INFORMATION GOVERNANCE POLICY
(INCORPORATING INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK)

AREA: Trust Wide

POLICY SPONSOR: Director of Finance

IMPLEMENTED: October 2009

REVISED: June 2011
March 2013
March 2015

DUE FOR NEXT REVIEW: 31 December 2019

DATE APPROVED: 9th March 2015

TO BE APPROVED BY:
Information Governance Group
Directors’ Meeting
Audit Committee (as endorsement delegation minuted by Trust Board)
CE signed off following Board Endorsement
Staff Side Approval

DISSEMINATED TO: Trustwide

Added to Intranet by: Mark Dobbs

Date Added / Removed: 14/04/15

Directorate: Corporate

Version: 4.0
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1  INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>2  INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK</td>
<td>4</td>
</tr>
<tr>
<td>3  INFORMATION HANDLING &amp; PROCESSING</td>
<td>9</td>
</tr>
<tr>
<td>4  PROPOSED INFORMATION SYSTEM PROCUREMENTS</td>
<td>10</td>
</tr>
<tr>
<td>5  TRUST DEFINITION OF PERSONALLY IDENTIFIABLE DATA (PID)</td>
<td>11</td>
</tr>
<tr>
<td>6  FREEDOM OF INFORMATION ACT</td>
<td>11</td>
</tr>
<tr>
<td>7  USE OF INFORMATION WITHIN THE TRUST</td>
<td>12</td>
</tr>
<tr>
<td>8  USE OF INFORMATION BETWEEN THE TRUST &amp; ITS PARTNERS</td>
<td>13</td>
</tr>
<tr>
<td>9  DISPOSAL OF CONFIDENTIAL WASTE &amp; THE USE OF SHREDDERS</td>
<td>13</td>
</tr>
<tr>
<td>10 INFORMATION GOVERNANCE BREACHES &amp; INCIDENT MANAGEMENT</td>
<td>13</td>
</tr>
<tr>
<td>11 ORGANISATIONAL PROCESS CHANGE, SERVICES, SYSTEMS &amp; INFORMATION</td>
<td>14</td>
</tr>
<tr>
<td>ASSET IMPLEMENTATION</td>
<td></td>
</tr>
<tr>
<td>12 PRIVACY IMPACT ASSESSMENT (PIA)</td>
<td>15</td>
</tr>
<tr>
<td>13 KEY SUPPORTING POLICIES &amp; GUIDELINES</td>
<td>16</td>
</tr>
<tr>
<td>14 POLICY DISTRIBUTION</td>
<td>17</td>
</tr>
<tr>
<td>APPENDIX A  TERMS OF REFERENCE OF IGG</td>
<td>18</td>
</tr>
<tr>
<td>APPENDIX B  MAJOR CHANGE REQUEST FORM</td>
<td>21</td>
</tr>
<tr>
<td>APPENDIX C  MINOR CHANGE REQUEST FORM</td>
<td>22</td>
</tr>
<tr>
<td>APPENDIX D  PIA PROCESS MAPS</td>
<td>23</td>
</tr>
<tr>
<td>APPENDIX E  PIA TEMPLATES</td>
<td>26</td>
</tr>
<tr>
<td>APPENDIX F  EQUALITY IMPACT ASSESSMENT FORM</td>
<td>32</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1 This document has been produced to set out the Trust’s general use of information and the governance surrounding it, the evidence of which will be provided annually by the Trust in the Information Governance Toolkit (IGT).

1.2 Information is an asset which, like other important business assets, has value to an organisation. Whatever form the information takes, or whatever means by which it is shared or stared, it should always be appropriately protected. Information can exist in many forms – it can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films or spoken in conversation.

1.3 **Everyone** working for the Trust has a legal duty and responsibility to protect information and keep it safe and secure, including all personally identifiable data (PID) held electronically or in paper format. It is the duty of all staff to be aware of the issues surrounding confidentiality, and to seek advise, in the first instance from line managers, if uncertain how to deal with them appropriately.

1.4 The Trust, through its policies, systems and guidelines, recognises the need to ensure that everyone within the organisation understands the need for effective information governance to manage, control or eliminate information risks.

1.5 The trust recognises the importance of information governance and the necessity to provide guidance and support regarding it in the delivery of care to service users. Various operational aspects of information governance and information use as they relate to specific areas and activities are documented and linked in the relevant Trust policies. The principal key supporting policies and guidelines are listed in section 13 of this policy.

1.6 By ensuring relevant policies are in place for staff, the Trust is able to provide assurance to service users and their carers, partner organisations (both current and prospective) and its regulatory bodies that the Trust continues to comply with information governance requirements and information governance best practice guidelines (including the annual IGT framework and requirements).

1.7 The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality healthcare. As such, it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes, both for patients and for service and performance management.

1.8 Data quality is the responsibility of **all** staff handling data. The Trust shall seek to improve its data quality by exception reporting to line managers where incidences of known or suspected poor quality data is identified. Any staff who have cause for concern over the reliability or accuracy of the data they are handling or processing shall bring this to the attention of their line manager in the first instance.

1.9 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of and the security arrangements in place to safeguard both personal information about patients and staff and commercially sensitive information.

1.10 The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.
2. INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

2.1 This framework sets out the process, governance arrangements and policy framework for the delivery of safe and effective information governance within the Trust.

2.2 Information Governance has four fundamental aims:

- to support the provision of high quality care by promoting the effective and appropriate use of information;
- to encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- to develop an information management structure to provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards;
- to enable the organisation to understand its own performance and manage improvement in a systematic and effective way.

2.3 This framework sets out how the Trust will achieve these aims.

2.4 Information assets encompassed by this framework will be any identifiable and definable assets owned or contracted by the Trust which are deemed ‘valuable’ to it including (but not limited to):

- personal and other information relating to patients, the workforce and the organisation (in electronic and paper form);
- software;
- hardware; and
- system / process documentation.

2.5 This framework also covers all aspects of handling information, including (but not limited to):

- structured record systems – paper and electronic; and
- transmission of information – such as by fax, email, post, text and email.

2.6 Information Governance provides a framework for managing information about patients and employees, with a particular emphasis on personal and sensitive information.

2.7 Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

2.8 The manner in which the Trust will deliver against these requirements is documented belc

2.9 The Trust has established an approach to information governance that ensures the organisation – from Trust Board level down – has the ability to fully comply with its requirements in terms of data protection and confidentiality.

2.10 Critically, it is also essential to ensure that the Board and the senior management of the organisation can be assured of continued compliance, and in particular, changes in performance can be monitored and managed.
2.11 The arrangements in place to achieve this are set out below:

**Overarching approach to confidentiality and data protection assurance**

2.12 The Trust has established a comprehensive information security assurance framework which is formalised within information security policies and operating procedures under the leadership of the Senior Information Risk Owner (SIRO) and the Information Security Manager, and embedded in the directorate structure of Information Asset Owners.

2.13 The Trust has in place an Information Asset Register which is maintained by the Information Asset Owners and regularly updated, ensuring that risks to the information assets are assessed and reviewed and reported to the SIRO. System level security and access control is also managed by the Information Asset Owners, along with the mapping of PID flows to ensure that the information is kept secure.

2.14 The Trust has also established business continuity and disaster recovery plans for all critical information systems and networks.

2.15 All risks associated with any aspect of information governance are entered onto local risk registers and managed locally to reduce them to the lowest possible level. Significant risks are also entered onto the Trust’s corporate risk register.

2.16 Incident reporting procedures are in place and further detail of the process is provided at Section 10 of this policy.

2.17 The Trust has the following senior organisational roles relating to Information Governance.

**Chief Executive**

- The Chief Executive has ultimate responsibility for compliance with the Data Protection Act 1998 and with Information Security Guidelines, and ensures that there is a structure for managing compliance and performance across the organisation. The Chief Executive also ensures that the roles of SIRO and Caldicott...
Guardian are assigned and supported.

- Responsibility for implementation of information governance, data protection and information security has been delegated to the Director of Finance Management.

**Senior Information Risk Owner (SIRO)**

- The Director of Finance has been appointed to the SIRO role, and is the Trust Board member who has corporate responsibility for information governance and ensures ownership of the organisation’s information risk policy, including providing advice and assurance to the Trust Board.

- The SIRO also provides written advice to the Accountable Officer in relation to information risk on the annual Statement of Internal Control.

- The SIRO is responsible for providing leadership and guidance to the Trust's Information Asset Owners and ensuring that the Trust’s Information Assets Register is maintained. The SIRO is supported by the Caldicott Guardian and members of the information governance expert advice unit (see section 7 below).

**Caldicott Guardian**

- The Director of Nursing & Quality has been appointed to the Caldicott Guardian role, and is the Trust Board member with responsibility for nursing, clinical and research governance.

- The Caldicott Guardian ensures that the NHS and partner organisations protect the confidentiality of patient level information, and is responsible for advising the Trust on confidentiality and information sharing issues. This also includes completing confidentiality audits to monitor access to confidential personal information, and highlighting confidentiality requirements and issues at Trust Board level.

- The Caldicott Guardian and Deputy is supported by the SIRO and the Information Governance Manager. who all form part of the broader Caldicott Function.

2.18 The senior organisation roles in paragraph 2.17 above are supported by an Information Governance expert advice unit including the Information Governance Manager / Information Security Manager, the Information Governance Manager, the IT Security Manager, the Freedom of Information Lead, the Registration Authority Manager, Records Management Leads, Information Asset Owners and the Information Governance Group (IGG) directorate representatives. These staff members are appropriately trained and receive regular updated training on the legal requirements of their roles.

**Data Protection Officer**

- The Head of Information acts as Data Protection Officer and Deputy Caldicott Guardian for the Trust. The Data Protection Officer ensures that the annual registration with the Information Commissioners Office has been fulfilled.

**Data Quality Lead.**

- The Head of Information is the Trust Data Quality Lead and is responsible for ensuring systems and processes are in place to provide accurate and timely validation of information in relation to services provided by the Trust.

**IT Security Manager**

- The Head of IT is responsible for the security of IT systems within the Trust.
• A key part of the role involves assisting the IG Manager with the development of the Trust's Information Assets Register and associated documentation, such as system level security documentation and access control procedures. The IT Security Manager is the designated Information Asset Owner for the Trust's IT infrastructure.

• The IT Security Manager is responsible for ensuring that the Trust has a business continuity strategy and plans in place for all business critical information assets and systems identified in the Information Assets Register, and for obtaining approval of the plans from the SIRO.

• Responsibilities also include ensuring the business continuity plans are regularly tested and the outcomes documented through simulation exercises.

Information Governance Manager

• The Information Governance Manager is responsible for developing and reviewing the Information Governance Strategy, including producing an annual Information Governance Work Programme to deliver the strategy, to ensure organisational compliance with the information Governance Toolkit, and conformance with the Data Protection and Caldicott principles.

• The Information Governance Manager is also responsible for developing or contributing to the development and review of Trust policies, procedures and processes relating to information governance, and working with the IT Security Manager to ensure that suitable and relevant information security policies are developed, implemented and complied with.

• The Information Governance Manager’s responsibilities also include maintaining the Trust’s Information Assets Register, ensuring that it remains up to date and supporting the SIRO in ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist.

• The Information Governance Manager is also responsible for developing and implementing mechanisms for defining and maintaining information flow maps within the Trust, and between the Trust and other organisations, and identifying and assessing risks associated with these information flows.

• Other responsibilities of the Information Governance Manager include developing and delivering Information governance training, including advance training for senior staff with information governance roles, and providing advice and support on information governance issues to staff in all areas of the Trust.

Registration Authority Manager

• The Associate Director, Human Resources (Specialist Services) has been designated as the Registration Authority Manager for the Trust in accordance with the Trust's Registration Authority Policy. The Director of Human Resources is the designated Information Asset Owner for the Trust's Registration Authority.

Freedom of Information Lead

• Trust Board Secretary has been delegated responsibility for Freedom of Information and for ensuring that all Freedom of Information processes are in place to comply with the Act. Assistance is provided by other members of the team who also handle Freedom of Information requests.

• The Freedom of Information Lead is responsible for ensuring that all staff are aware of their personal responsibilities for compliance and adhere to organisational
policies and procedures. This includes ensuring that training and written procedures are widely disseminated and available to all staff.

- Further responsibilities include ensuring the general public has access to information about their rights under the Act, ensuring the Trust’s Publication Scheme is up to date and establishing appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times.

**Records Management Leads**

- Responsibility for corporate records management has been delegated to the Trust Board Secretary / and responsibility for clinical records management has been delegated to the SIRO.

- It is the responsibility of each department / directorate to document and implement procedures for the effective management of corporate records in their area.

- The Information Governance manager works with the clinicians, managers and the IT department to develop clinical information and record systems embracing the concepts of clinical and information governance, and raise awareness of the importance of records management throughout the Trust. The Information Governance Manager is responsible for providing regular reports to the IGG on the records management work programme taking place across the Trust.

- The Information Governance Manager acts as a point of expertise for issues relating to health records, records management, subject access requests, clinical coding and the patient administration system.

- The Information Governance Manager works with the Caldicott Guardian in planning and implementing systems and training to ensure the protection of PID in all aspects of health records, records management and supporting information related issues.

- The Information Governance Manager is also responsible for the subject access function Trust-wide, including the management and maintenance of the Trust subject access database.

**Information Asset Owners**

- Beneath these expert leadership and advisory roles is a network of Information Asset Owners (IAOs) comprising of nominated senior members of staff. They are responsible for ensuring that all information assets are appropriately owned, managed and risk assessed.

- The IAO’s work with all members of staff in their directorates (and across directorates as appropriate) to ensure there is clear ownership and regular review of information assets and mapping of data flows to the information assets. They support the SIRO in managing the risk associated with information assets.

2.19 The Trust’s key governance bodies are:

**Information Governance Group**

- The Trust has established an Information Governance Group (IGG) comprising of representatives from across the Trust to promote a consistent approach to information governance. The IGG is responsible for developing and sharing best practice across the organisation and ensuring that information governance standards are included with other work programmes and projects.

- The committee co-ordinates the review of the Trust’s information governance management and accountability arrangements and produces and monitors the
annual information governance work programme. The Trust recognises that other key staff will be involved in, and contribute to, this work programme.

- The IG Group will report to the Executive Performance & Corporate Risk Group and issues will be escalated to the Board as appropriate.

- Terms of Reference for the IGG are attached as Appendix A.

**Formal Sub Committees to the Board – Audit Committee and Quality, Clinical Governance & Risk Committee**

- The IGG is responsible for preparing the annual Information Governance Toolkit assessment for sign off. In addition, the IGG reports on specific information governance issues to the Executive Performance & Corporate Risk Group.

- Information Governance also forms part of the annual internal audit process.

2.20 It is recognised that the successful achievement of the Trust’s Information Governance policy and framework is dependent upon the input and commitment of staff at all levels of the organisation.

2.21 All new starters receive basic information governance training as part of their induction training.

2.22 All existing staff must complete mandatory annual information governance refresher training. The Health and Social Care Information Centre (HSCIC) Information Governance e-learning Training Tool (IGTT) is the main delivery method for staff to complete their mandatory training, but to provide staff with greater choice and flexibility for completing their annual IG refresher training, the Trust Learning & Development Service provide taught sessions using the IG Toolkit material as an alternative to the on-line training. There is also a Information Governance Training Video via the Trust Intranet.

2.23 Additional training is provided to staff in key Information Governance roles, either via the HSCIC IGTT or by other means.

2.24 The IGG takes overall responsibility for ensuring compliance with the policies, procedures and guidelines summarised in this framework, reporting to the SIRO and the Caldicott Guardian, who ensure Trust Board level assurance. The SIRO and the Caldicott Guardian are also members of the IGG.

2.25 The Trust will carry out regular information governance audits to monitor the effectiveness of the framework and the supporting policies and guidelines. The results of the audits will be reviewed by the IGG to inform and develop the annual information governance work programme.

2.26 The Trust will carry out regular reviews of its use of patient personal information, ensuring that patients are informed of any new use of their information and communicate this to those affected. Any information literature relating to use will be updated as required to ensure patients are fully aware of how their information is being used.

3. **INFORMATION HANDLING AND PROCESSING**

3.2 Staff can ensure their compliance under the law by following Trust policies and the NHS best practice they incorporate.

3.3 In addition to its legal requirements, Trust policies in respect of information governance shall also take heed of NHS best practice in this area e.g. NHS Confidentiality – Code of Practice, NHS Records Management Code of Practice 2006, NHS Litigation Authority Risk Management Standards.

3.4 The Trust employs a number of systems to protect data, staff and service continuity. However, it is each staff member’s individual responsibility not to undertake any activity on Trust equipment that might compromise data security and / or confidentiality.

3.5 The Trust shall employ effective arrangements to maintain the confidentiality and security of data. These include:

- staff receive appropriate training before being permitted access to computer systems;
- ensure application security and password access protections;
- provide effective anti-virus and anti-malware software to ensure system access and data security are maintained;
- ensure the secure sending of emails to protect PID and prevent the sending of insecure email traffic;
- prevent the unintentional or intentional loss of PID and other information from our network, in particular:
  - ensure the secure encryption of all electronic removable media and portable computing devices;
  - restrict the connection of removable media devices to our network to only authorised devices.
- ensure the physical security of the computer equipment and systems;
- ensure secure and appropriate storage and access to paper records;
- ensure computer network resilience and allow for the disaster recovery of systems and data.

4. PROPOSED INFORMATION SYSTEM PROCUREMENTS

4.1 Any system, computerised or manual, that may hold PID, including PID relating to service users, carers or staff, shall be considered by the IGG before its procurement. The definition of PID is set out in Section 5 of this policy.

4.2 Information governance aspects to be considered by the IGG for each proposed system where it is intended, or likely in the future, to contain PID will be that:

- strong access controls are present;
- audit trails and monitoring of user activity are present;
- arrangements for data back-up and system resilience are understood;
- how data is to be considered for continuing relevance & secure final deletion / archiving is understood;
- confidentiality clauses are to be present in respect of any third party services employed in the development, installation or maintenance of the system;
- secure access to, rather than transfer of, data is present wherever practicable;
• whether, if involving data on large numbers of individuals, penetration testing should occur;
• if accreditation applies to the system that this has been obtained prior to procurement;
• the system’s forensic investigative readiness procedure is understood;
• the system will not adversely impair any other existing system’s availability or the data communications bandwidth between Trust sites.

4.3 The Trust endorses the proactive use of information to improve service delivery and the quality of care it provides. Information within the Trust should be of the highest quality possible (taking into account the cost effectiveness of achieving this standard) in respect of its accuracy, timeliness and relevance.

4.4 In supporting these goals it may not be possible to secure full assurance on the above points in every case for new systems, but the IGG shall ensure that risk management and mitigation is present for each to an acceptable level.

5. TRUST DEFINITION OF PERSONALLY IDENTIFIABLE DATA (PID)

5.1 Personally identifiable data or information (PID) is anything that contains the means to identify a person (e.g) name, address, postcode, date of birth, NHS number, National Insurance number, photograph etc.

5.2 The Caldicott Committee: Report on the Review of Patient-identifiable Information, December 1997 states:

“All items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patients and hence should be appropriately protected to safeguard confidentiality”

These items include:

<table>
<thead>
<tr>
<th>Surname</th>
<th>Forename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initials</td>
<td>Address</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>Other dates (e.g. death, diagnosis)</td>
</tr>
<tr>
<td>Postcode</td>
<td>Occupation</td>
</tr>
<tr>
<td>Gender</td>
<td>NHS Number</td>
</tr>
<tr>
<td>National Insurance Number</td>
<td>Ethnic Group</td>
</tr>
<tr>
<td>Local Identifier (e.g. Trust PAS index number, GP practice number)</td>
<td>Telephone Number</td>
</tr>
</tbody>
</table>

or anything else that may be used to identify a service user, carer or staff member directly or indirectly. For example, rare conditions, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

6. FREEDOM OF INFORMATION ACT

6.1 The Trust will undertake to make non-confidential information widely available in line with its responsibilities under the Freedom of Information Act. The procedures for staff to follow in the event of a request for information being made under the Act are set out in the trust’s intranet within the Directorate of Quality’s Protocol on Freedom of Information Act 2000.
7. **USE OF INFORMATION WITHIN THE TRUST**

7.1 **The Trust supports the proactive use of information within the organisation and shall maintain an Information Governance strategy to prioritise its support and development.**

7.2 **In addition to relevant policy, staff in their day to day use of information shall adhere to the six general Caldicott Principles and the eight Data Protection Act Principles when considering their use of data:**

**Caldicott Principles:**

1. Justify the purpose of retaining patient identifiable information.
2. Do not use patient identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient identifiable information.
4. Only access patient identifiable information on a strict 'need to know' basis.
5. Be aware of your responsibilities regarding patient identifiable information.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality

**Data Protection Act Principles:**

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

   (a) At least one of the conditions in Schedule 2 is met, and
   (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.3 **If any member of staff is unclear as to his or her responsibilities in respect to any of these principles they should seek advice, in the first instance from their line manager.**
8. USE OF INFORMATION BETWEEN THE TRUST AND ITS PARTNERS

8.1 The usage of service user data between partner organisations is principally covered within the relevant Trust policies set out in Section 13.

8.2 The circulation of anonymised data and general performance data outside the Trust shall always be subject to established procedures, normally as provided for within statute, contractual agreements or requirements set down by our regulator Monitor. The Trust supports the proactive use of information to support patient care, but any provision of such data, or similar, shall not occur outside the Trust without the prior permission of an Operational Director, Chief Executive or Director of Finance.

8.3 To avoid duplication and ensure consistency, requests for service delivery information from our partner organisations should be processed through the Head of Information.

9. DISPOSAL OF CONFIDENTIAL WASTE AND THE USE OF SHREDDERS

9.1 All paper PID that is no longer required must be disposed of either by shredding or the use of confidential waste bags / bins (as contracted by the Trust). Under no circumstances should paper PID be placed in a normal waste paper bin or used as scrap paper.

9.2 Where a shredder is used it must be a cross cutting, micro cutting or confetti cutting model which complies with at least security level DIN 3.

9.3 All software and electronic PID must be removed from redundant hardware and media storage devices before the hardware or devices are removed from the Trust.

9.4 It is important that all information is disposed of in a secure manner. The NHS is most at risk in this area and there have been many occasions when personal information concerning patients has been discovered in public amenity waste disposal or in other public areas.

9.5 All members of staff will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper by using examples of ‘real life situations’ during information governance training sessions, where staff will be informed of how to dispose of PID waste products.

10. INFORMATION GOVERNANCE BREACHES AND INCIDENT MANAGEMENT

10.1 Staff are encouraged to report all information security incidents, whether suspected or actual so that they can be investigated, appropriate actions taken to address the incident and lessons learnt to ensure that they do not re-occur.

10.2 All information security incidents and near misses should be reported by staff using the on-line incident reporting system, Ulysses, with the risks being graded in accordance with the risk matrix appended to the Trust’s ‘Policy for the Reporting and Management of Incidents including Serious Incidents’.

10.3 All IG SIRI’s level 2 will be reported via the IG Toolkit Incident Reporting Tool to the Department of Health, Information Commissioners Office and other regulators.

10.4 Information security incidents are reported to the IGG via the Caldicott Incident Log, which shows the outcome, the action taken and the further action required in respect of the incident.
10.5 In respect of data loss or confidentiality breaches the Trust shall comply with the Trust Annual Report disclosure; Serious Untoward Incident reporting processes and disclosure to the Office of the Information Commissioner as appropriate, depending upon the severity of the incident(s) concerned.

11. ORGANISATIONAL PROCESS CHANGE, SERVICES, SYSTEMS AND INFORMATION ASSET IMPLEMENTATION

11.1 The objective of this element of the Information Governance Policy is to have in place procedures to ensure that, prior to the implementation of processes, services, systems and other information assets the change is monitored and risk assessed by the IGG.

11.2 It is vitally important that the impact of any proposed changes to the organisation’s processes and / or information assets are assessed to ensure that the confidentiality, integrity and accessibility of personal information is maintained.

11.3 There are two processes for information asset changes depending on the scale and level of risk associated with the proposed implementation:

- Major Changes: This process encompasses changes which will have a major effect on Information Assets, for example:
  - Installing a brand new system (hardware, software etc);
  - Replacing an existing system (hardware, software etc);
  - Opening of a new ward / unit;
  - Transfer of premises for an existing ward / unit;
  - Significant changes to the working environment (e.g) an office move that will result in an increased level of foot traffic in and around sources of confidential information.

- Minor Changes: This process encompasses changes which will have a minor effect on Information Assets, for example:
  - Upgrades or updates to a system (hardware, software etc)
  - Small changes to the working environment (e.g) temporary change to working conditions as a result of work undertaken by a third party contractor.

As part of the process, if appropriate, a privacy impact assessment (PIA) should be carried out whenever a new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled - see Section 12 below.

11.4 The Change Implementation Process will involve:

- The completion of an appropriate Change Request Form (Appendices A and B);
- A form sent to the IGSC for circulation prior to the next available IGSC meeting;
- If required, attendance at the IGSC meeting by the Information Asset Owner or equivalent for discussion with IGSC pending approval;
- In the event that the change is not approved, feedback will be provided to the requester in order that appropriate action can be taken and for the form to be resubmitted.

11.5 It is important that proposed changes to the Trust’s processes and / or information assets are approached in a structured way which ensures that the implementation of such changes are introduced in a secure and considered manner.

11.6 Structured project management means managing the project in a logical, organised
way, following defined steps, for example utilising PRINCE2 methodology for major system changes.

12. PRIVACY IMPACT ASSESSMENT (PIA)

12.1 The objective of the Privacy Impact Assessment is for all new project, processes and systems to comply with confidentiality, privacy and data protection requirements. The purpose of the PIA is to highlight to the organisation any associated privacy risks.

12.2 A PIA is a structured assessment of the potential impact on privacy for new or significantly changed processes. The PIA should form part of the overall risk assessment of any process or project.

12.3 A PIA should be undertaken at the start of a project, before new processes or systems are introduced.

12.4 The key deliverable of a PIA is a report that details impacts identified and the solutions or actions that will deal with them.

12.5 The appointed Information Asset Owner (IAO) for the new information system is required to produce the PIA. The IGSC is responsible for receiving and reviewing the PIA on behalf of the Trust.

12.6 In order to conduct the PIA process, a decision tree is shown in Appendix D.

12.7 An initial assessment needs to be undertaken to determine whether a PIA is necessary for a project and, if so, what level of PIA is required - whether a full-scale PIA, a small-scale PIA or just a check against compliance with the law.

12.8 Before adequately answering the screening questions, the following information must be gathered:

- Project outline – depending on the project status, this can range from a single sheet summary to a full business case;
- Stakeholder analysis – this should include the key groups that may have an interest in or be affected by the project or other work activity;
- Environmental scan – this involves benchmarking other similar projects or cases where the intended technology has been utilised. It may also be useful to consider other PIAs which have already been undertaken within the Trust.

12.9 A Screening Process can then be carried out to determine which PIA to carry out.

12.10 There are three types of Privacy Impact Assessments:

- Full-scale PIA;
- Small-scale PIA;
- Data Protection Compliance check.

**Full Scale PIA:**

- These require more extensive consultation with stakeholders and the Project Board than small-scale PIAs;
- A PIA consultative group will need to be formed consisting of the project’s stakeholders to discuss the privacy impact in detail;
- The documentation is more formalised for a full scale PIA;
- A Privacy and Data Protection Compliance Check will also need to be completed for a full scale PIA.
Small Scale PIA:

• These are less formalised and require less resources to complete;
• It is more likely focused on specific aspects of a large-scale project rather than a project as a whole;
• A Privacy and Data Protection Compliance Check will also need to be completed for a small-scale PIA.

Data Protection Compliance Check

• A Data Protection Compliance check must be completed if a new or significantly changed process that involves PID is introduced.

12.11 The templates in Appendix E should be used as a basis for any full-scale, small-scale PIA and compliance check.

12.12 It is suggested that the five phases of conducting the PIA process are

• Preliminary phase – review outcomes and documents from the initial assessment; hold preliminary discussions with relevant parts of the organisation, any key participating organisations and advocates for stakeholder groups; prepare project background paper;
• Preparation phase – develop consultation plan; devise communication processes;
• Consultation and analysis phase – implement the consultation plan; identify design issues and privacy problems; document the problems and actions in an issues register;
• Documentation phase – consolidate the mitigation measures into a final version of the issues register; produce a PIA report which documents the PIA process and includes analysis of issues, justification of any privacy intrusion, lessons learned and expected outcomes;
• Review and audit phase - ensure that the design features arising from the PIA are implemented and are effective; prepare a review report to publish.

12.13 It is recommended that the PIA Handbook is referred to for guidance. It is available using the following link:


13. KEY SUPPORTING POLICIES AND GUIDELINES

13.1 Various operational aspects of information governance and information use as they relate to specific areas and activities are documented and linked in relevant Trust policies and guidelines, which are available to staff via the Trust Intranet. The principal integrated policies and guidelines are:

• Access to Records under DPA and Access to Health Record
• Health-Records-under-Data-Protection-and-Records-Management-NHS-Code-of-Practice
• Data Protection and Confidentiality Policy
• Securing Removable Media Devices and Secure Email Policy
• Freedom of Information Act - Trust Protocol
• Data Quality Policy
• Integrated Subject Access Request Policy
• IT Acceptable Use Policy
• Removable Media and Secure Email Policy
14. POLICY DISTRIBUTION

14.1 All policies and guidelines relating to information governance will be made available to staff through the Trust Intranet.

14.2 Key messages relating to information governance will also be communicated to all staff via cascades from the DM via their directorate specific management groups.
APPENDIX A

TERMS OF REFERENCE
INFORMATION GOVERNANCE GROUP

Dorset Healthcare University NHS Foundation Trust hereby establishes a group to be known as Information Governance Group (the ‘group’).

1. Purpose

1.1 The Information Governance Group is accountable to the Executive Performance & Corporate Risk Group. Its purpose is to support and drive the broader information governance agenda and to provide Trust Directors with the assurance that effective information governance best practice mechanisms are in place within the organisation.

2. Duties

2.1 To ensure that appropriate and comprehensive Information Governance framework and systems are in place throughout the organisation in line with national standards.

2.2 To review the Organisation’s management and accountability arrangements for Information Governance.

2.3 To develop, review and update IG policy and associated IG implementation strategy.

2.4 To prepare the annual Information Governance assessment for sign off by the Senior Information Risk Officer (SIRO) on behalf of the Board of Directors.

2.5 To develop the Organisation’s Information Governance work programme.

2.6 To ensure that the Organisation’s approach to information handling is communicated to all staff and made available to the public.

2.7 To oversee the activities of staff in respect of data protection, confidentiality, security, information quality, records management and Freedom of Information responsibilities.

2.8 To offer support, advice and guidance to the Caldicott Function and Data Protection programme within the Organisation.

2.9 To monitor the Organisation’s information handling activities to ensure compliance with law and guidance.

2.10 To ensure that training made available by the Organisation is taken up by staff as necessary to support their role.

2.11 To provide a focal point for the resolution and/or discussion of Information Governance issues.

3. Chair, Members

3.1 In extremis, any member of the group who is able to speak and be heard by each of the other members will be deemed to be present in person and will count towards the quorum.

- Senior Information Risk Officer (SIRO) (Chair)
- Caldicott Guardian / Deputy Caldicott Guardian
- Data Protection Officer / Deputy SIRO (Vice-Chair)
- Chief Clinical Information Officer
- IT Security Manager
- Trust Secretary
- Information Governance Manager
- Clinical Leads for Trust electronic patient record systems
• Freedom of Information Lead
• Health Records Manager / Corporate Records Manager
• Data quality lead / representative from Systems Management Group
• Learning & Development representation

Each member is required to nominate a deputy to attend in his/her absence as agreed with the chair.

3.2 The Senior Information Risk Officer or his/her deputy will chair the meeting.

4. **Quorum**

4.1 In order for decisions taken by the group to be valid, the meeting must be quorate. This will consist of five members of the group being present at the point when any business is transacted.

4.2 The Caldicott Guardian and the Senior Information Risk Officer or their respective deputies are required to be present in order for the group to be considered quorate.

5. **Frequency of Meetings**

5.1 The IG Group will meet at least quarterly to fulfil its remit.

5.2 The IG Group will report to the Executive Performance & Corporate Risk Group and issues will be escalated to the Board as appropriate.

5.3 **Organisation:**

The meeting agenda and supporting papers will be distributed at least 5 working days in advance of the meetings to allow time for members’ due consideration of issues. All papers will clearly state the agenda reference, the author and the purpose of the paper, together with the recommended actions to be taken.

Papers will be available at least 5 clear days before each meeting and will not be tabled unless exceptionally with the Group Chair’s agreement.

6. **Standing Agenda Items**

• Welcome and Apologies (Chair)
• Minutes of the last meeting (Chair)
• Matters Arising (Chair)
• Review of work plan (IG Manager / all)
• Caldicott Enquiry Review (Caldicott Guardian / Deputy)
• Data Quality Assurance Framework Report (Data Quality Lead)
• Freedom of Information Report (Freedom of Information Lead)
• Data Protection Breach report (IG Manager)
• Risk Register review (Trust Secretary)
• Review of national regulation / policy changes (IG Manager)
• IG Training review (Learning & Development representative)
• Policy approval and ratification (all)

7. **Relationships with Other Groups**
7.1 The minutes of the group meetings will be formally recorded and submitted to the Executive Performance & Corporate Risk Group on a quarterly basis. The Chair of the Group will draw to the attention of the Executive Performance & Corporate Risk Group any issues that require escalation.

7.2 The Dorset Healthcare University NHS Foundation Trust Board has appointed to the Board a Caldicott Guardian and a Senior Information Risk Officer. These representatives will escalate to the Board information governance agenda items which may need Board level approval.

7.3 The Group will act as a parent to the following sub-groups, which will relate to and report to the Group regularly by way of escalation and provision of agreed reports:

- Systems Management Group (for Data Quality Assurance Framework and production of system specific policy/procedures relating to Information Governance issues)

8. Monitoring Effectiveness

8.1 Review

Terms of reference are reviewed annually or in the light of changes in practice or national/local guidance. The group will review annually its own performance, including the extent to which it has operated in satisfaction of its terms of reference.

8.2 The IG Group shall submit an annual IG Toolkit report to the Board for sign off, prior to formal publication of the assessment, which is required before or on 31 March each year.

Reviewed: 28th January 2015, next review date January 2016

9. Document Owner

9.1 The Chair is the owner of this document and of any Board minute authorising any amendment.
APPENDIX B: MAJOR CHANGE REQUEST FORM

Major Change Request Form

This form constitutes the formal log of a change and must be kept as a record of that changes history. A copy must be kept by the Information Asset Owner and also by the Information Governance Committee. Form must be received by the Head of Information a minimum of one week before the next IGSC meeting. This date should be a minimum of four weeks before the proposed implementation date for Major Changes and two weeks before the proposed implementation date for Minor changes.

| Reference Number (Completed by IGG): |
| Request received from: |
| Information asset owner: |

| Change required to: Information System/Hardware/Ward/Unit/Other |
| Description of change to information asset and details if necessary of the tool used to approach the project |

| Why is the change needed? |

| What are the advantages of the change? |

| What are the disadvantages of the change? |

| What are the risks of implementing this change? |

| What are the risks of NOT implementing this change? |

| What are the potential impacts both positive and negative on the service and its users? |

| Timetable for implementation |
| Proposed implementation date: |
| Resource and effort involved in implementation: |

| The following section is to be completed at the IGG meeting where the proposed change is reviewed and assessed prior to implementation. |
| Has the IGG stated that a PIA should be completed prior to implementation Y/N: |
| Details: |
| Process change approved for implementation Y/N: |
| Details: |

| Signed and agreed by: |
| Requester: | IGG Chair: | Head of IT/Caldicott Guardian: | IGG Member: |
| Date: | Date: | Date: | Date: |
## APPENDIX C: MINOR CHANGE REQUEST FORM

### Minor Change Request Form

This form constitutes the formal log of a change and must be kept as a record of that changes history. A copy must be kept by the Information Asset Owner and also by the Information Governance Committee. Form must be received by the Head of Information a minimum of one week before the next IGSC meeting. This date should be a minimum of four weeks before the proposed implementation date for Major Changes and two weeks before the proposed implementation date for Minor changes.

<table>
<thead>
<tr>
<th>Reference Number (Completed by IGG):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request received from:</td>
</tr>
<tr>
<td>Information asset owner:</td>
</tr>
<tr>
<td>Change required to: Information System/Hardware/Ward/Unit/Other</td>
</tr>
</tbody>
</table>

1. **Description of change to information asset**

2. **Main reason for change**

3. **Timetable for implementation**
   - Proposed implementation date:
   - Resource and effort involved in implementation:

The following section is to be completed at the IGSC meeting where the proposed change is reviewed and assessed prior to implementation.

<table>
<thead>
<tr>
<th>Has the IGG stated that a PIA should be completed prior to implementation Y/N:</th>
<th>Process change approved for implementation Y/N:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details:</td>
<td>Details:</td>
</tr>
</tbody>
</table>

Signed and agreed by:

<table>
<thead>
<tr>
<th>Requester:</th>
<th>IGG Chair:</th>
<th>Head of IT/Caldicott Guardian:</th>
<th>IGG Member:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>Date:</td>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

---

IN-101 V.4 April 2015 22
APPENDIX D: PIA Process Maps

PIA Decision Tree

Initial Assessment

Full scale PIA?

YES

Complete full scale PIA & privacy & other legal compliance check, including DP compliance check.

NO

Small scale PIA?

YES

Complete small scale PIA & privacy & other legal compliance check, including DP compliance check.

NO

Privacy & other legal compliance check?

YES

DP compliance check?

NO

No further action required

NO
Initial Assessment Process Map

APPENDIX D: PIA Process Maps

1. Initial Assessment process map
2. Preparation
3. Project outline
4. Stakeholder analysis
5. See what else is out there
6. Go through PIA screening questions to highlight potential privacy issues
7. Decide which level of assessment is required
APPENDIX D: PIA Process Maps

Full Scale and Small Scale PIA Process Map

- Preparation
- Preliminary work
- External consultation/Information gathering
- Internal analysis
- Documentation and conclusion
- Review and audit
APPENDIX E: PIA TEMPLATES

FULL-SCALE PIA QUESTIONS

Enter the project title here - this box will expand as required

Technology
1) Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

This box will expand as required

Identity
2) Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

3) Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

Multiple organisations
4) Does the project involve multiple organisations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners')?

Data
5) Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?

6) Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?
7) Does the project involve new or significantly changed handling of personal data about a large number of individuals?


8) Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

Exemptions and exceptions

9) Does the project relate to data processing which is in any way exempt from legislative privacy protections?

10) Does the project’s justification include significant contributions to public security measures?

11) Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

Once each of the 11 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion whether a full-scale PIA is warranted. You should also consider, particularly on large projects, whether the whole project or perhaps only key sections should be assessed.

If your answers to the above questions indicate that a full-scale PIA is required then you should now undertake compliance checks (see page 20 below) to determine whether these are also required.

If your answers indicate that a full-scale PIA is not required then progress to the screening questions for a small-scale PIA.
**SMALL-SCALE PIA QUESTIONS**

Enter the project title here - this box will expand as required

**Technology**

1) Does the project involve new or inherently privacy-invasive technologies?

This box will expand as required

**Justification**

2) Is the justification for the new data-handling unclear or unpublished?

**Identity**

3) Does the project involve an additional use of an existing identifier?

4) Does the project involve use of a new identifier for multiple purposes?

5) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?

**Data**

6) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?

7) Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?
8) Does the project involve new linkage of personal data with data in other collections, or significant changes in data linkages?

Data Handling

9) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?

10) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?

11) Does the project involve new or changed data security arrangement that may be unclear or unsatisfactory?

12) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

13) Does the project involve new or changed data retention arrangements that may be unclear or extensive?

14) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

15) Will the project give rise to new or changed data-handling that is in any exempt from legislative privacy protections?
Once each of the 15 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion whether a small-scale PIA is warranted. You should also consider, particularly on large projects, whether the whole project or perhaps only key sections should be assessed.

It is important to consider the various perspectives of each of the stakeholder groups involved; this will ensure that potential risks are not overlooked.

If your answers to the above questions indicate that a small-scale PIA is required then you should now undertake compliance checks (see below) to determine whether these are also required.

If your answers indicate that a small-scale PIA is not required then progress on to the compliance checks.

**COMPLIANCE CHECKS**

Privacy and other legal compliance check

It is important that the proposed project complies with all relevant privacy-related laws. If any of the following questions are answered "Yes", then a privacy law compliance check should be conducted:

1. Does the project involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or other forms of regulation, other than the Data Protection Act?

In particular, the following should be considered:

- The Human Rights Act 1998
- The Privacy and Electronic Communications Regulations 2003
- All of the Trust’s relevant policies and procedures.

2. Does the project involve any activities (including any data handling) that are subject to common law constraints relevant to privacy?

In particular, the following should be considered:

- Confidential data relating to a person, as that term would be understood under the common law of confidence;
- The tort of privacy as it develops through case law.
3. Does the project involve any activities (including any data handling) that are subject to less formal good practice requirements relevant to privacy? In particular, the following should be considered:
   - industry standards, e.g. the BS ISO / IEC 17799:2005 Information Security Standard;
   - Industry codes, e.g. the NHS Code of Practice on Confidentiality.

4. Criteria for Data Protection Act compliance

If the following question is answered "Yes", then a Data Protection Act compliance check should be conducted:

Does the project involve the handling of any data that is personal data, as that term is used in the Data Protection Act?

‘Personal data’ means data which relate to a living individual who can be identified:
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act Section 1).

Note that compliance checking activities are usually conducted reasonably late in the overall project schedule, once detailed information about business processes and business rules is available.
## APPENDIX F……: Equality Analysis Form

<table>
<thead>
<tr>
<th>1. Policy/Practice/Service development</th>
<th>Directorate</th>
<th>New or existing?</th>
<th>Date of Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION GOVERNANCE POLICY (INCORPORATING INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK)</td>
<td>Finance and Performance Management</td>
<td>New</td>
<td>24/02/2015</td>
</tr>
</tbody>
</table>

2. Briefly provide an overview of the policy/practice/service development and describe the aims, objectives and purpose of the Policy/Service:
The purpose of this policy is to reinforce Dorset HealthCare University NHS Foundation Trust’s commitment to Information Governance and provide staff with clear guidelines as to their roles and responsibilities.

3. Who will be affected? E.g. staff, patients, service users etc
   Staff

3. Please demonstrate below the potential impacts on people or equality groups with protected characteristics. List the main sources of data, research and other sources of evidence reviewed to determine the impact or potential impact on each equality group (protected characteristic)

<table>
<thead>
<tr>
<th>Equality target group (protected characteristic)</th>
<th>Is the policy/practice/service development relevant to this equality area? Yes/No. If No what evidence did you rely on to reach this conclusion.</th>
<th>Assessment of Potential Impact: High/ Medium/ Low/ Not Known</th>
<th>Required Actions or Action Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive (+)</td>
<td>Negative (-)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy equally applicable to all staff with no sensitive specific</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>Gender reassignment</td>
<td>Policy equally applicable to all staff with no transgender sensitive specific</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>Race</td>
<td>Policy equally applicable to all staff with no ethnicity sensitive specific</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>Sex</td>
<td>Policy equally applicable to all staff with no gender sensitive specific</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>Disability</td>
<td>Policy equally applicable to all staff with no disability sensitive specific beyond those already existing in the use of IT and Systems with staff with a disability and for which Suitable accommodation will have been made</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>Age</td>
<td>Policy equally applicable to all staff with no age sensitive specific</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Religion or Belief</td>
<td>Policy equally applicable to all staff with no age sensitive specific</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>Sexual orientation</td>
<td>Policy equally applicable to all staff with no sexual orientation sensitive specific</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Impact</td>
<td>Mitigation</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>Marriage and Civil Partnership</td>
<td>Policy equally applicable to all staff with no marital sensitive specific</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Pregnancy and Maternity</td>
<td>Policy equally applicable to all staff with no Pregnancy or maternity sensitive specific</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

4. Engagement and Involvement. How have you engaged stakeholders in gathering evidence, testing the available evidence and what stakeholders/groups both internal and external were consulted and when? What was the outcome of that engagement and involvement?  
NA

5. Summary of Analysis: In considering the evidence and engagement activity listed above, summarise the impact of your work. Consider whether the evidence shows potential for differential impact, if so state whether this is adverse or positive and for which groups. Detail how any negative impacts will be mitigated. Are there any alternative measures that could be taken which could achieve the desired aim without the adverse impact identified? Can the adverse impact or indirect discrimination be objectively justified? Specify how certain protected groups will be included in services or how their participation in public life will be expanded.  
NA

6. Consider and detail below how the proposals impact on and have due regard to the need to eliminate discrimination, harassment and victimisation, advance equality of opportunity between people who share a protected characteristic and those who do not and foster good relations between people who share a protected characteristic and those who do not.  
NA

6.1 Eliminate discrimination, harassment and victimisation. Where there is evidence address each protected characteristic (age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation, marriage and civil partnership).  
NA

6.2 Advance equality of opportunity. Where there is evidence address each protected characteristic (age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation).  
NA
6.3 Promote good relations between groups. Where there is evidence address each protected characteristic (age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation). NA

7. What is the overall impact? Consider whether there are different levels of access experienced, needs or experiences, whether there are any barriers to engagement and what is the combined impact? NA

8. Addressing the impact on equalities. Provide an outline of what broad action should be considered by you or any other body to address any inequalities identified through the evidence and consultation. Outline what changes will be made to the policy, practice or service as a result, when and by whom. NA

9. Action planning for improvement and implementation. Provide an outline of the key actions based on any gaps, challenges and opportunities identified. Actions to improve the policy, practice or service development need to be summarised including any general action to address specific equality issues and data gaps that need to be addressed through further research or consultation. Use the attached Action Improvement Plan. NA

10. Monitoring and review. Detail the processes for monitoring, how this will be measured and when and how the policy, practice, service development will be reviewed. NA

11. Publication. Outline how and where this assessment will be published

This assessment will be published on the Trust Intranet

| Review Date | 26/02/2015 |
| Name of responsible Director | Jackie Chai |
| Assessment Completed By | Chris Gray | Date signed | 24/02/2015 |