University Hospitals of Morecambe Bay NHS Foundation Trust

Document Type: **Policy**	**Unique Identifier:** CORP/POL/069
Document Title: **Information Security**	**Version Number:** 2.3
	Status: Ratified
Scope: Trust Wide	**Classification:** Organisational
Author / Title: Fiona Prestwood, Information Governance Manager	**Responsibility:** Innovation, Information and Informatics (I3) Service
Replaces: Version 2.2, Information Security, Corp/Pol/069	**Head of Department:** Andy Wicks, Chief Information Officer
Validated By: I3 Risk Management Forum	**Date:** 05/01/2016
Ratified By: Procedural Document and Information Leaflet Group	**Date:** 17/02/2016
Review dates may alter if any significant changes are made	**Review Date:** 01/05/2019 (Review date extended form 054/2019)

Which Principles of the NHS Constitution Apply? **Please list from principles 1-7 which apply** 3 Principles	**Which Staff Pledges of the NHS Constitution Apply?** **Please list from staff pledges 1-7 which apply** 3 Staff Pledges

Does this document meet the requirements of the Equality Act 2010 in relation to Race, Religion and Belief, Age, Disability, Gender, Sexual Orientation, Gender Identity, Pregnancy & Maternity, Marriage and Civil Partnership, Carers, Human Rights and Social Economic Deprivation discrimination? **Yes**

Document for Public Display: Yes

Reference Check Completed by……Joanne Shawcross……..Date……16.2.16…….

To be completed by Library and Knowledge Services Staff

CONTENTS

BEHAVIOURAL STANDARDS FRAMEWORK

To help create a great place to work and a great place to be cared for, it is essential that our Trust policies, procedures and processes support our values and behaviours. This document, when used effectively, can help promote a workplace culture that values the contribution of everyone, shows support for staff as well as patients, recognises and celebrates the diversity of our staff, shows respect for everyone and ensures all our actions contribute to safe care and a safe working environment - all of which are principles of our Behavioural Standards Framework.

Behavioural Standards Framework – Expectations 'at a glance'

1. SUMMARY

The Information Security Management: NHS Code of Practice[1] states 'Information, whether in paper or digital form, is the lifeblood of NHS organisations because of its critical importance to NHS patient care and other related business processes. High-quality information underpins the delivery of high-quality evidence based healthcare and many other key service deliverables. Information has greatest value when it is accurate, up to date and is accessible where and when it is needed.

Inaccurate, outdated or inaccessible information that is the result of one or more information security weaknesses can quickly disrupt or devalue mission critical processes. These factors should be fully considered when commissioning, designing or implementing new systems. An effective information security management regime ensures that information is properly protected and is consistently available.'

2. PURPOSE

The purpose and objective of this Information Security Policy is to set out a framework for the protection of the Trust's information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuity and minimise business damage and in order to deliver strategic and operational objectives.

The Information Security Policy is a high level document, and adopts:

- Standards: mandatory activities, actions, rules or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. The Standards are derived from the international security standard ISO 27001
- Procedures: which define the details of how the policy, standards and guidelines will be implemented in an operating environment
- Guidelines: General statements designed to achieve the policy's objectives by providing a framework within which to implement controls not covered by procedures

This policy constitutes an Information Security Policy, as required under section 5 of ISO 27001:2013[2]. The policy sets out the approach by which UHMB will meet its responsibilities for the security, confidentiality, integrity and availability of Trust Information assets. It also describes the accountability arrangements for the risk management of those assets.

Information takes many forms and includes:

- Hard copy data printed or written on paper
- Data stored electronically
- Communications sent by post / courier or using electronic means
- Stored tape or video
- Speech

From this point forward University Hospitals of Morecambe Bay NHS Foundation Trust will be known as UHMB or the Trust. The Innovation, Information and Informatics (I3) Service will be known as I^3 Service.

3. SCOPE

The policy applies to all full-time and part-time employees of the Trust, non-executive directors, contracted third parties (including agency staff and volunteers), students, trainees, individuals on secondment and other staff on placement with the Trust plus staff of partner organisations with approved access (such as Social Services).

4. POLICY

4.1 Duties

4.1.1 Risks To The Trust

Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.

Data and information is put at risk by poor education and training, the misuse and breach of security controls of information systems. Consequently, this, may be used to misrepresent the Trust and result in the ineffective use of Trust's resources

Information security incidents can give rise to reputational damage, financial loss and non-compliance with Standards and Legislation as well as possible judgements against the Trust.

4.1.2 Statement Of Management Intent

It is the policy of UHMB to ensure that:
Information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorised individuals
- Integrity: safeguarding the accuracy and completeness of information and processing methods
- Availability: that authorised users have access to relevant information when required
- Accountability: who is responsible

The following groups, forums and committees will review and make recommendations on Security Policy, Policy Standards, Directives, Procedures, Incident Management and Security Awareness education. These being; Information Governance Steering Group, I^3 Risk Management Forum and I^3 Steering Group.

Regulatory, legislative and contractual requirements will be incorporated into Information Security Policy, Standards and Procedures as well as the Trust's Operational Procedures and contractual arrangements.

The Trust will work towards compliance with the ISO27000 series, the International Standards for Information Security.

All breaches of information security, actual or suspected, must be reported using the Trust defined procedure and will be investigated.

Business continuity plans will be produced, maintained and tested.
Information security education and training will be available to all employees and third

party contractors as necessary.

Information stored by the Trust is appropriate to their business requirements

4.2 Roles, Responsibilities And Accountabilities

4.2.1 Information Systems Manager (ISM)
Is responsible for the maintenance and review of this Information Security Policy and any associated policies, standards and procedures support provided by the Information Governance Manager and Information Security Officer. The ISM reports to the Chief Information Officer and the SIRO.

4.2.2 Senior Information Risk Officer (SIRO) and Designated Information Asset Owners (IAOs)
Are responsible for ensuring that all departments, Trust employees, contractual third parties and agents of the Trust are made aware of and comply with the Information Security Policy, its associated standards, procedures and expected working practices. This will ensure that individual responsibilities are clearly understood.

In addition, it ensures that the Trust's requirements for the reporting and management of information incidents and risk identification apply to all assets. It also, provides the mechanisms to support the minimisation of the incidents and risk severity and reduces the level of escalation procedures should they be required. The SIRO reports to the board with board level responsibility. The IAO reports to the SIRO with senior management status within the Trust and Divisions.

4.2.3 Internal Audit Service
Will review the adequacy of the controls that are implemented to protect the Trust's information and recommend improvements where deficiencies are found. Provided by Mersey Internal Audit Agency.

Each employee, contractual third party and agent of the Trust accessing Trust information is required to adhere to the Information Security Policy, associated standards and procedures including Health & Safety requirements. They are responsible for the appropriate use and operation of the equipment and information they are using in their work and role.

Failure to comply with the Information Security Policy, Standards and Procedures will lead to disciplinary or remedial action.

4.3 Organisation Of Information Security

The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the Trust and in its dealings with third parties.

Specialist advice will be drawn upon where necessary so as to maintain the Information Security Policy, Standards and Procedures to address new and emerging threats and Standards.

4.4 Asset Management

All assets (data, information, software, computer and communications equipment, service utilities and people) are identified and accounted for and have an Information Asset Owner assigned. The IAO will be responsible for the maintenance and protection of the asset(s) concerned. Ensuring that all risks associated with the asset are regularly recorded, assessed and managed according to Trust policy. Where the asset is data the individual is responsible for ensuring that the data it is accurate, complete and up-to-date.

All personal identifiable data is covered by the terms of the Data Protection Act[3] and must be protected and handled in accordance with the provisions of this legislation. All personal identifiable data is therefore classified as CONFIDENTIAL for risk management purposes, in order that associated protective controls are applied. The controls must be suitable for sharing or restricting access to the information and to the business impacts associated with such needs.

Patient and staff data that is held within the Trust's electronic information systems is subject to the protective controls specified within the Acceptable Use Policy. Data classed as CONFIDENTIAL within one system should maintain at least the same sensitivity level across all systems. The output from systems handling any personal identifiable data should be labelled as CONFIDENTIAL; output includes printed reports, magnetic media, electronic messages and file transfers. Access rights given to users should be consistent across all areas. Particular attention should be paid to the level of confidentiality of any data when downloaded to a PC, laptop or other mobile device.

For security purposes, each logical or physical set of data should be assigned an "owner". This Information Asset Owner should be responsible for identifying all the data within the area of responsibility, specifying how the data can be used, agreeing who can access the data, and what type of access each user is allowed, determining the classification or sensitivity level of the data, periodically reviewing that classification, approving appropriate security protection for the data, ensuring compliance with security controls and ensuring compliance, where necessary, with the Data Protection Act[3] and any other relevant legislation covering personal or medical data.

Supporting Documentation:

- Information Governance Policy and Framework
- Confidentiality

4.5 Human Resource Security

Security requirements for all staff, including contracted staff, will be addressed at the recruitment stage including Disclosing and Barring Service (DBS) checks and all contracts of employment will contain a confidentiality clause. Information security expectations of staff will be included within appropriate job descriptions and contracts will state the individual's and Trust's responsibilities for security.

Requirements for confidentiality will be regularly reviewed and should be considered if relevant changes occur; e.g. staff member changes roles or is given additional responsibilities. This control applies to both information assets (the confidentiality requirements of the information itself) and individuals (confidentiality requirements due to

job roles / responsibilities).

Third Parities agreements are required before any work is carried out or access to information or information systems, is granted. Agreements should include the agreed security arrangements, service definitions, aspects of service management and it should be ensured that they are implemented, operated and maintained by the third party. Agreements should be based upon full risk assessments carried out against the third parties. The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. Services, reports and records provided by third parties should be regularly monitored and reviewed with audits being carried out regularly. Emphasis should be placed on compliance with required information security controls and the management of information security incidents and problems.

In the case of outsourcing arrangements, necessary transitions (of information, information processing facilities and anything else that needs to be transported) are planned with emphasis on information security and the implementation of such plans needs to be thoroughly maintained.

4.6 Physical And Environmental Security

Physical security and environmental conditions must be proportionate with the risks to the area concerned. In particular critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls. In order to minimise loss of or damage to information assets, equipment will be physically protected from threats and environmental hazards and assessed regularly to ensure threats and vulnerabilities are mitigated.

Supporting documentation:

- Local Security Policy I^3 Service Furness General Hospital (FGH)
- Local Security Policy I^3 Service Royal Lancaster Infirmary (RLI)
- Local Security Policy I^3 Service Westmorland General Hospital (WGH)

4.7 Communication And Operations Management

Responsibilities and procedures for the management, operation and on-going security and availability of all data and information processing facilities will be established and documented by the relevant IAOs. Management of computer and networks will be controlled through standard documented procedures that have been authorised by I^3 Service.

Any changes to operating systems, the production environment and infrastructure are subject to formal change control procedures as defined by I^3 Service, and in accordance with Information Governance Toolkit guidelines. Alterations to minimum PC specifications will be assessed in a controlled environment and implemented only after testing. It is the responsibility of the System Support team to monitor for vulnerabilities and vendor releases of patches and fixes.

I^3 Service will ensure that all networked PCs including mobile devices (where appropriate) have software countermeasures and management procedures to protect the Trust against the threat of malicious software. For example the most up-to-date Anti-Virus software and patches installed on appropriate devices such as PCs and Laptops

Removable media of all types must be approved and procured via I[3] Service and must have a justifiable business need to be fully operational otherwise McAfee Endpoint Encryption will restrict functionality. Such media must also be fully virus checked before being used on the Trust's equipment.

I[3] Service will ensure that all information products are properly licensed and approved. It is a criminal offence and contrary to Trust Policy, to install software that has no legitimate licence or to take copies of licensed software for non-licensed use. Users must not install software on the Trust's property without permission. Users breaching this requirement may be subject to disciplinary action. Modifications to software packages are discouraged, limited to necessary changes, and all modifications are to be strictly controlled. Modifications are to be approved by I[3] Service Change Approval Board.

An audit trail where available of system access and data use by staff is maintained by the I[3] Service. The Trust is committed to safeguarding the privacy of patient information and in order to do this, has implemented measures to comply with our legal obligations. The Trust reserves the right to monitor staff system interactions, e-mail communications, internet activity and file content for investigative, disciplinary or technical purposes. Authority to access e-mails and/or files must be granted by the individual or via the authorised Working business partner. Any illegal activity will be reported to the Police via the process set out in the relevant Trust-specific policy, without necessarily consulting the individual. Prevailing HR disciplinary measures will be invoked but only with due regard for the accuracy and integrity of the evidence.

The IAO responsible for data quality within an individual system has responsibility for ensuring that the data held within the system is accurate, complete and up-to-date, and for overseeing processes to correct, update and validate data held in Trust systems. All staff that input into an information system must ensure that the data input is correct, is understandable (e.g. no unnecessary/inconsistent abbreviations) and is reasonable (e.g. ages are not recorded as 309 or -2).

All staff involved in the data output process need to carry out plausibility checks to test whether output data is reasonable and identify possible output errors.

Applications, generated data and logs are to be risk assessed and protected accordingly by the relevant IAO. Access controls and encryption should be applied as required to ensure appropriate levels of data security.

Information should only be shared when there is an identified need to do so. UHMB recognises that, in order to provide the best possible continuity of healthcare for our patients, healthcare providers need access to appropriate personal confidential data when and where it is required. Information sharing must have a lawful, defined and justifiable purpose that respects people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. The Trust will ensure that Information Sharing Agreements and Protocols are in place and recorded on the Information Sharing Gateway so that personal data on individuals will be properly protected and processed in compliance with the Data Protection Act 2018[3]. Data should be collected once, shared appropriately and used many times, where appropriate this should be fully automated in order to assure security.

Supporting documentation:

- Acceptable Use Policy for Information Communication and Technology (ICT) Systems and Equipment Access Control to Information Systems
- I^3 Service Backup Arrangements
- Network Security Management System
- Procedure I^3 Incident Management
- I^3 Project Management Handbook
- Change Management Policy
- Reporting and Investigation of Incidents including Serious Incidents
- Information Sharing Policy
- Privacy Monitoring Policy

4.8 Access Control

Access to information will be restricted to authorised users who have a justified and approved business need to access the information.

Access to computer facilities will be restricted to authorised personnel who have a business need to use the facilities.

Access to data, system utilities and programme source libraries will be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will be dependent on the availability of a licence from a supplier.

Supporting Documentation:

- Local Security Policy I^3 Service Furness General Hospital (FGH)
- Local Security Policy I^3 Service Royal Lancaster Infirmary (RLI)
- Local Security Policy I^3 Service Westmorland General Hospital (WGH)
- Access Control to Information Systems

4.9 Information Systems Acquisition, Development and Maintenance

Only software and hardware approved and commissioned by the I^3 Service can be connected to the Trusts network. The development of software must be monitored to ensure compliance with necessary security requirements. This includes PCs, laptops, PDAs, Smartphones and any form of removable data storage device (such as memory sticks, floppy disks and removable hard disks). I^3 Service will maintain a catalogue of products that are approved 'White List'. Additional items that are not part of the catalogue will need to be risk and operationally assessed before approval for connection is granted.

Procurement of new or enhancement to existing information systems must conform to all relevant information security policies and will require Project Board / Change Approval Board approval before the system commences operation. The Trust will ensure that all new information systems, applications and networks are risk assessed and where required an Information Governance Project Assurance assessment completed (includes Privacy Impact Assessment, Patient Safety Assessment and System Level Security Risk Assessment) as part of the system implementation. System details will recorded in the Information Systems Portal.

When testing new systems, confidential and protected information and databases should not be used. When changing current systems, a review of application control and integrity

procedures must be undertaken to ensure they have not been compromised by system change and that confidential and protected information is adequately protected and controlled during the change.

Equipment shall be regularly monitored and maintained to ensure its' continued availability and integrity. Daily reviews of equipment are to be carried out during backup and any potential problems are to be recorded and rectified.

Systems are to automatically generate capacity management logs and distribute these (via email) to relevant personnel. From these logs, resources are to be monitored, tuned and, if necessary, future capacity requirement projections are to be created (the frequency of reports, the time of day/week of reports, suspected user usage of systems etc. before unnecessary procurements are requested).

Supporting Documentations:

- I^3 Project Management Handbook
- Equipment Decommissioning and Disposal Standard Operating Procedure
- Change Management Policy
- Information Governance Policy and Framework

4.10 Information Security Incident Management

All information security events and suspected weakness must be reported according to Trust Policy. If it is felt that the incident is sensitive in nature report directly to the Information Systems Manager, Information Governance Manager, Information Security Officer or Information Governance Officer. All security events must be recorded on the Trust's Safeguard system.

Any breach of this policy or supporting policies will be investigated and may result in the matter being treated as a disciplinary offence under the Trusts disciplinary procedure.
Supporting Documentations:

- Procedure I^3 Incident Management
- Reporting and Investigation of Incidents including Serious Incidents

4.11 Information Risk Management

Information Assets must be documented in an asset register (information systems should be added to the Information Systems Portal) without this list it would be impossible to implement the required controls across the Trust.

Information Asset Owners (IAOs) are required to be identified for all information assets to understand and address risks to the assets that they own. IAOs will provide assurance to the SIRO on the security and use of these assets. Responsibility for the assignment of appropriate controls must be assigned. Responsibility for implementing and managing controls may be delegated, although accountability must remain with the nominated IAO for the asset.

The security of information systems and technical platforms will be regularly risk assessed. Risk assessments will be carried out in accordance with appropriate security policies. Information security risks must be identified at the earliest stage in the development of business requirements for any new information systems or enhancements to existing

information systems. Controls to mitigate the risks must be identified and implemented where appropriate.

All risks and their treatment plans will be documented and recorded via Safeguard Risk Management System where appropriate as defined by the Trust's Risk Management Strategy.

Supporting Documentation:
- Risk Management Strategy
- Information Risk Policy

4.12 Business Continuity Management and Disaster Recovery Plans

There is an existing process to develop and maintain appropriate plans for the speedy restoration of critical business processes and services in the event of serious business interruptions.

Business continuity and disaster recovery planning will include measures to limit the consequences of any threats that are realised and to provide a resumption of essential operations as soon as required.

Systems Managers are required, in conjunction with the Information Systems Manager, to have business continuity plans in place and conduct an annual review of these plans.

Supporting Documentation:
- UHMB Business Continuity Policy
- Individual Ward / Dept. Business Continuity Plans
- I^3 Disaster Recovery Plan
- High Severity Incident Toolkit / Disaster Recovery Toolkit

4.13 Compliance

The design, operation, use and management of information systems must take into consideration all statutory, regulatory and contractual security requirements.

The Informatics Systems Manager shall keep the Information Governance Steering Group and I^3 Steering Group and other user organisations informed of the information security status of the organisation.

The Information Systems Portal and supporting documentation will be subject to regular reviews. Triggers for update outside of normal review will include but not limited to updates or introduction of new legislation, new information governance requirements and new working practices.

5. ATTACHMENTS	
Number	**Title**
1	Equality & Diversity Impact Assessment Tool

6. OTHER RELEVANT / ASSOCIATED DOCUMENTS	
Unique Identifier	**Title and web links from the document library**
LSP/Pol/069	I^3 - Local Security Policy (FGH) http://uhmb/cs/tpdl/Documents/LSP-POL-069.docx
LSP/Pol/068	I^3 - Local Security Policy (RLI) http://uhmb/cs/tpdl/Documents/LSP-POL-068.docx
LSP/Pol/067	I^3 - Local Security Policy (WGH) http://uhmb/cs/tpdl/Documents/LSP-POL-067.docx
Corp/Pol/116	Acceptable Use Policy for Information Communication and Technology (ICT) Systems and Equipment http://uhmb/cs/tpdl/Documents/CORP-POL-116.docx
I3/SOP/003	I^3 Service Backup Arrangements http://uhmb/cs/tpdl/Documents/I3-SOP-003.docx
I3/SOP/004	Network Security Management System http://uhmb/cs/tpdl/Documents/I3-SOP-004.docx
I3/Proc/002	Forensic Legal Incident Management Procedure http://uhmb/cs/tpdl/Documents/I3-PROC-002.docx
I3/Pol/001	Change Management Policy http://uhmb/cs/tpdl/Documents/I3-POL-001.docx
Corp/Proc/022	Reporting and Investigation of Incidents including Serious Incidents http://uhmb/cs/tpdl/Documents/CORP-PROC-022.docx
Corp/Pol/061	Information Sharing Policy http://uhmb/cs/tpdl/Documents/CORP-POL-061.docx
I3/SOP/001	Equipment Decommissioning and Disposal http://uhmb/cs/tpdl/Documents/I3-SOP-001.docx
Corp/Pol/014	Information Governance Framework and Policy http://uhmb/cs/tpdl/Documents/CORP-POL-014.docx
Corp/Pol/015	Data Protection and Confidentiality http://uhmb/cs/tpdl/Documents/CORP-POL-015.docx
Corp/Pol/056	Privacy Monitoring Policy http://uhmb/cs/tpdl/Documents/CORP-POL-056.docx

7. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS

References in full

Number	References
1	DoH (2007) Information Security Management: NHS Code of Practice. [Online] Available at: http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf (accessed 16.2.15)
2	ISO (2013) ISO/ICE 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=54534 (accessed 16.2.16)
3	Great Britain (2018). Data Protection Act 2018. Available from: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 10/07/2018)

8. DEFINITIONS / GLOSSARY OF TERMS	
Abbreviation or Term	**Definition**
UHMB	University Hospitals Of Morecambe Bay NHS Foundation Trust
HSCIC	Health And Social Care Information Centre
IAO	Information Asset Owner
DPA	Date Protection Act 2018
ADR	Appraisal and Development Review
PDA	Patient Demographic Service
IG	Information Governance

9. CONSULTATION WITH STAFF AND PATIENTS Enter the names and job titles of staff and stakeholders that have contributed to the document	
Name	**Job Title**
Fiona Prestwood	Information Governance Manager
Gail Martin	Information Security Officer
Helen Speed	Information Systems Manager
I^3 Risk Management Forum	Senior Managers from the I^3 Service

10. DISTRIBUTION PLAN	
Dissemination lead:	Helen Speed
Previous document already being used?	Yes
If yes, in what format and where?	Trust Procedural Document Library
Proposed action to retrieve out-of-date copies of the document:	Replaced after ratification at Procedural Document and Information Leaflet Group
To be disseminated to:	
Document Library	
Proposed actions to communicate the document contents to staff:	Include in the UHMB Weekly News – New documents uploaded to the Document Library

11. TRAINING Is training required to be given due to the introduction of this policy? No		
Action by	**Action required**	**Implementation Date**

12. AMENDMENT HISTORY				
Version No.	**Date of Issue**	**Page/Selection Changed**	**Description of Change**	**Review Date**
1.0	01 February 2012	None	Draft to Final	February 2014
1.11	January 2014	All sections	Review and update as required to supporting document references	January 2016
2	December 2015	All Sections	Document reviewed references to Health Informatics changed to I^3 Service and document references updated where required.	February 2019
2.1	06/10/2017	Page 3	BSF page added	01/02/2019
2.2	10/07/2018	Throughout	Reference to Data Protection Act amended to 2018	01/02/2019
2.3	19/03/2019	Front Cover	Review date extended form 054/2019	01/05/2019

Appendix 1: EQUALITY & DIVERSITY IMPACT ASSESSMENT TOOL

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Age	No	
	• Disability	No	
	• Race	No	
	• Sex	No	
	• Religious belief – including no belief	No	
	• Sexual Orientation	No	
	• Gender reassignment	No	
	• Marriage and civil partnership	No	
	• Pregnancy and maternity	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination are there any exceptions - valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
4a	**If so can the impact be avoided?**		
4b	**What alternative are there to achieving the policy/guidance without the impact?**		
4c	**Can we reduce the impact by taking different action?**		

For advice in respect of answering the above questions, and / or if you have identified a potential discriminatory impact of this procedural document, please contact the relevant person (see below), together with any suggestions as to the action required to avoid/reduce this impact.

For Service related procedural documents: Lynne Wyre, Deputy Chief Nurse & Lead for Service Inclusion and Diversity

For Workforce related procedural documents: Karmini McCann, Workforce Business Partner & Lead for Workforce Inclusion and Diversity.