Executive Summary
The purpose of this Report is to outline the progress made towards addressing the key issues relating to Information Governance (IG) within the Trust for the period 1 April 2016 to 31 March 2017.

Improving IG is a key NHS priority. This is reflected in national standards set out in the IG Toolkit which the Trusts is required to complete and submit three times a year, specifically in March 2017 for this reporting period.

The Trust Information Governance Department has undertaken a programme of work covering a number of activities in order to provide assurance against the IG Toolkit requirements. This report summarises the outcomes of the key work programme over the period. This report provides a summary and overview from observations from the Interim Head of Information Governance & Security.

Recommendation to the Board
The Board of Directors is requested to:

- This report is presented for the Board’s information and RATIFICATION. It has previously been received and approved by the Audit & Risk Committee.
**Risk Implications**
Potential risks as identified by information governance processes and documented in the IG Toolkit submission.

**Finance Implications**
Potential costs to implement work as identified by information governance assessment and processes.

**Equality and Diversity Impact / Single Equalities Impact Assessment**
N/A
1. Introduction
The purpose of this Report is to outline the progress made towards addressing the key issues relating to Information Governance (IG) within the Trust for the period 1 April 2016 to 31 March 2017.

Improving Information Governance is a key NHS priority. This is reflected in national standards set out in the Information Governance Toolkit which the Trusts is required to complete and submit three times a year, specifically in March 2017 for this reporting period.

The Trust Information Governance Department has undertaken a programme of work covering a number of activities in order to provide assurance against the Information Governance Toolkit requirements.

This report summarises the outcomes of the key work programme over the period. This report provides a summary and overview from observations from the Interim Information Governance Manager.

2. Key Trust Roles & Reporting Structure over the Period
Key Trust Roles - Definition

- **Senior Information Risk Officer (SIRO)**
  **Director of Nursing**
  The SIRO is the Executive Board member who is familiar with information risks and provides the focus for the management of information risk at Board level. S/he must provide the Chief Executive with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted for by the organisation.

- **Caldicott Guardian**
  **Head of Psychology**
  The Caldicott Guardian is the senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

Support to the above 2 roles at the Trust over the period came from:

- **Head of Governance and Quality Assurance** – is responsible for overseeing the management of the Information Governance department, agenda and the Information Governance Framework, and to ensure the Trust’s Information Governance Strategy is developed and implemented.

- **Information Governance Manager** - is responsible for managing the information governance team, implementing the Information Governance Framework, Freedom of information requests and the Trust’s Information Governance Strategy

- **Information Governance Officer** – dealing with Access to Health Records Requests
**Reporting Structure for Information Governance**

The Information Governance Committee oversaw the work of the Information Governance team and progress towards the Trust’s Information Governance strategic objectives. Updates and relevant reporting documentation including relevant policy approvals go to the Risk and Audit Committee.

3. **IG Toolkit: 1 April 2016 to 31 March 2017 – Version 14**

The IG Toolkit is the online system which allows NHS organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations’ IG Toolkit assessments.

There are 45 separate requirements in the IG Toolkit relevant to a Mental Health Trust. The Toolkit is split into six different sets of requirements:

- Information Governance Management;
- Confidentiality and Data Protection Assurance;
- Information Security Assurance;
- Clinical Information Assurance;
- Secondary Use Assurance;
- Corporate Information Assurance.

To reach an overall ‘satisfactory’ assurance level, each of the 45 requirements must, according to the Toolkit, attain level 2. Each individual requirement is split into four attainment levels. The criteria for the specifics on each assessment level vary, but as an example:

0 – Nothing applicable is in place.

1 – Policies or relevant documentation in place.

2 – Implementation work with evidenced documentation.

3 – Monitoring/reviewing/auditing of progress with evidenced documentation.

The objective is for the Trust to provide appropriate evidence to justify the assessment level scored. In some cases evidence is straightforward (for example, an approved Policy), in others less so, for example, the appropriate evidence may be contained in papers and/or minutes of Trust meetings concerning progress etc.

The Trust achieved an overall score of 96%, ‘satisfactory’ for the Version 14 submission of the IG Toolkit in March 2017. This was a 5% increase over version 13 2015/16 score. This increase was attributed to an increased evidence base for requirements of the IG toolkit that have been approved by the IG Committee and stronger engagement from all areas of the Trust with regards to Information Governance.

The Trust achieved 96.4% compliance in regards to the Information Governance training for 2016-17 and along with adjustments to the self-assessment attainment level, this resulted in the ‘satisfactory’ score for the IG Toolkit.
The below tables show the achieved levels of the IG Toolkit by requirement for the most recent financial year and previous year:

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Stage</th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Not Relevant Total Req'ts</th>
<th>Overall Score</th>
<th>Self-assessed Grade</th>
<th>Reviewed Grade</th>
<th>Reason for Change of Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 14 (2016-2017)</td>
<td>Published</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>39</td>
<td>1</td>
<td>45</td>
<td>96%</td>
<td>Satisfactory</td>
<td>n/a</td>
</tr>
<tr>
<td>Version 13 (2015-2016)</td>
<td>Published</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>33</td>
<td>1</td>
<td>45</td>
<td>91%</td>
<td>Satisfactory</td>
<td>n/a</td>
</tr>
</tbody>
</table>

The Trust achieved level 3 on 39 requirements across the various six areas on which the IG toolkit is structured: Information Governance Management, Confidentiality & Data Protection Assurance, Information Security Assurance. Clinical Information Assurance, Secondary Use Assurance and Corporate Information Assurance, Policies and Framework, access to personal data, Freedom of Information procedures, confidential information access monitoring, information security risk, registration authority and smartcards.

When analysing the attainment levels in comparison to previous years (i.e. Version 12), it is of note that in version 14, the Trust improved on the number of level 3 requirements due to an increased evidence base, more structured way of completing the toolkit requirements. This year the Trust did not receive a KPMG review of the IG toolkit instead KPMG undertook a cyber-security review which demonstrated the need for a more robust information asset system. Something the Committee and team have started work on.

4. **Information Governance Training 1 April 2016 - 31 March 2017**

   In line with requirement 142 – 2a of the Information Governance Toolkit;

   ‘All staff, including new starters, locum, temporary, student and contract staff members have completed on at least one occasion, mandated IG training using the NHS IG Training Tool or equivalent formally agreed Department of Health plans or Department of Health approved materials’

   For the 2016/17 year the organisation achieved 96.4% compliance in regards to Information Governance training.

   This area is important for Trust staff to ensure that key responsibilities around Information Governance are understood.

   This has been developed over the reporting period by:
• New staff being briefed on Information Governance requirements and responsibilities as part of their induction.
• Advice and guidance given to staff via emails, meetings and the use of Information Governance related documentation.
• The IG Toolkit requirement – Trust staff were required to go through the Information Governance training awareness module.
• Development of the use of the Intranet and the staff weekly bulletin to disseminate relevant information.
• Provision of Information Governance related training and guidance material.
• Use and advice on policy issues – for example, appropriate use of e-mail.
• Control and advice on setting up and using generic e-mail accounts.

5. Information Governance/Security Related Policies – Keeping Up to Date

Keeping Trust documentation up to date and relevant in terms of the Information Governance/Information Security is critical for ensuring and maintaining an appropriate level of Information Governance. Writing new and updating existing related policies have therefore been a key requirement over this period. Approved (either new or updated) policies undertaken over the reporting period were:
• **Data Protection Policy**
• **Information Governance Policy**
• **Information Governance Management Framework**
• **Freedom of Information Policy**
• **Information Risk Policy**

These policies were reviewed and updated where applicable on a regular basis and approved by the Trust’s Information Governance Committee. The policies have been placed on the Trust’s Intranet for easy access and also were disseminated to staff via Associate Directors.

6. Freedom of Information (FOI) Requests

The Freedom of Information Act provides a general right of access to recorded information held by any public authority as defined within the Freedom of Information Act 2000. Anyone can make a request for information – there are no restrictions on the requesters’ nationality or where they live.

Under the Freedom of Information Act 2000, the Trust must respond to all written requests for information within 20 working days. Failure to comply with this deadline could lead to a complaint by the specific requestor to the Information Commissioners Office (ICO). The ICO has the power to serve a Decision Notice on the public authority for failing to comply with the 20 working day deadline.

Over the last two years the Trust has managed to considerably improve its performance in terms of responding to FOI requests within the required 20 working day deadline.
The total number of FOI requests received by the Trust during the period 1 April 2016 – 31 March 2017 was 217. Over this period the FOI requests came in from a wide variety of sources. These included commercial organisations (for example, employment agencies, ICT companies, medical suppliers), the media (for example, broadcasting companies and the local and national press), Members of Parliament and direct from individuals.

In the interest of openness and transparency and in conjunction with the launch of the Trust’s new website, work has re-commenced on the FOI Disclosure log.

Section 50 Decision Notices 2016/17

Under section 50 of the Freedom of Information Act 2000, the ICO has the power to issue section 50 Decision Notices on a public authority after a requestor has made a complaint to the ICO about the manner in which a public authority has handled its FOI request.

There were 0 Decision Notices served on the Trust during the 2016/17 financial year.

7. Access to Health Records Requests

The main legislative measures that give rights of access to health records include:

- **The Data Protection Act 1998** - rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual’s behalf (for example, a solicitor)
- **The Access to Health Records Act 1990** - rights of access to deceased patient health records by specified persons
- **The Medical Reports Act 1988** - right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes.

Under the Data Protection Act the Trust must give individuals the right of access to their personal information. An individual can send a subject access request requiring the personal information held by the Trust, and to provide them with a copy of that information. The Trust has 40 calendar days to respond to a valid access to health records request.
### Subject Access Requests:

<table>
<thead>
<tr>
<th>Breakdown by Type</th>
<th>2015/16</th>
<th>2016/17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Council</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>NHS</td>
<td>19</td>
<td>14</td>
</tr>
<tr>
<td>Police</td>
<td>35</td>
<td>55</td>
</tr>
<tr>
<td>Solicitors</td>
<td>114</td>
<td>109</td>
</tr>
<tr>
<td>Service User</td>
<td>71</td>
<td>86</td>
</tr>
<tr>
<td>Voluntary sector</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Other legal organisation (such as the citizens advice)</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>259</strong></td>
<td><strong>280</strong></td>
</tr>
</tbody>
</table>

The table above outlines the varied sources of Subject Access Requests over the last two reporting periods.

The process of obtaining the requested information can be lengthy and complex. The number of pages relating to a request can be extensive and need to be copied before vetting. From a particular individual request – the Trust Services at which the requested records may be held first need to be identified by the Information Governance Department via RiO or other sources. Requests will then go to various Trust Services for specific requested notes. The notes are then be located at the service or requested from Iron Mountain (Records Management Storage) if historical. A senior clinician/manager at a particular service then has to vet (redact where necessary) the specific notes, then make copies, before sending them back to the Information Governance Department.

There were some difficulties at times with the requested vetted information not coming back from various Trust Services within the specified timeframes in order to collate all the vetted information before a particular request can be completed.

### 8. Information Governance/Security Breaches

Confidential information is held largely in electronic form in the Trust’s electronic patient records system CareNotes and IAPTus but some information is held in paper records.

All incidents that involve the loss or unauthorised disclosure of personal information are reported centrally and are closely monitored.

An addition to local clinical and corporate incident management and reporting tools (including Strategic Executive Information System – STEIS) a new requirement came in to effect on 1 June 2013 for all organisations processing health and social care personal data, to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRI’s (Information Governance (Serious Incidents Requiring Investigation) to the Department of Health (DH), The Information Commissioners Office (ICO) and other regulators.

During the year (2016/17) there were 84 Information Governance incidents reported via the local reporting tool (Datix). None were reportable to the Information Commissioners Office (ICO) via the IG Incident Reporting Tool and were managed following local protocol. In reviewing the types of breaches which had occurred, they were in the main associated to human error and adherence to local procedures.
The below table shows the number of reported Information Governance and Security Breaches for the previous financial years:

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>2015/16</th>
<th>2016/17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach of Confidentiality</td>
<td>35</td>
<td>54</td>
</tr>
<tr>
<td>Theft of I.T. equipment</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Information Security – Near Miss</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Loss of Information (e.g. records, memory sticks, laptops, diary)</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Mislaid Information</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Unauthorised Access to Information</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Network Security Breach</td>
<td>No category</td>
<td>0</td>
</tr>
<tr>
<td>Smartcard - Loss or Theft of Smartcard</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Inappropriate Internet Access</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Unauthorised Access to IT equipment</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Theft of Information</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Unauthorised Use of Information</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>73</strong></td>
<td><strong>84</strong></td>
</tr>
</tbody>
</table>

Appendix 1 outlines more information about the above Information Governance/Security breaches. The ‘Datix’ Incident Reporting system – run by the Trust Clinical Governance Department was used to capture the information including what action was taken where appropriate.

The number of Information Governance/Security breaches has increased from the last reporting year. Further analysis suggests that this is representative of increased reporting across all categories in the Trust. Camden & Islington Foundation Trust has continued to raise awareness of the Incident reporting system and encouraging more staff to report incidents to ensure future risks can be mitigated and lessons learnt can be put into place. The information governance team continue to issue guidance, provide equipment and training to prevent reoccurrences in order to improve information governance and information security compliance.

**Information Commissioners Office Notification**

During the reporting period, no incidents were reported to the Information Commissioners Office, via the NHS Digital IG SIRI Incident Reporting Toolkit.

9. **Cyber Security**

Work was progressed over the period to evaluate and improve information governance and security processes. These include expanding on and reviewing key documentation including the key areas of information risk assessments for key systems in the Trust as well as a new Information Risk Policy and Information Asset Register.
A cyber-attack is an incident designed to maliciously affect Trust information assets, systems and infrastructure, usually for financial gain. At present the Trust doesn’t have the ability to detect cyber-attacks such as denial of service, phishing emails or any malicious internal damage.

During the recent cyber-attack on the 12th May the Trust wasn’t affected mainly because of limited connectivity to neighbouring organisations. However precautionary measures were taken to reduce the risk of infection including ensuring that the Trust antivirus and Microsoft security patches were updated across Trust ICT desktops and laptops. Prior to the attack it was highlighted that the Trust's antivirus solution wasn't properly maintained due to lack of resources, and was approaching end of support. As a result a business case was in progress at the time of the attack to address these concerns by putting the antivirus under a managed contract.

The Trust also receives weekly bulletin messages from NHS Digital's CareCERT team which offers advice and guidance to help health and social care organisations to respond effectively and safely to cyber security threats. A process is currently being reviewed by ICT and Information Governance to ensure these bulletins are reviewed and acted on where required.

It is also essential to ensure continued investment in ICT infrastructure and support from manufacturers to ensure the Trust can protect itself from any future cyber threats.

10. **Caldicott**

The Caldicott Guardian role is a mandatory role for all NHS organisations introduced by the Department of Health. The role is responsible for patient confidentiality across the organisation and should normally be a senior health professional. The Trust has nominated Dr Jeff Halperin, Head of Psychology who is adequately trained to the required level to occupy the role. The Caldicott Guardian role is well established amongst services and the Caldicott guardian now receives queries directly as a pose to through the IG office.

The role has been important and contributed heavily in the development of CareNotes and has continued to deal with patient confidentiality queries in conjunction with the Trust’s IG Manager. Over the period April 2016 – March 2017 the number of queries received under Caldicott have been 46. Each query is complex and interpretation of NHS guidance, as well as legislative and ethical requirements are important to ensure patient safety and confidentiality.

11. **Development Plans for Next Year**

   a. **IG Toolkit** – The Trust has a dynamic action plan to refresh and improve its compliance with the IG toolkit standards. The new version of the toolkit has been not released however IG is engaging more with IT to incorporate into the work plan for the year.

   b. **Information Governance Committee** – The group now meets every two months, appendix 2 ToR.

   c. **Information Asset Register** - Work with Information Asset Owners (IAO) to embed effective information risk management activities across the Trust embedding these responsibilities in day to day activities

   d. **Working with the NHS networks** to ensure the Trust is able to adopt The General Data Protection Regulation and incorporate new working practices which would include, reviewing consent procedures, updating the Trust’s fair processing notice, nominating a Data Protection Officer and familiarising staff with new terminology.
12. Conclusion
The Trust has a robust process for managing Information Governance and the associated responsibilities that come with our commitment to adopt best practice processes and procedures in order to protect patient and service user information. In summary, much has been achieved in the last year, which is supported by the ‘Satisfactory’ rating in the IG toolkit assessment. However, some objectives in the toolkit are harder to achieve and evidence can be improved upon and for this reason they are being currently worked on to achieve a much higher scoring for the next version of the toolkit.

There has been substantial progress in the comprehensiveness, rigour and quality of the Trusts IG arrangements during 2016/17. This can be illustrated in the increased number of incidents where they are being reported in more detail frequently. Furthermore, the volume of queries and requests made to the team has increased which is a positive indicator.

We are to continue to respond to the challenges faced by changing working practices in order to ensure that we keep pace with the ever-changing information society we work in. Going forward this will only become even more demanding. National developments have a direct impact on the information governance programme such as the General Data Protection Regulation (GDPR) and cyber security of which is currently the main focus at the IG Committee supported by the SIRO and Caldicott Guardian.

13. Recommendations
1. Accept this report as a true reflection of current and future state of Information Governance within the Trust.
2. Support information governance training and early completions throughout the Trust.
3. Support investment in IT security

14. Appendix 1
Table of Information Governance/Security Breaches

15. Appendix 2
Information Governance Committee ToR (Approved)