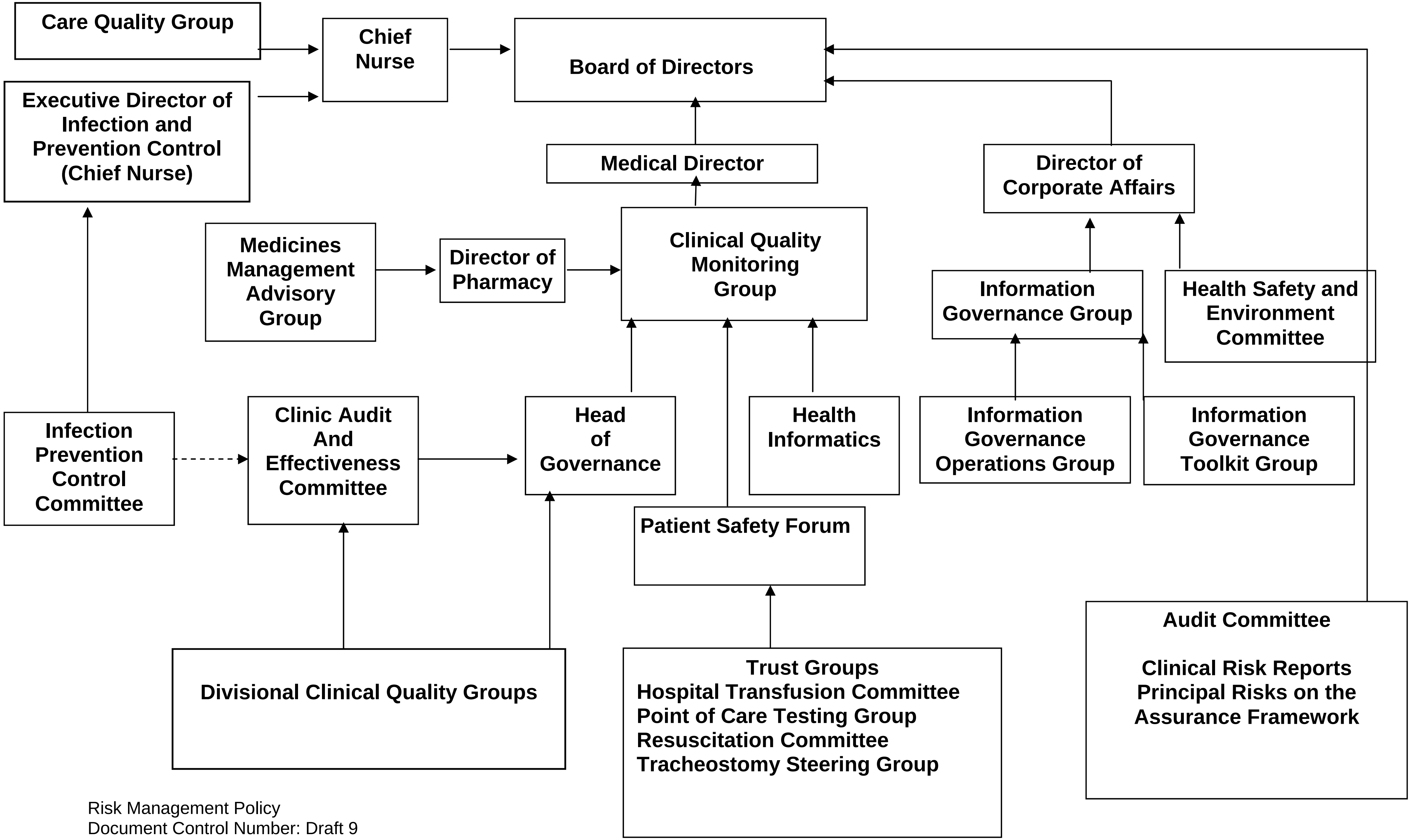
Monitoring **Appendix A**

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
Risks are managed in accordance with the risk management structure and reported to the BoD and Audit Committee Appropriately and managed appropriately locally and by the right people at all levels.	Risk Management Advisor	DCA Governance Group	Review of risk registers to ensure risks are being populated according to the structure and managed and escalated at the right level. Also review the risk registers to ensure key individuals involved in risk management are complying with their duties. Review Reports that go to BoD and Audit and provide assurance that the BoD and Audit receive relevant reports	Quarterly
Senior Managers and BoD members receive the relevant Risk Management Training	Risk Management Advisor	DCA Governance Group	Training records will be reviewed by the Risk team and It will be reported on an exception basis if the process outlined in the Procedure for Board/Senior Manager Risk Awareness Training is not adhered to. This will include identifying those who have not received the relevant training	Quarterly
Internal Auditors carry out an annual audit programme to provide assurance regarding risk management process	Director of Corporate Affairs	Audit Committee	Annual Audit programme	Annual

Compliance with the Risk Register and Risk Register Process is monitored.	Risk Management Advisor	Audit Committee	Audit of Specialty and Divisional compliance with Risk Register and Risk Assessment process	Quarterly

Risk Management Reporting Framework

Appendix B



Care Quality Group

Chief Nurse

Board of Directors

Executive Director of Infection and Prevention Control (Chief Nurse)

Medical Director

Director of Corporate Affairs

Medicines Management Advisory Group

Director of Pharmacy

Clinical Quality Monitoring Group

Information Governance Group

Health Safety and Environment Committee

Infection Prevention Control Committee

Clinic Audit And Effectiveness Committee

Head of Governance

Health Informatics

Information Governance Operations Group

Information Governance Toolkit Group

Patient Safety Forum

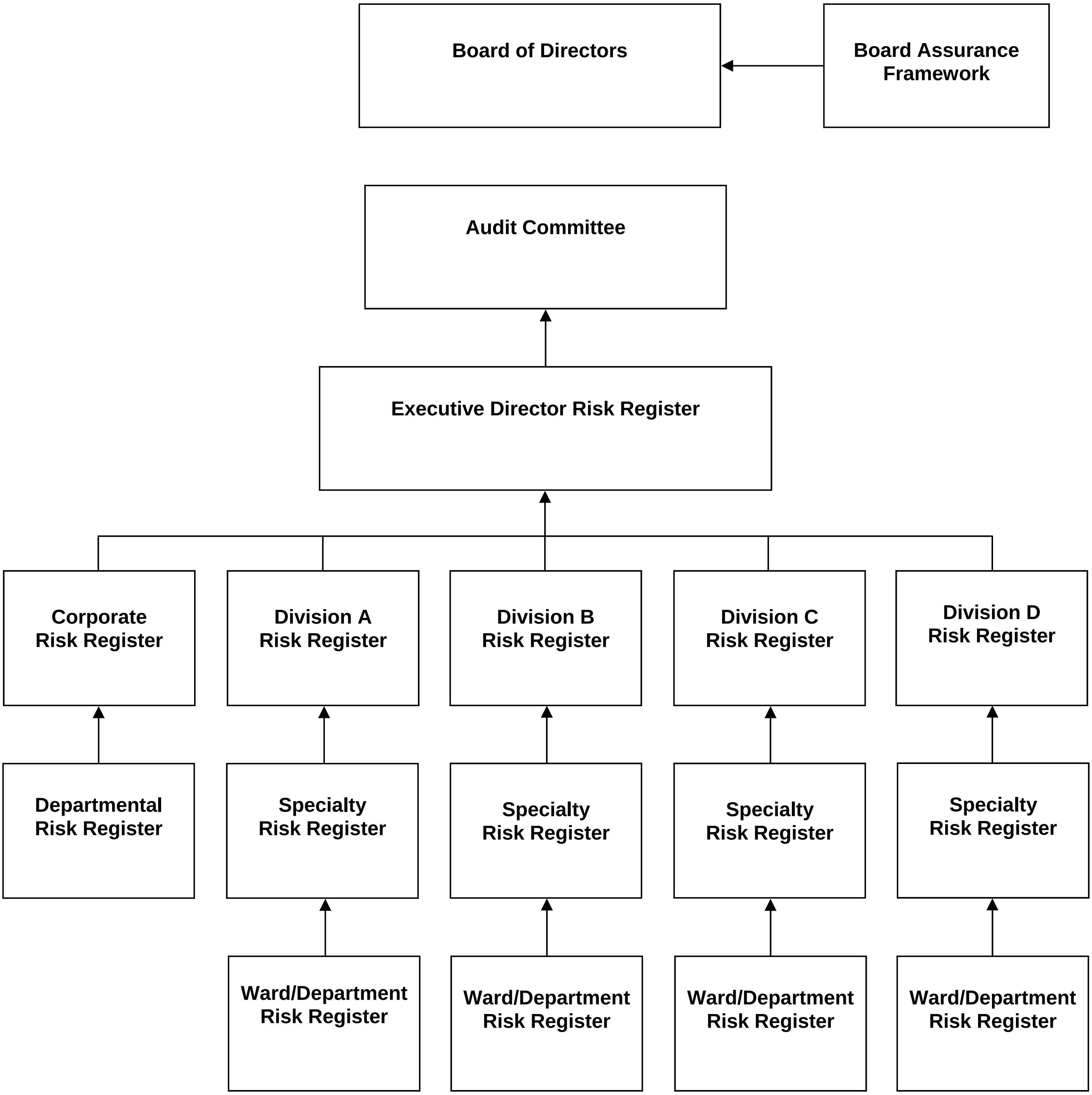
Divisional Clinical Quality Groups

Trust Groups
Hospital Transfusion Committee
Point of Care Testing Group
Resuscitation Committee
Tracheostomy Steering Group

Audit Committee

Clinical Risk Reports
Principal Risks on the Assurance Framework

Appendix C Risk Register Flowchart



APPENDIX B

CONTROLLED DOCUMENT

University Hospitals Birmingham NHS
NHS Foundation Trust

Security Policy (including The Prevention and Control of Violence & Aggression)

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE	To set out the principles and framework for the management of Security within the Trust, to ensure that all staff understand their roles and responsibilities.
Controlled Document Number:	**146**
Version Number:	**4**
Controlled Document Sponsor:	New Hospitals Project Director
Controlled Document Lead:	Trust Security Management Specialist
Approved By:	Board of Directors
On:	
Review Date:	
Distribution: • **Essential Reading for:** • **Information for:**	All Trust Staff

Contents

1 Policy Statement

1.1 The Trust is committed to providing a safe and secure environment for patients, visitors, staff and all workers engaged within the Trust. In particular, the Trust will not tolerate harassment, violence and/or aggression without lawful justification or excuse.

1.2 The objective of this policy is to ensure that the Trust provides a secure and safe environment which minimises security risks to all patients, staff and visitors alike and also protects the property, assets, service delivery and the reputation of the Trust so that:

1.2.1 There is a safe and secure environment with regards to persons, functionality and physical assets;

1.2.2 There is a unified, structured and proactive approach to the management of security and violence and aggression within the Trust with all due consideration of legislative, regulatory and mandatory obligations; and

1.2.3 All persons are aware of their roles, responsibilities and obligations with regards to security matters;

2 Scope

2.1 For the purposes of security this policy applies to all Trust staff, including Contractors, Agency and Locum workers as well as those undertaking secondments whether they are involved in Trust business whilst on any property owned or controlled by the Trust or off Trust premises. Nominated managers must therefore ensure that any non employed workers are aware of the requirements of this policy and the associated procedures and how to apply them.

2.2 The policy is applicable in all of the following circumstances:

2.2.1 Violence from staff towards, other staff, patients and visitors/public

2.2.2 Violence from Patients to staff, other patients and visitors/public

2.2.3 Violence from Visitors/public to staff, patients and other visitors/public

2.3 Definitions

Within the context of this policy the following definitions, taken from NHS Protect guidance, are used:

2.3.1 assault is described as `the intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort'; and

2.3.2 Verbal aggression is `the use of inappropriate words or behaviour causing distress and/or constituting harassment`.

3 Framework

3.1 This section describes the broad framework for the Security Policy. Detailed instructions are provided in the associated procedural documents.

3.2 The New Hospitals Project Director shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

3.3 Security – General

In order to achieve a safe and secure environment for all, the Trust shall:

3.3.1 Ensure that risks are properly identified, assessed, and that appropriate mitigation measures are put into place ("Security Risk Assessments") in accordance with the Security Procedure;

3.3.2 Make available appropriate resources to implement this policy effectively. The Trust's security service for the main sites is provided by Balfour Beatty Workplace, (BBW), who have a dedicated security manager with overall responsibility for BBW security staff;

3.3.3 Clearly set out the responsibilities of staff at all levels;

3.3.4 Provide guidance on how to manage security issues and incidents;

3.3.5 Monitor the effectiveness of such measures taken and to make any necessary amendments to policies and procedures;

3.3.6 Provide suitable support, advice and guidance to those involved and exposed to security incidents; and

3.3.7 Sustain positive relationships with other key stakeholders e.g. law enforcement organisations, neighbours, the National Counter Fraud and Security Management Service, the Health and Safety Executive and other regulatory bodies

3.4 Management of Violence and Aggression

For all incidents of violence and aggression the Trust will ensure, where appropriate, that:

3.4.1 potential triggers to violence and aggression are risk assessed as part of the security risk assessments;

3.4.2 reasonable measures to reduce the likelihood of violence and aggression are devised and implemented to address specific risks;

3.4.3 consideration is given to excluding patients/public who present an unacceptable risk in accordance with the Withholding Treatment Procedure;

3.4.4 specialist advice on appropriate control mechanisms will be provided by the Security Management Specialist and/or Health and Safety Adviser;

3.4.5 support is provided to any member of staff involved in an incident of violence or aggression;

3.5 Where staff are either violent and/or verbally aggressive the Trust's Disciplinary procedure will be followed.

3.6 Where a patient is subject to violence and or verbal aggression from another patient and or a member of the public and it appears that there is a safeguarding risk the Trust's Safeguarding Policy shall be adhered to.

3.7 All incidents of violence and aggression will be reported to the Trust Security Management Specialist and BBW Security who will manage the incident. Police should be informed should a criminal offence be committed and all security involvement will be documented.

3.8 The instructions provided in the associated Prevention and Control of Violence and Aggression Procedures shall be followed.

3.9 **Major Incidents and Serious Threats**

3.9.1 The Trust Major Incident Plan may be implemented in the event of a major security incident.. In such circumstances, this plan will supersede or enhance the security measures outlined within this policy and associated procedures.

3.9.2 Serious threats, including terrorist threats, to the Trust will be assessed and appropriate measures will be implemented commensurate with the nature and level of risk.

3.9.3 The implementation of general preventative measures will reflect the five national levels of threat, ranging from low (i.e. unlikely attack) to critical (i.e. expected imminent attack) and will include an increase in the frequency of BBW Security's preventative patrols in the event of a rise in the national threat level. The security patrols are to be recorded in the security log.

3.9.4 If the Trust is advised by the County Terrorism Security Advisors of a specific terrorist threat or other serious threat to the Trust or health bodies generally, the Trust Security Management Specialist will inform BBW Security and BBW will assess the individual risk and put in place measures to counteract the risk.

3.10 **Lock-down**

3.11 A lock down procedure enables an entire building/site or parts of the building/site to be locked down in the event of a serious incident. The TSMS shall, in conjunction with BBW Security where appropriate, ensure that a lock down procedure, approved by the Executive Director for Security Management, is in place for each site/building under the Trust's control by 31 December 2011 or, if later, within six months of the date on which the Trust takes control of a building/site. Lockdown can only be authorised by the Hospital On-Call Manager or the Major Incident Command Control Centre Manager. The Trust's Lock Down Procedure provides full details of the lock down for each site.

3.12 Management of Security Incidents

The Trust will report any security incidents to BBW and also report details of the incident on the Trust incident reporting system. The Trust and BBW shall respond to all Security Incidents. The Trust shall monitor BBW's level and nature of response to ensure that it is appropriate to each particular security incident.

The incidents will be documented by BBW and TSMS will be informed on a weekly basis or, in the event of a Major Incident, as soon as practicable

3.13 Security of Trust Assets

3.13.1 All Managers are responsible for the safety and security of all Trust assets within their area of responsibility. This responsibility includes carrying out a local risk assessment and putting in place suitable security measures for when the equipment is in storage.

3.13.2 Equipment must not be removed from its intended point of use or safe storage without permission from a suitably authorised person.

3.13.3 All materials and equipment must be used, stored and maintained in accordance with their intended purpose and manufacturer's recommended instructions.

3.14 Identification Badges and Access Control Cards

All Trust staff must display authorised Trust identity badges at all times when on duty. Routine stop-checks will be undertaken by BBW security.

3.15 Key Management

All Wards and Departments are responsible for implementing a safe and secure system for the management of keys that are issued for their use as part of local security procedures. BBW will put in place a secure, robust and fully auditable system for the management and distribution of keys used by security, including master sets.

3.16 Termination of Employment

Upon termination of employment, Line Managers shall ensure that the individual returns all Trust assets which will include: all equipment, uniforms, ID badges, Access/Smartcards, keys and car parking permits. BBW security office must be informed to ensure that all access control permissions are removed.

3.17 Lone Working

Nominated Managers shall be responsible for identifying any staff who are subject to lone working and completing a risk assessment. They will develop and agree suitable working practices, in accordance with the Trust Lone Worker guidelines including the consideration to the issue of `Reliance` lone worker alarms.

3.18 Intellectual Property and Security of Information

3.18.1 Staff are required to respect confidentiality of information and must adhere to the Trust's Information Governance policies and procedure.

3.18.2 It is the responsibility of all staff to ensure that information is kept secure.

3.18.3 Staff are required to comply with the Trust policies and procedures associated with the security of computer hardware and information technology.

3.19 Security of Trust Vehicles

3.19.1 All vehicles owned or leased by the Trust must only be used by authorised personnel and doors and windows locked when left unattended. Keys must be in the possession of the driver at all times.

3.19.2 All items contained within a vehicle must be appropriately stored and concealed from public view, so far as is reasonably practicable.

3.20 Car Parking

3.20.1 All vehicles parked on Trust property shall be at the owners risk and the Trust will not be held liable for any damage, however caused.

3.20.2 All drivers are required to abide by the terms and conditions that are contained within the Trust's Traffic Management Policy and any associated procedures.

3.21 Waste and Hazardous Items

All waste including potentially hazardous items must be segregated, handled, contained, secured and stored in accordance with the Trust's Waste Policy and its associated procedure.

3.22 Patient Property

All property bought into the Trust will be managed in accordance with the patient property procedures.

3.23 Training

The Trust will ensure security and violence and aggression awareness training, including conflict resolution training, is provided in accordance with the Trust Training Needs Analysis.

4 Duties

4.1 Executive Director for Security Management

4.1.1 In accordance with the requirements of the Secretary of State for Health, the New Hospitals Project Director has been appointed as the Trust's Security Management Director (SMD). The post holder shall act on behalf of the Board of Directors as the named Director with overall responsibility for Security Management arrangements within the Trust.

4.1.2 They shall provide assurance to the Board of Directors on compliance with this policy and report any material failures of compliance or other security concerns including violence and aggression.

4.2 Head of Technical Services and Construction

The Head of Technical Services and Construction (HTSC) shall have responsibility for the planning and delivery of security management arrangements.

4.3 Trust Security Management Specialist

The Trust's Security Management Specialist (TSMS) will be responsible for co-ordinating and delivering a professional operational security management service. In so doing, the post holder shall:

4.3.1 ensure that BBW has completed a security risk assessment for all Trust sites;

4.3.2 ensure BBW carry out the site security risk assessments;

4.3.3 Provide specialist support, advice and assistance in relation to all security and violence and aggression matters;

4.3.4 Develop and implement appropriate Trust-wide security policies and procedures;

4.3.5 Monitor and support the development of localised operational security procedures within all areas of the Trust;

4.3.6 Act as the main point of contact with the National Counter Fraud & Security Management Service, law enforcement agencies and other such organisations;

4.3.7 Monitor security equipment to ensure that it is functional and appropriately maintained;

4.3.8 Liaise with the Police where necessary and to provide information on identified perpetrators of violence and other crime;

4.3.9 Collate and analyse reported security incidents, identifying trends in the interventions required of security staff in respect to all security incidents including violent incidents; and

4.3.10 Advise on the availability and use of `Reliance` lone worker alarms.

4.4 Senior Divisional and Corporate Directors/Managers (Including Directors of Operations and Associate Directors of Nursing)

Senior Divisional & Corporate Directors/Managers will be responsible for ensuring that this policy and associated practices, as well as local security procedures are developed, implemented and effectively managed within each of their areas of responsibility. They willensure that each department under their control undertake a security risk assessment, including the potential for violence and aggression, implement controls where risks are identified and monitor these for effectiveness.

4.5 Heads of Departments, Group Managers and Matrons and Nominated Managers

All Heads of Departments, Group Managers and Matrons and Nominated Managers are responsible for:

4.5.1 ensuring local security procedures are in place;

4.5.2 undertaking a comprehensive departmental risk assessment and creating an environment and climate where violence is less likely;

4.5.3 ensuring that the Policy, the associated Procedures, guidelines and are made known and available to all their staff;

4.5.4 supporting any member of staff who has been involved in any security incident including violence and aggression;

4.5.5 ensuring that an online Datix Incident Report Form is completed for every security incident including violence and/or aggression and the Trust Security Management Specialist together with the Health and Safety team is informed; and

4.5.6 Prevention, control measures and monitoring arrangements are implemented;

4.5.7 All staff are made aware of their obligations and receive appropriate education, training and development; and

4.5.8 Human Resource policies and procedures are strictly adhered to, including with regard to Criminal Record Checks (CRB).

4.6 Ward/Departmental Managers and Supervisors

Ward/Departmental Managers and Supervisors will be responsible for ensuring that Security policies, practices and procedures are complied with, which shall include:

4.6.1 Ensuring that local security procedures are adhered to and that all actual or potential breaches, acts of assault, violence or aggression are reported using the Trust incident reporting system and action plans devised as required;

4.6.2 ensuring that all security equipment is fully functional and reporting any faults to BBW helpdesk;

4.6.3 Ensuring that all Trust assets, property and information are not left unattended and are correctly and securely stored at all times;

4.6.4 Ensuring that the department is kept secure and locked when unattended;

4.6.5 Ensure that all patients are made aware of the risks associated with bringing in large amounts of money or valuables into the Trust and where this responsibility is delegated to staff that the patient property guidelines are followed.

4.7 All staff

All staff are responsible for assisting and supporting in the provision of a secure and safe environment and to this aim they must:

4.7.1 Comply with this policy and associated procedures, including local security arrangements;

4.7.2 Maintain a high degree of vigilance and not undertake any actions that may compromise their own personal safety, or that of colleagues, patients or visitors;

4.7.3 Routinely assess potential and actual security risks and report any concerns to their Line Manager;

4.7.4 Attend relevant security training and awareness sessions;

4.7.5 Report any malfunctioning of security equipment at the earliest possible opportunity, using the BBW helpdesk;

4.7.6 Not interfere with or misuse any security equipment, property or the environment as a whole;

4.7.7 Ensure that they wear an authorised Trust ID badge, in a visible position at all times;

4.7.8 Challenge any persons not known to them and not wearing an authorised Trust ID badge;

4.7.9 Ensure that Trust assets are not removed from their intended location without appropriate authorisation;

4.7.10 Ensure that their personal property is kept secure at all times;

4.7.11 Try to de-fuse violent/aggressive situations if they feel safe to do so and immediately summon assistance when aware of a potential or actual violent incident;

4.7.12 If involved in an incident either as a victim or when going to someone's assistance, use the minimum of force necessary to control the violent person(s) bearing in mind the legal/medical constraints and personal responsibility to act within the law; and

4.7.13 Complete an online Datix Incident Report Form immediately following such an event or as soon as possible thereafter.

4.8 Compliance with this policy and associated procedures is mandatory and failure by any member of staff to comply with such requirements will result in consideration of the use of disciplinary action.

4.9 Trust Health, Safety and Environment Committee

The Trust Health Safety and Environment Committee regularly assesses and reviews security activity, trends, risks and issues across the Organisation as a whole. The Committee recommends the development of action plans by the TSMS with a view to mitigating or eradicating such risks. The Chair of the Committee reports to the Trust Board.

4.10 Divisional and Corporate Consultative Committees

4.10.1 The Divisional & Corporate Consultative Committees act as a local forum for reviewing local security activity, trends, risks and issues.

4.10.2 The Chair of each Committee report to the Trust Health, Safety and Environment Committee through the Directors of Operations and the Trust's Security Management Specialist.

4.11 Facilities and Estates Management

Facilities & Estates Management is provided by Balfour Beatty Workplace (BBW). The Manager of BBW will ensure that:

4.11.1 All site security risk assessments are completed in accordance with the their contract with the Trust;

4.11.2 a secure, robust and fully auditable system is established for the management and distribution of keys used by security, including master sets;

4.11.3 BBW undertake lock and unlock procedures for designated Trust premises. This includes promptly attending and assessing premises where a breach of security has been reported;

4.11.4 A method statement outlining BBW service provision is produced annually

4.11.5 Ensure that all security equipment is fully functional

4.11.6 Respond and assist with potential and actual security incidents, including acts of assault, violence and aggression;

4.11.7 provide continuous surveillance of security monitoring systems and undertake regular patrols (as defined within BBW method statements) of Trust premises and grounds with a view to identifying potential risks and resolving any actual breaches of security; and

4.11.8 Investigate any breaches of security and report the finding to the Trust Security Management Specialist.(TSMS)

5 Implementation

5.1 This policy will be implemented by all levels of management in the Trust and made available to all staff via the Trust intranet.

5.2 In addition, information on security issues will be provided to wards and departments by the TSMS to encourage a pro-security culture among staff.

5.3 The TSMS will provide advice, assistance and support on various security related matters

5.4 Security awareness will be included as part of Trust induction with additional training sessions made available to staff as required.

6 Monitoring

The standards to be achieved and the monitoring arrangements to ensure compliance are detailed at appendix A.

7 References

7.1 Secretary of State’s Directions for Violence & Aggression and Security Management (2003 / 2004).

7.2 Health and Safety at work Act 1974

7.3 The Management of Health and Safety at Work Regulations 1999

7.4 The Corporate Manslaughter and Corporate Homicide Act 2007

7.5 The Civil Contingencies Act 2004

7.6 NHS Litigation Authority

7.7 The Management of Health and Safety at Work Regulations Working Alone in Safety (HSE) Publication

7.8 Data Protection Act 1998 (CCTV)

8 Associated Policy and Procedural Documentation

The Security Management (including violence and aggression) Policy should be used in conjunction with the following policy and procedural documents:

8.1 Withholding Treatment Procedure for Aggressive Patients

8.2 Bomb Warning Procedure

8.3 Lone Worker Guidelines

8.4 Health and Safety Policy

8.5 Disciplinary Policy

8.6 Counter Fraud Policy

8.7 Information Security Policy

8.8 Risk Management Policy

8.9 CCTV Policy

8.10 Security Contract

8.11 Traffic Management Policy

8.12 Recruitment Procedures

8.13 Major Incident Procedures

8.14 Operational Security Procedures for each area of the Trust

8.15 Lock down Procedures.

8.16 Mass Casualties Plan

8.17 Trust Waste Policy

Appendix A: Monitoring Matrix

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
Monitoring of the Security service provided by Balfour Beatty Workplace.	Trust Security Management Specialist. (TSMS)	Trust Security Management Director	BBW send weekly and monthly reports containing security responses to incidents to the TSMS. The TSMS then ensures compliance with the security contract. Any breaches are reported to the TSMD	Reports sent weekly and monthly.
Compliance with the policy	Trust Security Management Specialist. (TSMS)	Trust Security Management Director	Security Report submitted to Trust Health and Safety Committee. This includes actual security incident figures, trends, and actions taken and any other emerging issues including violence and aggression.	Quarterly.
Any trends in violence and aggression compared to other Trusts.	Trust Security Management Specialist. (TSMS)	Trust Security Management Director	Violence and Aggression statistics submitted to NHS Protect by TSMS	Annually
The Trust will assess the risks of violence & aggression and security and implement appropriate control measures to reduce risks to the lowest possible level.	Trust Security Management Specialist.	Health and Safety Committee	Completed security risk assessments including violence and aggression	Quarterly
Staff involved in incidents of violence will be provided with both psychological and practical support as required.	Occupational Health and Safety Department	Head of Health and Safety Department.	Records held by Health and Safety.	Ad hoc
The Trust ensures the safety of Lone Workers and has in place a Lock Down Procedure	Trust Security Management Specialist. (TSMS)	Trust Security Management Director	The Trust has in place Lone Worker Guidelines and a Lock Down Procedure which is reviewed every 3 years or sooner if necessary	Every 3 years or sooner if required

CONTROLLED DOCUMENT

APPENDIX C

University Hospitals Birmingham NHS
NHS Foundation Trust

Policy for the Development and Management of Controlled Documents.

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE:	To set out the principles and framework for the development, approval and monitoring of policies and procedural documents throughout the Trust
Controlled Document Number:	1
Version Number:	2
Controlled Document Sponsor:	Director of Corporate Affairs
Controlled Document Lead:	Senior Manager Corporate Affairs
Approved By:	Board of Directors
On:	
Review Date:	
Distribution: • Essential Reading for: • Information for:	All Directors, Senior Managers and Department Heads All Staff

Contents

1 Policy Statement

1.1 The purpose of this policy and its associated documents is to ensure that the Trust has in place policies and procedural documents ("Controlled Documents") which are implemented appropriately.

1.2 The objectives of this policy are to ensure that all Controlled Documents are

1.2.1 developed, approved, implemented and monitored through a clear process;

1.2.2 developed in consultation with those who fall within their scope, or who may be affected by them;

1.2.3 assessed for any impact they have on the Trust and the delivery of services,

1.2.4 written clearly and succinctly, using plain language appropriate to the intended audience;

1.2.5 implemented effectively by ensuring adequate awareness and providing appropriate training and support;

1.2.6 easily accessible to all staff and published in accordance with the Trust's Freedom of Information Act Publication Scheme; and

1.2.7 reviewed and revised regularly, responding to changes in legislation, standards and good practice.

2 Scope

This policy applies to all Controlled Document Leads and Sponsors and all Controlled Documents within the Trust. All Controlled Documents in existence prior to the issue of this policy will remain in effect until such time as they are reviewed, replaced or cancelled.

3 Framework

3.1 This section describes the broad framework for the development and management of Controlled Documents. Detailed instructions are provided in the associated Procedure for the Development and Management of Controlled Documents. The procedure may be amended from time to time by authority of the Director of Corporate Affairs, provided that such amendments are compliant with this policy.

3.2 Definitions

Controlled Documents are divided into two categories:

3.2.1 Policy

A statement of intent and principles explicitly stating individuals' responsibilities and accountabilities, which provides the basis for consistent decision making, actions and resource allocation. A policy provides a documented framework enabling individuals or specific groups of staff to carry out interventions, plans or care. Policies include documents such as Standing Orders and Standard Financial Instructions. Compliance with policies is not open to interpretation, or professional judgement and is non negotiable.

3.2.2 Procedural Document

A ‘procedural document’ is a description of operational tasks to be undertaken to implement, or in support of, a policy. Procedural documents can have a number of titles including, for example, Care Pathways, Codes Of Conduct, Codes Of Practice, Guidelines, Procedures, Protocols, Schemes and Standards.

Procedural documents may apply across the Trust to all sites and services or be limited to one or more specific areas of the Trust.

Appendix B defines the applications for the type of procedural documents.

3.3 The Trust’s framework for ensuring that controlled documents are developed and managed appropriately consists of the following stages:

3.3.1 Development of Controlled Documents

Controlled Document Leads will:

a) comply with the standards set out in the Procedure for the Development and Management of Controlled Documents and adhere to the templates within that procedure, save that, for controlled documents used in certain areas subject to particular external regulatory or equivalent requirements (such as Labs see associated procedure) the format of this documentation may deviate from these templates subject to approval by the Director of Corporate Affairs;

b) only introduce a controlled document if required and ensure it does not duplicate information in existing controlled documents;

c) identify and consult with all relevant stakeholders The length of the consultation will vary depending on the nature of the document but should not normally be less than 2 weeks and no more than 4 weeks; and

d) assess the impact of the document in relation to resources required for implementation, equality and diversity, privacy and compatibility with other controlled documents, external standards and legislation and environmental impacts;

3.3.2 Approval of Documents

Controlled Document Leads will:

a) Arrange for any Policies to be submitted along with the associated report (see Controlled Document Procedure appendix E) to the Senior Manager Corporate Affairs so that it can be presented to the Policy Review Group (PRG). Following review by the PRG, policies considered satisfactory must be brought before the Chief Executive /Board of Directors for approval as determined by the Director of Corporate Affairs.

b) Arrange for any procedural documents to be submitted along with the associated report (see Controlled Document Procedure appendix E) to the Controlled Document Sponsor who should then review the document and approve it in writing.

3.3.3 All Controlled Documents must be submitted to the Senior Manager Corporate Affairs once approved before they are placed on the intranet. Webmaster will not publish any controlled documents on the intranet without permission from the Senior Manager Corporate Affairs. Notification and Implementation of Documents

a) The Controlled Document Lead is responsible for ensuring that the existence of the approved Controlled Document is communicated to whom it specifically applies to, in accordance with the Implementation section of the associated report (Controlled Document procedure appendix E).

b) The Controlled Documents Leads will be required to have fully implemented their document within 3 months of it being approved and this will be reported to the Senior Manager Corporate Affairs who will notify the Policy Review Group of any non-compliance.

3.3.4 Review of Controlled Documents

a) Controlled Documents will be reviewed and revised in response to changed circumstances and in any event at intervals of not more than three years. Shorter review periods may be stipulated by the approving Body.

b) Where, following review, no or only minor changes to a Controlled Document are required, then fresh consultation or impact assessments are not required and the Controlled Document may be submitted to the relevant body for approval.

c) Where substantial changes are required, the Controlled Document Lead must make sure that stakeholder involvement, consultation and impact assessments are undertaken.

3.3.5 Document Control

a) The Trust will have one register (the "Controlled Documents Register") that will catalogue all Controlled Documents by document type (see appendix B), issue date and document control number and will be maintained by the Senior Manager Corporate Affairs.

b) The version of a Controlled Document held on the intranet shall be the definitive version to which reference should be made in the event of any confusion as to the status of a particular version or copy of a Controlled Document.

c) Controlled Documents will remain in force until such time that they are replaced or removed.

d) When Controlled Documents are amended, superseded or cancelled, they will be removed from the intranet and archived in accordance with the Controlled Document Procedure.

e) Staff should always refer to controlled documents electronically to ensure they are the most up-to-date version. If a paper copy is referred to, staff should always check the review date to ensure it is the most current document. Any paper copies held locally should be disposed of and replaced with the latest version of the document.

3.3.6 Cancellation of Documents

a) When a Controlled Document Sponsor or Lead identifies that a Controlled Document is no longer required it must be cancelled in the following way:

(i) Policies will be cancelled by the Chief Executive/Board of Directors and evidenced via the relevant minutes.

(ii) Procedural documents will be cancelled by the Document Sponsor and evidenced via an email from the Document Sponsor to the Senior Manager Corporate Affairs

When a controlled document is cancelled the email or minutes evidencing this must be sent to the Senior Manager Corporate Affairs before they will be removed from the intranet. Webmaster will not remove any controlled documents on the intranet without the Senior Manager Corporate Affairs permission.

3.4 Variation

The Trust will need to develop some policies and procedural documents in conjunction with partner organisations. In these circumstances the principles set out within this policy must still be adhered to. However, there is some flexibility for variation from the associated procedure. This must be approved by the Director of Corporate Affairs.

4 Duties

4.1 Board of Directors

The Board of Directors will:

4.1.1 Approve any new and revised policies reserved to the Board of Directors for approval (Reserved Policies) and may debate in full any policy presented to it.;

4.1.2 Approving the cancellation of reserved policies that are no longer required; and

4.2 Chief Executive

The Chief Executive will:

4.2.1 Approve all new and revised policies, other than Reserved Policies, and reserve the power to debate in full any policy presented for approval; and

4.2.2 Cancel policies, other than reserved policies, that are no linger required;

4.3 Director Of Corporate Affairs

The Director of Corporate Affairs will provide assurance to the Board of Directors on compliance with this policy and will present an annual report on the development and management of Controlled Documents to the Audit Committee for consideration.

4.4 Policy Review Group (PRG)

The PRG is responsible for

4.4.1 reviewing new and revised policies and, where considered fit, recommend such policies to the Chief Executive or, in the case of Reserved Policies, the Board of Directors, for approval; and

4.4.2 reviewing the overdue controlled document report and identifying any action that needs to be taken.

4.5 Audit Committee

The Audit Committee will receive an annual report on the development and management of controlled documents which will include any non-compliance with this policy and its associated procedures.

4.6 Directors and Divisional Directors

Directors and Divisional Directors are responsible for

4.6.1 Approving any procedural documents for their areas of responsibility;

4.6.2 Ensuring that all procedural documents approved by them are compliant with Trust policies; and

4.6.3 Ensuring that all controlled documents within their Division or areas of responsibility are reviewed at least every three years and/or when changes in legislation, guidance, etc occur.

4.7 Senior Manager Corporate Affairs

The Senior Manager Corporate Affairs is responsible for:

4.7.1 Maintaining the Controlled Document Register

4.7.2 Maintaining the Trusts electronic library of Controlled Documents and for publishing new and revised documents.

4.7.3 Advising the Controlled Document Leads on implementing the process for the approval of Controlled Documents

4.7.4 Preparing reports for PRG and the Audit Committee on compliance with the Policy.

4.8 Controlled Document Leads

4.8.1 Each Controlled Document will have an identified lead manager (the “Controlled Document Lead”) who is responsible for the development and management of the document. This includes:

a) obtaining the approval of the appropriate Controlled Document Sponsor for the drafting of a new Controlled Document;

b) assessing the justification for the development of the document;

c) identifying the people who need to be involved in the development of the document (Stakeholders, as defined at 3.13 below);

d) making sure that there is appropriate consultation with all key stakeholders including any relevant committees/ groups;

e) ensuring that appropriate impact assessments have been undertaken and that the results of the assessments are made available at the time of approval;

f) preparing a plan for the dissemination of the document;

g) arranging for the document to be presented for review/approval. The Controlled Document Lead or their representative will attend the review to answer any questions raised; and

h) advising staff on the implementation of the document.

4.8.2 The Controlled Document Lead will make sure that each Controlled Document is reviewed and revised at appropriate intervals. This includes assessing the need for policy change as a result of changes in legislation, guidance etc and for initiating and co-ordinating the process of review and revision and subsequent submission for

4.9 Controlled Document Sponsor

4.9.1 Development of any policy must be approved by the Board Director who heads the area of the Trust to which the policy most relates. This person will be the Controlled Document Sponsor for that policy.

4.9.2 Development of procedural documents must be approved by the relevant Controlled Document Sponsor who will be the Director/officer of the Trust specifically authorised to approve the development of the Procedural Document, as set out in the relevant Policy or elsewhere.

4.9.3 Where there is any uncertainty as to the identity of a Controlled Document Sponsor for a particular Controlled Document, the Director of Corporate Affairs shall determine the Controlled Document Sponsor.

4.10 All Managers and Supervisors

It is the responsibility of all managers and those with responsibility for supervising the work of others to make sure that their staff are aware of and understand the Controlled Documents which apply to them, their employment and work activities. Managers and supervisors must also make sure that staff are alerted to new and revised Controlled Documents and know how to access them.

4.11 All Staff

4.11.1 It is the responsibility of all staff to make sure that they are familiar and adhere to the Controlled Documents which apply to them, their employment and work activities.

4.11.2 Incidences of non-adherence to a Controlled Document will be investigated and therefore may be subject to disciplinary procedures.

4.11.3 All staff have a duty to report non-compliance with Trust Controlled Documents as soon as possible.

4.11.4 Staff should always refer to controlled documents electronically to ensure they are the most up-to-date version. If a paper copy is referred to staff should always check the review date to ensure it is the most current document. If the paper copy is out-of-date it should be disposed of and the current document should replace any paper copies and should not be circulated to staff.

4.12 Stakeholders

4.12.1 Stakeholders are all those individuals or groups who have a stake in or may be impacted by a given Controlled Document. Accordingly, stakeholders should influence the Trust's services, policies and procedures. Examples of stakeholders include , internal stakeholders such as staff, staff side, the human resource and finance departments and external stakeholders including Consort Healthcare, patient user groups and interested members of the public.

4.12.2 The interests of potential stakeholders should be considered by the Controlled Document Lead and appropriate consultative mechanisms should be agreed. Stakeholders have a duty to respond in a constructive manner and within the timescales of the consultation process.

5 Implementation of this policy

5.1 Implementation

5.1.1 This policy will be available on the Trust's Intranet Site. The policy will also be disseminated through the management structure within the Trust;

5.1.2 The Senior Manager Corporate Affairs will provide advice and support to Controlled Document Leads about the implementation of this policy.

5.1.3 Templates for different types of Controlled Document will be available on the Trust's intranet.

5.2 Monitoring

5.2.1 Appendix A provides full details on how the policy will be monitored by the Trust.

6 References

NHSLA, 2007. An Organisation-wide Policy for the Development and Management of Procedural Documents, (online) available from: http://www.nhsla.com (cited 6 August 2007).

7 Associated Controlled Documents

Procedure for the Development and Management of Controlled Documents.

Procedure for the Development and Management of Controlled Documents within Labs

Appendix A

Monitoring Matrix

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
All Controlled Documents adhere to the correct style and format including referencing and associated documents	Document Lead	Policy Review Group and Senior Manager Corporate Affairs/Document Sponsor	The PRG will ensure all policies adhere to the Template in the Controlled Document procedure before any documents are approved. For all other controlled documents the document sponsor should ensure it complies with the Controlled Document procedure and the Senior Manager Corporate Affairs will not publish any document that doesn't.	As required (eg when the document is approved)
That the consultation and ratification process is followed for all controlled Documents	Document Lead	Policy Review Group and Senior Manager Corporate Affairs/Document Sponsor. BD Minutes and CEAG Minutes	The PRG will not accept any policies that are not accompanied with appendix E of the Controlled Document Procedure. Any non adherence to the implementation plan will be reported to the PRG by exception. All policies will be reported to the BOD or CEAG and evidence of this will be in the minutes. For all other controlled documents the Senior Manager Corporate Affairs will not publish any document until a Appendix E of the Controlled Document Procedure has been submitted along with written proof from the document sponsor that they have approved the document.	As required (eg when the document is approved)

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
All Controlled Documents adhere to the correct style and format and the consultation and ratification process is followed for all controlled Documents	Senior Manager Corporate Affairs	Audit Committee	Minutes from the BoD and CEAG show that policies are approved appropriately and this information is detailed in the Controlled Document Annual Report. A review of the documents approved within the last year will also be undertaken to ensure they comply with the Controlled Document procedure and any non-adherence will be identified in the Controlled Document Annual report	Annually
Compliance that document leads are reviewing and getting their controlled documents approved before the review date	Senior Manager Corporate Affairs	Policy Review Group	A report to the Policy Review Group is submitted showing all those controlled documents that are overdue	Monthly
Control of documents including archiving arrangements	Senior Manager Corporate Affairs	Audit Committee	Minutes from the BoD and CEAG show that policies are approved appropriately and this information is detailed in the Controlled Document Annual Report	Annually

Appendix B

Definitions of Procedure Documents

Care Pathway	A procedural document which describes the anticipated care designed to help a patient with a specific symptom or set of symptoms move progressively through a clinical experience. Appropriate variation from the pathway may occur to meet the needs of an individual patient.
Code Of Conduct	A procedural document which states the regulations and rules relating to conduct which must be followed to implement a policy.
Code Of Practice	A procedural document which provides practical advice on strategy and/or practical means of achieving compliance with general duties or specific regulatory requirements.
Guideline	A procedural document which provides a set of recommendations of principles/best practice for the implementation of a policy that are evidence based/referenced, within which individuals can use their professional judgement. Guidelines are less rigid than procedures and allow appropriate flexibility.
Procedure	A procedural document which provides day-to-day working instructions consisting of a series of actions to be undertaken in a regular order, to implement a policy. Procedures are mandatory documents and must be followed. Procedures can be mapped using a flow chart.
Protocol	A procedural document which describes a specific procedure. Protocols are rigid statements allowing little or no flexibility or variation. Protocols are targeted at relevant staff groups enabling safe autonomous practice, including enhanced practice, often at local level. They have a specific use and are non-transferable. Deviation is not permissible and carries legal implications. Protocols can be mapped using a flow chart.
Scheme	A procedural document which describes orderly and systematic arrangements for consistent decision making, actions and resource allocation to implement a policy.
Standard	A pre-determined criterion, against which performance can be measured. Standards should be “SMART” - specific, measurable, achievable, realistic and, where appropriate, time bound. They provide a framework for continuing improvement in performance and set a baseline which must be met, e.g. uniform.