## 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 digital information across the Trust in line with the Department of Health Information Security Management NHS Code of Practice (April 2007)</td>
</tr>
<tr>
<td>Controlled Document Number:</td>
<td>168</td>
</tr>
<tr>
<td>Version Number:</td>
<td>003</td>
</tr>
<tr>
<td>Controlled Document Sponsor:</td>
<td>Executive Medical Director</td>
</tr>
<tr>
<td>Controlled Document Lead:</td>
<td>Lead Security and Test Manager</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Chief Executive</td>
</tr>
<tr>
<td>On:</td>
<td>April 2018</td>
</tr>
<tr>
<td>Review Date:</td>
<td>April 2021</td>
</tr>
<tr>
<td>Distribution:</td>
<td></td>
</tr>
<tr>
<td>- Essential Reading for:</td>
<td>All staff</td>
</tr>
<tr>
<td>- Information for:</td>
<td>All staff</td>
</tr>
</tbody>
</table>
Contents

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Policy Statement</td>
<td>3</td>
</tr>
<tr>
<td>2 Scope</td>
<td>3</td>
</tr>
<tr>
<td>3 Framework</td>
<td>4</td>
</tr>
<tr>
<td>4 Duties</td>
<td>12</td>
</tr>
<tr>
<td>5 Implementation and Monitoring</td>
<td>16</td>
</tr>
<tr>
<td>6 References</td>
<td>17</td>
</tr>
<tr>
<td>7 Associated Policy and Procedural Documentation</td>
<td>18</td>
</tr>
</tbody>
</table>

Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Monitoring Matrix</td>
<td>20</td>
</tr>
<tr>
<td>B User Responsibilities</td>
<td>22</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 University Hospitals Birmingham NHS Foundation Trust (the Trust) has an overall digital information security management framework; to protect, to a consistently high standard, all Trust digital 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. The Record Management and Information Lifecycle Policy applies to all Trust information held in paper format.

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 Through the Information Governance Group, which comprises the Trust’s SIRO, Senior Information Governance Manager and the Information Security Manager, common approaches are agreed to aspects of Information Governance and Security, where appropriate.

3.4 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 Controlled Documents:

3.4.1 Access Control Procedure - Secure access to network services and systems provided by IT.

3.4.2 IT Acceptable Use Policy – Acceptable practices and responsibilities expected of staff with access to computers and moveable devices (e.g. laptops, phones, etc.).

3.4.3 Procurement Policy and Procedure - Appropriate supplier checks and relevant contractual clauses for third party suppliers who will have access to the Trust network, information systems or data.

3.4.4 Policy and procedure for the management of medical devices - Data security questions as part of the pre-acquisition questionnaire for third Party medical devices

3.4.5 Digital Equipment Disposal Procedure *

3.4.6 Mobile Devices – Defines the use of all mobile devices capable of storing information.
3.4.7 Removable Media Procedure – Defines the use of all removable media capable of storing information.

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

3.5.1 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, through auditing monitoring and reporting.

3.5.2 Introducing a consistent approach to Information Security, ensuring that all members of staff fully understand their own responsibilities.

3.5.3 Describing the principles of Information Security and explaining how they shall be implemented in the Trust.

3.5.4 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.

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

3.5.6 Ensuring staff do not remove information from the Trust unless approved to do so in consultation with Information Governance.

3.6 Information Security Awareness and Training

3.6.1 Information security awareness is included in the mandatory training, the Communications Plan and the key user responsibility document (Appendix B) which is issued to all new IT account holders.

3.6.2 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.

3.6.3 Training is provided at face to face sessions and as e-learning, such as induction and mandatory training days.
3.7 **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.

3.8 **Security Control of Assets**

3.8.1 Each IT asset, (hardware, software, application or data; internally or externally supplied) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset. IAO’s can be assisted by one or more Information Asset Administrators (IAA). Information Governance maintains a copy of the asset register.

3.8.2 The flow of data between an IAO’s assets and any internal or external systems or parties shall be included in the asset register.

3.8.3 Assets shall be classified in terms of business value and criticality.

3.8.4 Agreements with suppliers shall include requirements to address information security risks.

3.8.5 Maintenance and repair of organisational assets shall be performed and logged in a timely manner, with approved and controlled tools.

3.9 **Access Controls**

Only authorised personnel who have a justified and approved business need shall be given access to restricted services, or areas containing information systems or stored data. Exceptional access privileges will only be given with approval from a member of the endorsed Approvers Group.

3.10 **User Access Controls**

Access to information shall be restricted to authorised users who have a legitimate business need to access the information and in accordance with the principle of least privilege.
3.11 **Computer Access Control**

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

3.12 **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.

3.13 **Digital 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.

3.14 **Computer and Network**

3.14.1 Management of computers shall be controlled through standard documented procedures that have been authorised by the Trust.

3.14.2 IT schedules back-ups on business critical databases and network files to enable recovery. Off-line, network disconnected copies shall be kept in addition to network accessible copies.

3.14.3 Trust digital 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.

3.14.4 Provision of the network is contracted via a Commercial Third Party (CTP), who must abide by the nationally defined NHS HSCN Connection Agreement/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.

3.14.5 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.

3.14.6 Network integrity shall be protected through employing segregation and cryptographic techniques where appropriate.

3.15 Remote Access (Teleworking Policy)

3.15.1 Remote access to Trust network and systems shall be through software and services provided by the Trust which requires additional user authentication. Staff and third party suppliers using remote access facilities shall do so from private locations and using secure network connections.

3.15.2 Third party support access will be provided by IT Services, via accounts providing the least privilege necessary to perform the required duties for the shortest amount of time.

3.15.3 Staff shall ensure that computers used for remote access are using up to date malicious software (“malware”) protection. Any personally identifiable data (PID) or Trust intellectual property accessed from remote locations shall not be stored locally.

3.15.4 Staff will ensure that family and friends do not have access to trust services and systems at the remote location and protect against eaves-dropping when using mobile devices in public places.

3.16 Information Risk Assessment

3.16.1 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.

3.16.2 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.

3.16.3 The NHS Digital good practice guides, National Cyber Security Centre (NCSC) 10 steps to Cyber Security, NCSC Cyber Essentials assurance framework and ISO 27001 Information Security Management Standard will be considered when risk assessing information security risks.

3.17 Information Security Events and Weaknesses

3.17.1 All information security events and suspected weaknesses are to be reported to the IT Service Desk, by logging a call via the Service Portal at QEHB, 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. External event reporting will be in agreement between Information Governance and Information Technology departments.

3.17.2 The primary goal of handling an information security incident shall be to resume the normal security level, followed by the necessary recovery and corrective actions. Information security threat and vulnerability information is to be received and actively sought from a variety of authoritative and special interest information sharing sources.

3.17.3 Serious events that require forensic investigation will do so in accordance with the NHS Digital Forensic Readiness Good Practice Guide.

3.17.4 Reporting must happen as soon as the event is discovered.

3.17.5 Software and hardware shall be maintained through its lifetime with the implementation of updates and alterations ("patches").

3.18 Protection from Malware

The Trust shall use software countermeasures and management procedures to protect itself against the threat of malware. 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 must be raised with the IT Service Desk, by logging
a call via the Service Portal at QEHB. Users breaching this requirement may be subject to disciplinary action. The Trust shall undertake scans for vulnerabilities from malware.

3.19 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external digital 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. Further details are available in the Removable Media Procedure. Users breaching this requirement may be subject to disciplinary action.

3.20 Monitoring System Access and Use

3.20.1 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. The scope and retention of audit trail data shall be sufficient to support retrospective analysis of individuals’ activities.

3.20.2 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.

3.20.3 Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

3.21 Accreditation of Information Systems

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

3.21.2 IAOs are responsible for carrying out Privacy Impact Assessments, annual risk assessments and maintaining 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.

3.22 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 Group (CAG). System developments shall follow a defined life-cycle.

3.23 Intellectual Property Rights

The Trust shall ensure that all digital information products are properly licensed and approved by the Trust. The Trust will take appropriate steps to protect its intellectual property rights to any locally developed systems and will protect that right accordingly.

3.24 Business Continuity and Disaster Recover Plans

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

3.25 Digital Equipment Disposal

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

- NHS Digital 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)

3.25.3 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 and is detailed in the Digital Equipment Disposal and Disposal Procedure.

3.26 Reporting

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

3.27 Audit

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

3.28 Further Information

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

4. Duties

4.1 Members of the Information Governance Group (IGG)

The Information Governance Group (IGG) comprises the Trust’s SIRO, Senior Information Governance Manager/Head of Information Governance, the Information Security Manager, divisional representatives, as well as representatives from Informatics, Medical Records and Therapies. Through this group, the Board is advised of common approaches to Information Governance/Security and assured of Trust practices. The Information Security Advisory Group and several Task & Finish Groups report into IGG.
4.2 Members of the Information Security Access Group (ISAG)

A combination of Information Governance and IT Security personnel meet to ensure a coherent approach is undertaken when information governance and IT Security matters overlap. ISAG reports to the Information Governance Group. Responsibilities for ISAG include, but are not limited to the following:

4.2.1 Discussing solutions to any incidents which have both Information Governance and IT Security concerns;
4.2.2 Reviewing and consulting on privacy impact assessments;
4.2.3 Monitoring the Trust’s compliance and performance against the Data Security Standards;
4.2.4 Discussing current threats and drafting a Trust wide strategy;
4.2.5 Reviewing the third party due diligence submissions; and
4.2.6 Monitoring IG/IT security audits (Internal and external).

4.3 Director of IT Services

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

4.4 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 and their regulatory and legal requirements, including privacy and civil liberty obligations. The SIRO is responsible for determining the approval processes for enhanced privileges or exceptional access rights. The Director of Corporate Affairs is the Trust’s SIRO.

4.5 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.
4.6 **Lead Security and Test Manager**

The 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:

4.6.1 Ensuring that policies, procedures and working practices align themselves to this Information Security and Access Control Policy;

4.6.2 Monitoring and reporting on the status of IT security within the Trust;

4.6.3 Ensuring compliance with relevant legislation and regulation;

4.6.4 Providing advice and guidance to staff so they are aware of their responsibilities and accountability within information security;

4.6.5 Monitoring for potential security breaches;

4.6.6 Working closely with those responsible for, Data Protection, confidentiality of data subjects and other Information Governance work areas;

4.6.7 Providing direct input to the information security components of the IG Toolkit; and

4.6.8 Continuous review and improvement of protection processes along with the outward sharing of these improvements with others.

4.7 **Senior Manager/Head of Information Governance**

The Senior Manager/Head of Information Governance 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.

4.8 **Head of Technical Operations and Infrastructure (IT)**

4.8.1 The system owner responsible for:

a) Maintaining a baseline configuration of, and tested recovery processes for infrastructure systems (email,
network, authentication services, data storage and backup processes, desktop computers and remote access);

b) Malware vulnerability detection scanning systems;

c) Infrastructure capacity planning.

4.9 **Head of Service Delivery (IT)**

The Head of Service Delivery (IT) is the system owner responsible for the timely administration of user access control credentials for new, changed and removed accounts.

4.10 **Trust Security Management Specialist**

The Trust Security Management Specialist is responsible for maintaining a physically secure environment and premises which contain sensitive and critical information processing facilities.

4.11 **Managers**

Anyone who has a responsibility for staff must ensure that:

4.11.1 They are kept appraised of all information security and governance guidance;

4.11.2 All members of staff are aware of their security responsibilities;

4.11.3 All staff have read this policy, including the users key responsibilities detailed in Appendix B;

4.11.4 All members of staff have appropriate training for the systems they are using;

4.11.5 Appropriate levels of access are granted to specific individuals (e.g. Registration Authority (RA) role for staff who issue smartcards));

4.11.6 Ensure that all staff sign confidentiality agreements as part of their contract of employment;

4.11.7 Ensure that IT, RA and system managers are informed of staff role changes, new starters and leavers; and

4.11.8 The security of physical environments where information is processed or stored.
4.12 Staff

All staff must:

4.12.1 Comply with this Policy and associated policies, procedures and best practice;

4.12.2 Report information security incidents in accordance with Trust incident reporting procedures; and

4.12.3 Must comply with the confidentiality obligations detailed in their contract of employment; and

4.12.4 Be aware of their responsibilities as key users as detailed in Appendix B.

4.13 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 must be obtained through the Trust’s managers 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 PID, confidential or sensitive information 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 A 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

Caldicott Principles (from the Caldicott Committee Report 1997 and the Caldicott Review 2013

Care Quality Commission

Common Law Duty of Confidentiality

Computer Misuse Act 1990

Copyright, Designs and Patents Act 1988

Data Protection Act 1998 and its subsequent Act as amended by the GDPR

Department of Health: Confidentiality Code of Practice 2003

Department of Health: Information Security Code of Practice

Department of Health: Records Management Code of Practice

Department of Health NHS Information Governance Guidance on Legal and Professional Obligations 2007

Freedom of Information Act 2000

General Data Protection Regulation (GDPR) 2016

Guidance for Classification Marking of NHS Information

HSCN Connection Agreement

Human Rights Act 1998


Interception of Communications Code of Practice 2016


Network and Information System Directive (NIS) 2016
NHS Digital A guide to confidentiality in health and social care 2013

NHS Digital Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation

NHS Digital Code of practice on confidential information 2014
NHS Digital Forensic Readiness Good Practice Guide

NHS Digital Information Governance Toolkit

Police and Criminal Evidence Act 1984


Reporting, Managing and Investigating IG Serious Incidents Requiring Investigation (SIRI) 2015

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 Procedures

Business Continuity Plan

Corporate Records and Archiving Procedure

Data Protection and Confidentiality Policy

Data Quality Policy

Disciplinary Policy & Procedure

Emergency Preparedness Policy

Flexible Working Policy

Freedom of Information ACT and Environmental Regulations Policy & FOI Procedure

Information Asset Procedure
Information Governance Policy

IT Acceptable Use Policy

Digital Equipment Disposal Procedure *

Procurement Policy and Procedure*

Record Management and Information Lifecycle Policy

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

Risk Management Strategy and Policy Procedure
## Monitoring Matrix

<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>An audit trail of system access and data use by staff.</td>
<td>IT Security Lead</td>
<td>Information Security Access Group</td>
<td>E.g. reports on high volume data transfers).</td>
<td>By exception</td>
</tr>
<tr>
<td>Trend analysis on system access.</td>
<td>IT Security Lead</td>
<td>Information Security Access Group</td>
<td>E.g. persistent offenders; regular password requestors, etc.</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Completion of mandatory Information Security training.</td>
<td>Senior Manager/Head of Information Governance</td>
<td>Information Governance Group</td>
<td>All staff will receive security training as part of their induction and at annual intervals. The training will include an assessment of their understanding.</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Review of enhanced privileged access assignment to digital Information Assets.</td>
<td>IT Security Lead</td>
<td>Information Security Access Group</td>
<td>Review of staff who have been granted privileged access.</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Spot checks on continued use of privileged access to digital Information Procedure.</td>
<td>IT Security Compliance Manager</td>
<td>Information Security Access Group</td>
<td>Spot check of continued use of privileged access.</td>
<td>Quarterly</td>
</tr>
</tbody>
</table>

---

Information Security and Access Control Policy  
Issue Date: 25.04.2018  
Controlled Document Number: 168  
Version: 003  

* Documents to be drafted  
* Procedure to be incorporated into the Trust Procurement Procedure
| Reports on lost or stolen mobile devices. | IT Security Lead | Information Governance Group | As and when reported. | Quarterly |
| Reports on redundant mobile devices usage. | IT Security Lead | Information Governance Group | Periods since last use. | Quarterly |
| Monitoring of network activity. | IT Security Lead | Information Governance Group | Establishing inappropriate access to the network by use of Trust monitoring software. | Quarterly |
Appendix B

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:

- IT Acceptable Use Policy
- Access Control Procedures
- Data Protection and Confidentiality Policy
- Information Governance Policy
- Information Security and Access Control Policy
- 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** – Information shall be available and delivered to the right person, at the time when it is needed

1.4 By following this policy, 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 (PID), confidential or sensitive information 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 mobile devices) unless it is encrypted. Please contact the IT department for further guidance.
- Ensure that portable media (including mobile devices) 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).