Information Security and Access Control Policy

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASSIFICATION:</td>
<td>IT</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>To provide a balance between security and ease of use by providing a comprehensive and consistent approach to the security management of information across the Trust in line with the Department of Health Information Security Management: NHS Code of Practice (April 2007)</td>
</tr>
</tbody>
</table>

Controlled Document Number: 168

Version Number: 2.2

Controlled Document Sponsor: Executive Medical Director

Controlled Document Lead: Lead Security and Test Manager

Approved By: Chief Executive

On: 01 September 2014

Review Date: 01 September 2017

Distribution:
- Essential Reading for: All staff
- Information for: All staff
## Contents

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>15</td>
</tr>
</tbody>
</table>

**Appendices**

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>User Responsibilities</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Monitoring Matrix</td>
</tr>
</tbody>
</table>
1. **Policy Statement**

1.1 The purpose of this Information Security and Access Control Policy and its associated documents is to ensure an overall information security management framework; to protect, to a consistently high standard, all Trust information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

1.2 This policy provides a comprehensive and consistent approach to the security management of information across the Trust. It will ensure continuous business capability, and minimise both the likelihood of occurrence and the impacts of any information security incidents.

1.3 All users of Trust IT systems must abide by the rules set out in this Information Security and Access Control Policy and associated documents. Users will be held personally responsible for failure to comply with the policy and may be subject to disciplinary action.

1.4 The objectives of this Policy are to preserve:

1.4.1 **Confidentiality** - Access to data is confined to those who have legitimate authority to view it.

1.4.2 **Integrity** – Data is timely and accurate and detected or amended only by those specifically authorised to do so.

1.4.3 **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

1.5 The Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Trust, who may be held personally accountable for any breaches of information security; failure to comply could result in the individual or the Trust being prosecuted. The Trust shall comply with the legislation, detailed in the Information Security and Access Control Policy, and other legislation as appropriate.

2. **Scope**

This policy applies to all areas and activities of the Trust, including system accounts, and to all individual users employed by the Trust including contractors, volunteers, students, locum and agency staff, staff employed on honorary contracts, non-executive directors and any other individual or organisation granted access to Trust systems (all of the above referred to in this policy as “staff”). This policy applies to all information held on
electronic assets, including Trust information in transit and activities carried out on mobile devices.

3. Framework

3.1 This policy sets out the broad framework for Information Security within the Trust. Detailed instructions are provided in associated policy and procedural documentation, as specified in section 7.

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

3.3 This policy sets out the high level framework for Information Security within the Trust. Specific aspects of Information Security are dealt with in more detail in the following operational procedures:

- **Access Control** - Secure access to network services and systems provided by IT.
- **Email and Internet** - Proper use of the Trust’s Email and Internet system determining what the Trust deems as acceptable and unacceptable use.
- **IT Equipment Disposal** – Secure disposal of IT Equipment capable of storing information.
- **IT Procurement** - Procurement of IT equipment, in line with Trust policies, national policies, legislation and IT Strategy.
- **Mobile Devices** – Use of all mobile devices capable of storing information.

3.4 In conjunction with Information Governance and Caldicott principles, the aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust, by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and associated policies and procedures.
- Introducing a consistent approach to Information Security, ensuring that all members of staff fully understand their own responsibilities.
• Describing the principles of Information Security and explaining how they shall be implemented in the Trust.

• Creating and maintaining within the Trust a level of awareness of the need for Information Security as an integral part of the day to day business.

• Protecting information assets under the control of the Trust, to include any hosted on external applications.

• Ensuring staff do not remove information from the Trust unless approved to do so.

3.5 Information Security Awareness and Training

• Information security awareness training is included in the staff induction process.

• An on-going awareness programme is established and maintained in order to ensure that staff awareness is refreshed and updated as necessary through the Information Governance annual mandatory training requirement.

• Training is provided at face to face sessions, such as induction and mandatory training days.

3.6 Contracts of Employment

Staff security requirements are addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. Information security expectations of staff are included within appropriate job definitions.

3.7 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) and Information Asset Administrator (IAA) who shall be responsible for the information security of that asset. Corporate Affairs maintain a copy of the asset register.

3.8 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.
3.9 **User Access Controls**

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

3.10 **Computer Access Control**

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

3.11 **Application Access Control**

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

3.12 **Equipment Security**

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. This will be achieved by the effective use of suitable security measures i.e. physical controls within buildings, entry systems and secure storage facilities to protect assets from theft/damage.

3.13 **Computer and Network**

3.13.1 Management of computers shall be controlled through standard documented procedures that have been authorised by the Trust. IT schedules back-ups on business critical network files to enable recovery. Trust equipment must not be used for private work, commercial activities, advertising or fundraising if not directly connected with the Trust, unless it has had formal Trust approval. Provision of the network is contracted via a Commercial Third Party (CTP), who must abide by the nationally defined NHS N3 code of connection procedures. The CTP is required to meet the terms and conditions of the IG Assurance Statement and the obligations of the IG Toolkit which requires the CTP to obtain, and maintain, a “Satisfactory” annual self-assessment, of the IG Toolkit, which includes:

- Confidentiality and Data Protection Assurance
- Information Governance Management
- Information Security Assurance
3.13.2 The CTP must agree with the terms and conditions set out in the Information Governance Statement of Compliance (IG SoC), as required by all non-NHS CTP’s, in order to preserve the integrity of systems, and safeguard services and information for all.

3.14 Information Risk Assessment

3.14.1 The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

3.14.2 Once identified, information security risks shall be managed on a formal basis, by their IAO, in line with Risk Management Strategy and Policy. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Trust’s risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

3.15 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported with the IT Service Desk, by logging a call via the IT Service Portal, for the attention of the Lead Security and Test Manager. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events. Incidents and near misses will be reported in line with the Trust’s Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy & Procedure.

3.16 Protection from Malicious Software

The Trust shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the Trust’s property without permission from the Trust; any such requirements should be raised with the IT Service Desk, by logging a call via the IT Service Portal. Users breaching this requirement may be subject to disciplinary action.
3.17 **User Media**

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Trust before they may be used on Trust systems. Read-only access to removable media is permitted, provided such media is fully virus checked before being used on the Trust’s equipment. Users breaching this requirement may be subject to disciplinary action.

3.18 **Monitoring System Access and Use**

3.18.1 An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis; in so far as is practicably possible, subject to technical limitations.

3.18.2 The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees’ electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

3.18.3 Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.
3.19 **Accreditation of Information Systems**

3.19.1 The Trust shall ensure that all new information systems, applications and networks include an approved security plan before they commence operation.

3.19.2 IAOs are responsible for carrying out risk assessment and System Level Security Policies (SLSPs) for systems under their control; in order to distinguish between the security management considerations and requirements in this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system.

3.20 **System Change Control**

Changes to information systems, applications or networks shall be reviewed and approved by the Trust. IT changes are subject to the completion and approval of the “Request for Change” form; change requests are reviewed at the Change Advisory Board (CAB).

3.21 **Intellectual Property Rights**

The Trust shall ensure that all information products are properly licensed and approved by the Trust. Users shall not install software on the Trust’s property without permission from the Trust. Users breaching this requirement may be subject to disciplinary action.

3.22 **Business Continuity and Disaster Recover Plans**

The Trust shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

3.23 **Equipment Disposal**

3.23.1 NHS and third party systems which deal with Person Identifiable Data, confidential or sensitive information (PID) will be disposed of in line with national requirements, to prevent unauthorised disclosure.

3.23.2 All redundant equipment must be disposed of in line with:

- Health and Social Care Information Centre (HSCIC) Disposal and Destruction of Sensitive Data
- The Information Commissioner’s Office (ICO) IT asset disposal for organisations
• The Waste Electronic and Electrical Equipment Directive (WEEE)

3.23.3 The Trust currently outsources the disposal of such equipment to a Commercial Third Party (CTP), who provides disposal in line with these requirements. This process is audited as part of IT’s audit schedule.

3.24 Reporting

The Lead Security and Test Manager shall report the information security status of the Trust at the Information Governance Group (IGG).

3.25 Audit

This procedure shall be subject to the Trust’s internal audit process.

3.26 Further Information

Further information and advice on this policy can be obtained from the Lead Security and Test Manager.

4. Duties

4.1 Director of IT Services

The Director of IT has been delegated with responsibility for information security on behalf of the Chief Executive. The day to day activities required to effectively implement and maintain this policy will be performed through the Lead Security and Test Manager.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is accountable for fostering a culture for protecting and using data, providing a focal point for managing information risks and incidents and is concerned with the management of all information assets. The Director of Corporate Affairs is the Trust’s SIRO.

4.3 Caldicott Guardian

The Caldicott Guardian has a strategic role in ensuring that there is an integrated approach to information governance, developing security and confidentiality policy and representing confidentiality requirements and issues at Board level. The Trust’s Executive Medical Director is the Caldicott Guardian.
4.4 **Lead Security and Test Manager**

The Trust's Lead Security and Test Manager will be supported by the IT Security and Compliance Manager and is responsible for the implementation and enforcement of the Information Security and Access Control Policy.

Responsibilities include:

- Ensuring that policies, procedures and working practices align themselves to this Information Security and Access Control Policy.
- Monitoring and reporting on the status of IT security within the Trust.
- Ensuring compliance with relevant legislation and regulation.
- Providing advice and guidance to staff so they are aware of their responsibilities and accountability within information security.
- Monitoring for potential security breaches.
- Working closely with those responsible for, Data Protection, patient confidentiality and other Information Governance work areas.
- Providing direct input to the information security components of the IG Toolkit.

4.5 **Senior Manager Information Governance**

4.5.1 The Senior Information Governance Manager is responsible for promoting a culture of good information governance within the Trust and developing and maintaining policies, procedures and protocols in compliance with this policy and strategy and in accordance with good practice.

4.5.2 In addition there exists an Information Governance Group which comprises the Trust’s Senior Information Governance Manager and the Information Security Manager. Through this group, common approaches are agreed to aspects of Information Governance and Security, where appropriate.

4.6 **System Managers**

4.6.1 An Information Asset Owner (IAO) will be designated for each information system within the Trust. The Trust’s IAO’s role is to
understand and address risks to the information assets they 'own'; and provide assurance to the SIRO on the security and use of these assets.

4.6.2 The Information Asset Administrator (IAA) will be responsible for the day to day management of that system, including a system specific Information System Level Security Policy, Information Asset Registration and Risk Assessment. The IAA will ensure compliance with the Information Security and Access Control Policy and associated procedures and will make sure breaches are reported to their IAO, the responsible line manager and in line with Trust incident reporting.

4.7 **Managers**

Anyone who has a responsibility for staff must ensure that:

- They are kept appraised of all information security and governance guidance.
- All members of staff are aware of their security responsibilities.
- All members of staff have appropriate training for the systems they are using.
- Appropriate levels of access are granted to specific individuals (e.g. Registration Authority role for staff who issue smartcards).
- Ensure that all staff sign confidentiality agreements as part of their contract of employment.
- Ensure that IT, RA and system managers are informed of staff role changes, new starters and leavers.
- The security of physical environments where information is processed or stored.

4.8 **Staff**

All staff must:

- Comply with the Information Security and Access Control Policy and associated policies, procedures and best practice.
- Report information security incidents in accordance with Trust incident reporting procedures.
• Sign a general statement of confidentiality on commencement of employment.

4.9 Contractors

In addition to the responsibilities for individual staff, as detailed above, any contractor must obtain authorisation for use of their laptop, or alternative mobile device, on Trust premises. This should be obtained through the Trust’s manager they are reporting to, who will co-ordinate the request with IT. Any requirement to store Trust’s data on a contractor’s mobile device must have been specifically authorised by the Trust’s manager, and where appropriate, if Person Identifiable Data, confidential or sensitive information (PID) is stored then Information Governance approval is also required; with the contractor’s mobile device needing to be encrypted to the Department of Health (DH) approved level, this can be verified with IT.

5. Implementation and Monitoring

5.1 Implementation

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

5.1.2 Information Security training is included in the mandatory annual Information Governance Training Tool (IGTT), along with additional recommended modules.

5.2 Monitoring

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

6. References

The Trust’s Information Security arrangements take into account statutory requirements and good practice, including:

Access to Health Records Act 1990

Broadcasting Act 1990

Caldicott Principles (Revised, to include 7th principle, 2013)

Care Quality Commission

Common Law Duty of Confidentiality

Page 13 of 18
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Criminal Justice and Public Order Act 1994
Data Protection Act/ Processing of Sensitive Personal Data Order 1998/2000
Freedom of Information Act 2000
Health and Safety at Work Act 1974
Health and Social Care Act 2012
HSCIC Information Governance Toolkit
Human Rights Act 1998
Information Technology Infrastructure Library (ITIL)
Interception Of Communications Code of Practice 2010
N3 Code of Connection
NHS Code for Records Management 2006
NHS Code of Practice 2006
Police and Criminal Evidence Act 1984
Reporting, Managing and Investigating IG Serious Incidents Requiring Investigation (SIRI) 2013
Telecommunications Act 1984
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Trade Mark Act 1994
Waste Electronic and Electrical Equipment Directive (WEEE)
7. **Associated Policy and Procedural Documentation**

Access Control Procedure

Assessment of Risks and Management of Risk Registers Procedure

Business Continuity Plan and Procedural Documents

Corporate Records Procedure

Data Protection and Confidentiality Policy

Data Quality Policy

Disciplinary Policy & Procedure

E-Mail and Internet Access Procedure

Flexible Working Policy

Freedom of Information Act and Environmental Regulations Policy & FOI procedure

IT Acceptable Use Policy

Information Governance Policy

Record Management and Information Lifecycle Policy

Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy & Procedure

Risk Management Strategy and Policy
Users Key Responsibilities

1. Users Key Responsibilities

1.1 The purpose of this appendix is to summarise the key user responsibility requirements as laid out in the following key documents:

- Access control Procedure
- Data Protection and Confidentiality Policy
- Flexible Working Policy
- Information Governance Policy
- Information Security and Access Control Policy
- Internet and E-Mail Access Procedure
- Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy & Procedure

1.2 These documents support the Trust’s overall Information Security and Access Control Policy which sets out guidelines within the framework of the Department of Health (DH) Information Security Management: NHS Code of Practice (April 2007). It is your manager’s responsibility to ensure that you are aware of those policies which are relevant to your role within the Trust.

1.3 The purpose being to preserve:

- **Confidentiality** – Access to data is confined to those who have legitimate authority to view it.

- **Integrity** – Data is timely and accurate and detected or amended only by those specifically authorised to do so.

- **Availability** – Data is available to those authorised when it is needed

By following the guidelines in this statement users can minimise risks in relation to information security. Non-compliance may result in disciplinary action being taken in accordance with the Trust's disciplinary policy, and may lead, in very serious cases to dismissal, for gross misconduct; as detailed in the Trust’s Disciplinary Policy, a copy of which is available via the policies and procedures link from the UHB home page.
2. **Safeguarding Data – IT Essentials**

- Use your own password, ensure that it is kept secret at all times and never use somebody else’s.

- Do not leave computers open for unauthorised access, ensure either logged out or locked (Ctrl+Alt+Delete) when unattended.

- Do not use the internet inappropriately; just because a site isn’t blocked doesn’t mean that it is approved.

- Save all data to appropriately restricted UHB network drives, not to your hard drive (i.e. C:\), as network data is secure and backed up.

- Only share Person Identifiable Data, confidential or sensitive information (PID) with those who are authorised to see it.

- Any PID leaving the Trust must first be approved and encrypted.

- Do not hold PID on portable media (including laptops) unless it is encrypted. Please contact the IT department for further guidance.

- Ensure that portable media (including laptops) are backed up regularly to a network drive and that they are logged onto the network regularly to receive antivirus and other major updates.

- All mobile devices, capable of storing information, should be encrypted.

- Do not load unofficial software onto Trust computers or portable media devices (including laptops).
<table>
<thead>
<tr>
<th>MONITORING OF IMPLEMENTATION</th>
<th>MONITORING LEAD</th>
<th>REPORTED TO PERSON/GROUP</th>
<th>MONITORING PROCESS</th>
<th>MONITORING FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaches in policy and incidents will be identified and reported. Initially logged as a call with the IT Service Desk, via the IT Service Portal, for evaluation and, where appropriate, an Incident being raised in line with Trust process. This policy, along with associated documents, shall be subject to the Trust’s internal audit process.</td>
<td>Investigating officer will report breaches and incidents to the Lead Security and Test Manager</td>
<td>Breaches will be reported to the Information Governance Group</td>
<td>Monitoring will be undertaken using the annually completed, self-assessed, Information Governance Toolkit, which is signed off by the Information Governance Group and the Board of Directors.</td>
<td>Low level breaches and incidents will be reviewed at Trust’s quarterly Information Governance Group; Serious incidents will also follow this process and are additionally included in the Trust’s Statement of Internal Control and annual report, in line with HSCIC SIRI guidance.</td>
</tr>
</tbody>
</table>