INFORMATION GOVERNANCE POLICY

<table>
<thead>
<tr>
<th>Version:</th>
<th>3.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorisation Committee:</td>
<td>Information Strategy Steering Group (ISSG)</td>
</tr>
<tr>
<td>Date of Authorisation:</td>
<td>May 2014</td>
</tr>
<tr>
<td>Ratification Committee Level 1 documents):</td>
<td>Quality Governance Steering Group (QGSG) Policy ratification and monitoring group</td>
</tr>
<tr>
<td>Date of Ratification Level 1 documents):</td>
<td>18 June 2014</td>
</tr>
<tr>
<td>Signature of ratifying Committee Group/Chair Level 1 documents):</td>
<td>Martin Stephens AMD Clinical Effectiveness</td>
</tr>
<tr>
<td>Lead Job Title of originator/author:</td>
<td>Trust Records Manager</td>
</tr>
<tr>
<td>Name of responsible individual:</td>
<td>Paul McMahon</td>
</tr>
<tr>
<td>Date issued:</td>
<td>21 August 2014</td>
</tr>
<tr>
<td>Review date:</td>
<td>21 August 2017</td>
</tr>
<tr>
<td>Target audience:</td>
<td>Trust Managers Information Governance leads and Information leads</td>
</tr>
<tr>
<td>Key words:</td>
<td>Information, Information Governance, Information handling, IG, IGT, Information assurance</td>
</tr>
<tr>
<td>Main areas affected:</td>
<td>Information handling and management</td>
</tr>
<tr>
<td>Consultation:</td>
<td>Members of IGSG and ISSG Committees.</td>
</tr>
<tr>
<td>Changes made to this version:</td>
<td>Version 3.2 issued Aug 2014 including new section on approval of IG Toolkit assessment, removal of IG incident management section and other minor updates to wording.</td>
</tr>
<tr>
<td>Minor changes approved:</td>
<td>Update approved by PRAM</td>
</tr>
<tr>
<td>Equality Impact Assessments</td>
<td>10 May 2010</td>
</tr>
<tr>
<td>Number of pages:</td>
<td>18 including appendices</td>
</tr>
<tr>
<td>Type of document:</td>
<td>Level 1</td>
</tr>
</tbody>
</table>

The Trust strives to ensure equality of opportunity for all, both as a major employer and as a provider of health care. This Information Governance Policy has therefore been equality impact assessed by the IGSG to ensure fairness and consistency for all those covered by it, regardless of their individual differences, and the results are available on request.
## Contents

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>1 Introduction.</td>
<td>3</td>
</tr>
<tr>
<td>2 Scope.</td>
<td>3</td>
</tr>
<tr>
<td>3 Purpose.</td>
<td>4</td>
</tr>
<tr>
<td>4 Related Trust Policies.</td>
<td>4</td>
</tr>
<tr>
<td>5 Roles and Responsibilities.</td>
<td>4</td>
</tr>
<tr>
<td>6 Information Governance Management.</td>
<td>6</td>
</tr>
<tr>
<td>7 Implementation.</td>
<td>10</td>
</tr>
<tr>
<td>8 Education and Dissemination</td>
<td>10</td>
</tr>
<tr>
<td>9 Process for Monitoring Compliance and Effectiveness.</td>
<td>10</td>
</tr>
<tr>
<td>10 Arrangements for review of the policy.</td>
<td>11</td>
</tr>
<tr>
<td>11 References.</td>
<td>11</td>
</tr>
</tbody>
</table>

### Appendices

- **Appendix A** UHSFT Information Governance Steering Group Terms of Reference | 12
- **Appendix B** UHSFT Information Governance Reporting and Committee Structure | 14
- **Appendix C** UHSFT Guide to Conducting a Privacy Impact Assessment | 15
EXECUTIVE SUMMARY

- Information Governance is a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.
- Within the NHS Information Governance requirements have been traditionally addressed by separate work streams covering the following areas:
  - Confidentiality and Data Protection
  - Information Security
  - Data Quality
  - Records Management
- The NHS has established a framework of Information Governance assurance based on organisations completing an assessment of compliance with requirements published in the NHS Information Governance Toolkit.
- This policy outlines the Trust’s approach to the management of Information Governance and information handling.
- This policy explains the accountability and reporting arrangements for Information Governance in the Trust, describes how assurance is provided that the Trust continues to meet the minimum standards of Information Governance compliance required by the NHS Information Governance Toolkit.

1. INTRODUCTION

1.1 Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in Clinical Governance, service planning and performance management.

1.2 It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and management accountability and structures are in place to provide a robust governance framework for information management. Within the NHS this aspect of information management is termed Information Governance (IG).

1.3 This policy details the arrangements in place to provide a robust IG framework in the Trust and to provide assurance that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

2. SCOPE

2.1 IG is formed by those elements of law and policy from which applicable IG standards are derived. It encompasses legal requirements, central guidance and best practice in information handling including:

- The common law duty of confidentiality
- Data Protection Act 1998
- Human Rights Act
- Information Security
- Information Quality
2.2 This policy provides a high level description of the arrangements in the Trust for developing, implementing and monitoring IG policy and procedure. Detailed procedural guidance for staff is contained in separate specific policies listed in section 4 and therefore the contents of this document are most relevant to staff who exercise a supervisory or managerial role or have a role with an information management component.

3. Purpose

3.1 The purpose of the policy is to provide a policy statement on the use and management of information in the Trust and describe the arrangements for providing assurance to the Trust Board that IG standards are defined and met and IG incidents appropriately managed.

4. RELATED TRUST POLICIES

4.1 The following Trust Policies relate to the management of information and together underpin the Trust’s IG Assurance Framework and form part of the Trust IG Framework.

   a. Data Protection and Confidentiality Policy
   b. Freedom of Information Policy
   c. IM&T Security Policy
   d. Records Management Policy
   e. Access to Personal Records Policy and Procedure
   f. Data Quality Strategy and Policy
   g. Raising concerns /Whistle Blowing Policy
   h. Risk Management Policy and Procedures
   i. Incident Management and Reporting Policy
   j. Communications policy
   k. Web policy

4.2 The Trust has also published an IG Strategy with a work plan that is updated annually to provide a programme of continual improvement in the standards of Information Governance applied in the Trust.

5. ROLES AND RESPONSIBILITIES

5.1 Trust Board

5.1.1 The Trust Board is ultimately responsible for ensuring that the Trust corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

5.1.2 The Trust Board will be updated on Information Governance issues via reports from the Information Strategy Steering Group (ISSG) who
have delegated responsibility from the Trust Executive Committee (TEC) for monitoring the standards of Information Governance within the Trust. The Director of Transformation as Lead executive for Information Governance and Senior Information Risk Officer (SIRO) will bring to the Boards attention individual issues relating to Information Governance not covered in ISSG reports as appropriate.

5.2 Chief Executive

5.2.1 The Chief Executive has overall responsibility for the standards of Information Governance in the Trust. As the accountable officer she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

5.3 Caldicott Guardian

5.3.1 The Trust's Caldicott Guardian is the Director of Nursing who has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Trust Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

5.3.2 The duties and responsibilities of the Trust Caldicott Guardian are outlined in the Trust Confidentiality and Data Protection Policy.

5.4 Director of IM&T/Information Governance Steering Group

5.4.1 The Director of IM&T is responsible for the routine management and co-ordination of IG within the Trust.

5.4.2 The Director of IM&T acts as chair of the Information Governance Steering Group (IGSG). The IGSG is responsible for the development and delivery of the Trust IG strategy and its members oversee the day to day management of the individual component parts of the Trust IG framework.

5.4.3 The membership and terms of Reference for IGSG are included at Appendix A.

5.5 Trust Records Manager

5.5.1 The Trust Records Manager is the senior manager responsible for leading the development and implementation of IG policy and procedure and for ensuring the separate work streams that underpin IG work are implemented in a co-ordinated way to achieve IG compliance.
5.7 All Staff

5.7.1 The majority of Trust staff handle information in one form or another. Staff who in the course of their work create, use or otherwise process information have a duty keep up to date with and adhere to relevant legislation, case law and national guidance. The Trust policies and procedures listed in paragraph 4 above will reflect such guidance and compliance with these Trust policies will ensure a high standard of Information Governance compliance within the Trust.

5.7.2 The Trust has a legal obligation to maintain the confidentiality of the personal information it processes and must do so to maintain the trust and confidence of those who use our services. Breaches of confidentiality will be treated as serious disciplinary incidents which in some circumstances can lead to dismissal. All staff should ensure they are aware of the relevant Trust policy in respect of any personal information they may process.

6. INFORMATION GOVERNANCE MANAGEMENT

6.1 Principles

6.1.1 There should be proactive use of information within the organisation, both for patient care and service management as determined by law, statute and best practice.

6.1.2 There should be proactive use of information between the Trust, other NHS and partner organisations to support patient care as determined by law, statute and best practice.

6.1.3 The Trust will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Information Governance Toolkit (IGT).

6.1.4 The Trust will annually assess its performance against the requirements set out for Acute Trusts in the IGT. The Trust will report the results of its self assessment to the Department of Health in accordance with current guidance in the IGT.

6.1.5 The Trust will follow a program of continual improvement to increase IG compliance in the Trust year on year.

6.1.6 Individual members of staff will be provided with the opportunity to attend training and awareness sessions to equip them to meet their individual responsibilities in relation to IG.

6.1.7 Where appropriate the principles of information management and handling outlined in this policy are to be applied to identifiable information about Trust staff as well as service users.
6.1.8 All new developments and changes to policies and procedures will be assessed to identify any impact of information handling and information quality.

6.2 The IG Framework

6.2.1 The Information Governance framework for Health and Social Care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that these standards are clearly defined and met.

6.2.2 The Information Governance Framework for UHSFT is the combination of policies, responsibilities and arrangements for the management of IG described in this document. The IG framework in UHSFT will be reviewed annually by the IGSG as part of the IGT assessment process.

6.2.3 There are a number of separate work steam with individual functions that combined underpin IG in the Trust. These are:

- Data Protection
- Freedom of Information
- Information Security
- Information Quality
- Clinical Records Management
- Corporate Records Management

6.2.4 The Trust leads for these areas of work comprise the core membership of the IGSG and carry out the assessment of compliance for IGT requirements related to their area of expertise

6.3 Openness

6.3.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

6.3.2 Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection and Freedom of Information Acts.

6.3.3 Non-confidential information on the Trust and its services will be available to the public through a variety of means including the procedures established to meet requirements in the Freedom of Information Act 2000. The Trust will follow established procedures to deal with queries from patients and the public and will have clear procedures via the communications department for liaison with the press and broadcasting media.
6.4 IG Accountability and Reporting Structure

6.4.1 Appendix B outlines in a diagram the arrangements for reporting and managing IG in the Trust.

6.4.2 The Trust ISSG has been delegated powers from the Trust Executive Committee on behalf of the Board to oversee and monitor IG in the Trust. ISSG will seek the necessary assurance that the Trust is achieving the required compliance with IG requirements outlined in the IGT. IG will be a standing agenda item at ISSG meetings and a report on IG will be submitted to the Board annually.

6.4.3 The primary responsibilities of the Trust Information Governance Steering Group are:

- To monitor NHS IG policy and procedure and ensure any changes to legislation or national policy are reflected in local IG policy and procedure.
- To complete and submit the assessment of compliance with IG requirements published in the IGT and provide assurance to ISSG that the minimum mandated level of compliance is met.
- To develop and implement a programme of improvement designed to show year on year improvement in IG compliance across the Trust as measured by the IGT assessment.
- To carry out a training needs analysis for IG for all staff groups and work with the Training and Development to ensure the required training is delivered.
- To receive regular reports from IG leads and escalate to ISSG as appropriate items for Board approval and issues that require executive consideration.

6.5 IGT Toolkit Assessment Procedure

6.5.1 Annually in March each year the Trust will complete a self assessment of compliance with the requirements applicable to acute Trusts in the current version of the IGT. The summarised results of this assessment will be made publically available on the IGT and details will be shared with regulators such as CQC and Monitor to assist with their continual assessment of Trust governance and performance.

6.5.2 In year during July and October the Trust will also submit interim self assessments which are only made available to the Department of Health digital policy team.

6.5.3 All assessments are completed by making a formal declaration of the level of compliance assessed for each requirement and identifying and uploading copies of appropriate evidence (documents, policies, meeting minutes etc) to support the level of compliance assessed.

6.5.4 Each requirement in the IGT will be allocated to an IG initiative lead to manage and assess. The appropriate lead will be responsible for assessing compliance in line with the guidance and criteria set for the requirement and maintaining the currency of the evidence supporting
the declared assessment level. A minimum assessment of level 2 compliance is expected in order to demonstrate adequate governance practice and procedure. Where this is not being achieved actions to improve should be identified and implemented.

6.5.5 Prior to each assessment submission the IGSG will review and approve the proposed assessment with a focus placed on those requirements not assessed at the minimum level 2 compliance rating. Where necessary actions to improve compliance will be agreed.

6.5.6 Following IGSG approval a report will be submitted to ISSG summarising the proposed assessment and seeking ISSG approval for the submission.

6.5.7 In addition to the above processes prior to the final submission in March each year the Chair of IGSG (Director of IM&T) will review the evidence submitted in support of each criteria and independently confirm agreement with the assessed level of compliance.

6.5.8 As part of the annual Information Governance Audit the Trust internal audit team will test a sample of evidence submitted as part of the IGT assessment process to provide assurance around this procedure. The annual report to the Trust Board on IG will include a summary of the annual submission of Trust compliance with the IGT requirements.

6.6 Continual Improvement

6.6.1 The Trust IG strategy is to follow a programme of continual improvement to show a year on year increase in IG compliance as measured by the annual assessment against the IG requirements set out in the IGT.

6.6.2 Annually in June the IGSG will agree a work plan for the year identifying the priorities of work and actions required to improve IG compliance in the Trust. The results of the previous years IGT assessment will identify key areas for improvement and will be used in conjunction with audit findings and other sources of information to identify priorities for action.

6.5.1 The annual work plan will be monitored by IGSG and progress against the plan will be reported regularly to ISSG.

6.7 Change Management

6.7.1 The introduction of change can have an adverse impact on the quality, security and confidentiality of the information we handle. At an early stage in the change process sponsors should consider the need to conduct a full Privacy Impact Assessment to assess the impact on IG resulting from a change project.
6.7.2 Guidance for staff in how to undertake an assessment of the impact of proposed changes on IG standards and processes is included at Appendix C.

7 EDUCATION AND DISSEMINATION

7.1 As executive lead for IG the Chief Executive has overall responsibility for the implementation and dissemination of this policy. The routine management and co-ordination of IG in the Trust is the responsibility of the Director of IM&T who will exercise this responsibility through the IGSG.

7.2 The attention of staff will be drawn to this policy during IG training sessions and it will be made available to all staff on the Trust intranet.

8 PROCESS FOR MONITORING COMPLIANCE

8.1 Compliance with this policy will be undertaken as summarised in the table below. Any identified areas of non-adherence or gaps in assurance arising from the monitoring of this policy will result in recommendations and proposals for change to address areas of non-compliance and/or embed learning. Monitoring of these plans will be co-ordinated by the group/committee in the monitoring table below.

<table>
<thead>
<tr>
<th>Element of Policy to be monitored</th>
<th>Lead</th>
<th>Tool/Method</th>
<th>Frequency</th>
<th>Who will undertake</th>
<th>Where results will be reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Information Governance Framework</td>
<td>Trust Records Manager</td>
<td>Review of IG Framework carried out as part of IG Toolkit assessment</td>
<td>Annual</td>
<td>Trust Records Manager</td>
<td>Part of IG toolkit assessment reported to ISSG</td>
</tr>
<tr>
<td>Assurance of annual IG Toolkit self assessment</td>
<td>Director of IM&amp;T</td>
<td>Audit of evidence of sub section of Toolkit requirements</td>
<td>Annual</td>
<td>Internal Audit Team as a part of annual assurance programme</td>
<td>Trust Audit and Assurance Committee</td>
</tr>
<tr>
<td>Level of compliance with IG policies and procedures</td>
<td>Trust Records Manager</td>
<td>Monitoring of IG Incidents Reported by Trust Staff</td>
<td>Bi-annual report to IG Steering Group</td>
<td>Trust Records Manager</td>
<td>IG Steering Group</td>
</tr>
</tbody>
</table>
9 ARRANGEMENTS FOR REVIEW

9.1 This policy will be reviewed every three years and by IGSG as part of the review of IG arrangements carried out to meet IGT requirements.

10 REFERENCES

10.1 Information Governance Toolkit: https://nww.igt.hscic.gov.uk/
Appendix A to Trust Information Governance Policy

INFORMATION GOVERNANCE STEERING GROUP TERMS OF REFERENCE

1. **Purpose of Group**

   1.1. The Information Governance Steering Group (IGSG) is established to:

      1.1.1. Provide policy direction and guidance to the Trust on Information Governance related procedures and issues.
      1.1.2. Prepare the annual submission of the Information Governance Toolkit.
      1.1.3. Develop and implement a strategy to lead and improve standards of Information Governance across the Trust.

2. **Specific Responsibilities and Scope of Group**

   2.1. To develop an IG policy and associated IG strategy and maintain the currency of the policy.
   2.2. To prepare the annual Information Governance Toolkit (IGT) assessment for sign off by the Trust Information Strategy Steering Group (ISSG) on behalf of Trust Board.
   2.3. To develop and lead the Trust’s Information Governance work programme.
   2.4. To review reports and other documentation produced relating to IG.
   2.5. To ensure that the Trust’s approach to data/information handling is communicated to all staff and made available to the public.
   2.6. To coordinate the activities of staff with data protection, confidentiality, information security, data quality, records management and freedom of information responsibilities in their job responsibilities.
   2.7. To provide assurance that the relevant policies and procedures are in place to ensure compliance with the law and guidance in respect of information handling.
   2.8. To ensure that appropriate training is provided to Trust staff as necessary to support their role and obligations in respect of Information Governance.
   2.9. To develop and implement procedures to ensure new or proposed changes to organisational processes or information assets that may impact on Information Governance are identified and assessed.
   2.10. Provide a focal point for the resolution and/or discussion of Information Governance issues.

3. **Membership**

   3.1. The IGSG core membership will comprise:

      - Chair: Director of IM&T
      - Trust Records Manager
      - Trust Information Manager
      - Trust IT Manager
      - FoI/DP Officer
      - IT Security Officer
      - Health Records Centre Operations Manager
      - Pharmacy Rep
• Radiology Rep
• Nursing Rep

3.2. Other individuals may be invited to attend specific meetings to advise on areas of expertise

3.3. Support will be provided by the FOI/DP office.

3.4. The Chair will follow up the repeated non attendance of any group members.

4. **Frequency of Meetings**

4.1. Meetings will be monthly.

5. **Quorum**

5.1. For the group to be a quorum there must be 4 members present including either the Director of IM&T or the Trust Records Manager as Chair.

6. **Accountability**

6.1. The IGSG is accountable to the Trust Board through the Information Strategy Steering Group (ISSG).

7. **Reporting**

7.1. Information governance will be a standing agenda item at meetings of ISSG.
7.2. The annual submission of the IG toolkit will be approved by ISSG before submission.
7.3. IGSG will provide regular reports to ISSG on the progress with the agreed IG work plan during the year.
7.4. IGSG will provide ISSG with a draft IG annual report for ISSG to approve and submit to Trust Board.

8. **Review**

8.1. The group will review these terms of reference annually in May of each year.
Appendix B to Trust IG Policy – UHSFT Information Governance Reporting and Accountability Arrangements

Trust Board
- Trust Executive Committee
  - Director of Transformation (SIRO)
  - Information Strategy Steering Group (ISSG)
    - Director of IM&T
    - Information Governance Steering Group (IGSG)
    - Information Asset Owners
      - Information Governance Steering Group (IGSG)
      - Information Asset Owners

Records Manager
- Clinical Records Manager
  - IT Manager
    - IT Security Officer
      - Data Quality and Secondary Use
    - Clinical records
      - Corporate Records and Freedom of Information
  - IT Security
    - Registration authority
      - Data Quality and Secondary Use
  - Data Protection and Confidentiality
  - IG Management
    - Clinical records
      - Corporate Records and Freedom of Information
    - Clinical Records Manager
      - Records Manager
        - Quality Governance Steering Group
          - Caldicott Guardian
            - Trust Board
              - Trust Executive Committee
                - Director of Transformation (SIRO)
      - Information Governance Steering Group (IGSG)
        - IT Manager
          - IT Security Officer
            - Data Quality and Secondary Use
          - Clinical Records Manager
            - Records Manager
              - Quality Governance Steering Group
                - Caldicott Guardian
                  - Trust Board
                    - Trust Executive Committee
                      - Director of Transformation (SIRO)

Disclaimer: It is your responsibility to check against Staffnet that this printout is the most recent issue of this document.
Appendix C to Trust Information Governance Policy

UHSFT Guide to Conducting a Privacy Impact Assessment

Introduction

1. All organisations experience change in one form or another. Where a proposed change involves any form of information processing or storage it is important that our change procedures include an assessment of the potential impact on the confidentiality, security and accessibility of that information. This is formally called a Privacy Impact Assessment (PIA).

2. Before putting new processes in place, project and system sponsors should carry out a simple PIA as set out in this guidance. This will identify if there is a potential impact which will require more detailed analysis to be undertaken.

3. Confirmation that this aspect of change has been considered will be sought as part of the approval process for new business cases and systems.

Business Case Approval

4. Business cases submitted to TEC and Trust Board include a requirement to answer the following statement:

   *This matter has been assessed for potential impact on personal data and privacy: Yes/No*

5. Before answering YES to this statement sponsors of Business Cases should consider whether any changes proposed impact on any aspect of privacy, confidentiality or information security. They should consider the points outlined in appendix C1 to this policy and if there is a potential impact on our ability to comply fully with current legislation or guidance they should seek advice from the appropriate Trust Information Governance lead. (See appendix C2 for contact details of leads)

6. Any risks identified as a result of the review will need to be dealt with in accordance with the procedure outlined in the Trust Risk management strategy. If appropriate the IG lead will raise the issue with the Information Governance Steering Group (IGSG) for consideration.

New System Approval

7. The introduction of new data handling or storage systems requires the approval of the Trust Information Strategy Steering Group (ISSG).

8. The ISSG System development proforma, used to outline any proposal for new system developments or purchase, includes sections on Data Protection, Confidentiality and Security. The information included in these sections will identify any potential impact on privacy and confidentiality and these will be addressed as part of the ISSG approval process.
9. The introduction of new information assets or major changes to existing assets will be managed using the PRINCE (PRojects In a Controlled Environment) methodology.

Other Changes to Systems and Processes

10. In a bid to improve efficiency, reduce costs and update our technology we continually change and improve the way we work. Even minor changes to the way we process information can impact on our ability to keep information safe and secure, and comply with current legislation and best practice.

11. Technical changes and upgrades to core information systems will be subject to formal change control procedures managed by IM&T. For other changes and developments the points outlined at appendix 1 provide a reasonable checklist to assess if there may be an adverse impact on data protection confidentiality or information security as a result of any change. It should be used before introducing any change in process and any issues arising from this outline review should be resolved before proceeding with any change.

Conclusion

12. Changes introduced to the way we handle information can adversely impact on data protection, information security and confidentiality. In order to ensure we remain compliant with current legislation and guidance sponsors of new processes and systems and staff introducing changes to processes and systems should consider the impact of the changes they are proposing.

13. Appendix 1 provides a checklist of things that should be considered in relation to data protection confidentiality and information security. If the checklist indicates there may be a potential adverse impact arising from the change the matter should be raised in the first instance with the appropriate Information Governance specialist. If necessary the issue will be considered by the Trust IGSG.

14. This guidance document will be reviewed annually by the IGSG.
Appendix C1 to Trust Information Governance Policy

Conducting an Initial Privacy Impact Assessment

Answer the following questions in relation to the new system or process being introduced or the change being proposed. If the answer to one or more questions is YES there is a possibility that the Trust may breach its duties to comply with current legislation and guidance for information handling and protecting privacy. In these circumstances before proceeding with any change further advice should be sought from one of the specialist staff identified at appendix 2.

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does this proposal change the way we handle personal information or introduce any new ways of handling or processing personal information?</td>
<td></td>
</tr>
<tr>
<td>2. Does this proposal involve third party organisations accessing or processing personal information held by the Trust? i.e. other providers of healthcare, system suppliers, education and research institutions.</td>
<td></td>
</tr>
<tr>
<td>3. Does this proposal involve the export of personal data held by the Trust outside the UK, or provide access to personal data held by the Trust to organisations outside UK?</td>
<td></td>
</tr>
<tr>
<td>4. Does this proposal involve personal information collected by the Trust for direct healthcare purposes being processed for any other purpose? i.e. research, marketing, billing, administrative support.</td>
<td></td>
</tr>
<tr>
<td>5. The Trust has a duty to protect personal information it holds from unlawful or unauthorised access and from accidental loss, destruction or damage. Does this proposal introduce any new risks that could have an adverse impact on our ability to discharge this duty?</td>
<td></td>
</tr>
<tr>
<td>6. Does the proposal in any way reduce the quality of information we collect or our ability to validate it?</td>
<td></td>
</tr>
</tbody>
</table>

Notes

1. Personal Information: Information which can be used to identify a living person or facts about them, including opinions and intentions towards them.
2. Processing: Obtaining, recording or holding information or data, or carrying out any operation or set of operations on the information or data including disclosure.
Appendix C2 to Trust Information Governance Policy

Contact Details for Information Governance Specialist Staff

If the initial PIA raises some issues that cannot be effectively resolved by the project/change sponsor then advice should be sought in the first instance from one of the staff listed below appropriate to the issue(s) identified.

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Job Title</th>
<th>Tel Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records Management and IG</td>
<td>Trust records manager</td>
<td>SGH x4743</td>
</tr>
<tr>
<td>Information Quality</td>
<td>Trust information manager</td>
<td>SGH x6728</td>
</tr>
<tr>
<td>Information Security</td>
<td>IT security officer</td>
<td>SGH x5713</td>
</tr>
<tr>
<td>Data Protection and Confidentiality</td>
<td>Data protection officer</td>
<td>SGH x5079</td>
</tr>
<tr>
<td>Health Records</td>
<td>Health Records Operational Manager</td>
<td>(023) 8074 8014</td>
</tr>
</tbody>
</table>