1 Introduction

The effective and efficient use of computerised data processing is a vital part of the operation of the Trust. This policy sets out to clarify how computer facilities should be operated to ensure data is secure and to identify prohibited actions which could put the security of data in jeopardy or adversely affect the integrity of the Trust or which would be in breach of national legislation.

2 Scope

2.1 Authorised Trust staff will be given access to portable computer systems and equipment to facilitate the execution of their duties. This policy defines the terms and conditions under which systems and equipment must be used and gives notice of improper or prohibited uses of portable computer systems and data.

2.2 For the purposes of this document portable computers are defined as Laptop and Notebook computers, and digital storage devices such as PDAs (Personal Digital Assistants), Palmtops, USB memory sticks Writable CDs and Advanced Mobile Phones.

2.3 Only authorised staff shall have access to portable computers and systems provided by the Trust. This policy applies to all Trust staff and contractors.

2.5 All Trust staff must abide by the conditions of this policy.

3 Aims

This details the technical requirements for protecting electronic data in transit and the staff responsibilities for securing the devices holding the data.

4 Duties (Roles and responsibilities)

4.1 Staff shall be familiar with all Trust policies covering data processing and shall not perform any action in breach of those policies that could render the Trust liable at law nor shall any member of staff process or use data in breach of Trust policies in such a way as to bring the Trust into disrepute.
4.2 The software and information held on portable computer systems is subject to the same audit procedures as all other Trust systems. This also applies to data stored on removable data media.

4.3 Users should also be familiar with the Trust IT Security Policy and Access Control Policy

5 Definitions

PDA is a personal digital assistant. Smartphones are personal mobile telephones with the capacity to hold data and connect to the internet, iPhone, Blackberry or Android.

6 Specific policy

6.1 Authorised Trust staff will be given access to portable computer systems and equipment (e.g. Laptop and Notebook computers, PDAs, Palmtops, Advanced Mobile Phones) if required to facilitate the execution of their duties.

6.2 Only legally acquired software and licensed programs must be used and staff may not install any software products without authorisation. All software and data files are the property of the Trust and the approved Anti-Virus software package must be installed and updated regularly.

6.3 Portable data storage media shall not be used to carry personal identifiable information outside Trust premises without Caldicott Guardian approval and must be password protected and encrypted. Disposal of any portable media should comply with the Trust disposal procedure.

6.4 The security of portable computing devices is the individual’s responsibility at all times and must be locked securely away when unattended in any public place. When using a vehicle, staff must lock equipment in the luggage compartment and remove it if the vehicle is to be left unattended.

6.5 Back-ups must be made to the Trust network on a regular basis. Incidents that constitute a loss of hardware or data should be reported through the Trust Incident Reporting Procedure and to the IT Helpdesk.

6.6 The Trust will maintain a register of devices and will use software to manage the type of data transferred between Trust systems and portable devices.

6.7 Software and programs used on any Trust system or computer shall be legally acquired and in the case of licensed software, each copy shall be licensed and the Trust will adhere to the relevant licensing agreement.
6.8 Staff may not install any software products onto Trust computers nor connect any device to Trust computers or networks without authorisation from the IT Helpdesk.

6.9 Software and data files created by staff on Trust equipment are the property of the Trust.

7 **Authorised Usage**

7.1 Staff will be issued with system access passwords, in line with the Trust [Network Security and Access Control Policy](#).

7.2 Portable data storage media such as CDs, diskettes or tapes shall not be used to carry personal identifiable information outside Trust premises without authorisation from the Caldicott Guardian and data files so authorised must be encrypted.

7.3 The Trust uses Pointsec protector as the standard device encryption tool for portable data media. Portable data storage media; USB memory sticks, pda’s, advanced mobile phones, digital music players that are connected to the Trust network will be registered on initial connection.

7.4 After registration the software will monitor any data transferred between the Trust network and the device.

7.5 Data held on a personal device will be accessible without encryption however if any data is subsequently copied from the Trust network into that device then enforced encryption of the whole device will take place.

7.6 Any data transferred from Trust systems to either a USB memory stick or writable CD should be automatically encrypted. Users will be prompted to select a decrypt key of their own choosing. If the data is then accessed from a Trust device the data will be decrypted automatically. If the data is accessed from a non Trust device the encryption key will be required before data can be accessed. Users are responsible for ensuring that the device has been encrypted in line with this policy. Help and guidance is available through the IT Service desk Ext 21000

7.7 Data transferred from the Trust via a portable media device to a non Trust PC will be autoencrypted if the data remains on the PC when the portable data device is removed.

7.8 Certain file types will not be transferrable between Trust PC and storage device. These would include executable files, software and program files, music and video files.

8 **Laptops**

8.1 Portable computer equipment may only be used outside Trust premises with appropriate authorisation and must be protected at all times against loss or theft.
The security of portable computing devices is the individual’s responsibility at all times, and staff should check their home and car insurance policies.

8.2 Trust laptops will have their hard drives fully encrypted. It is the responsibility of staff to ensure that the laptop they are using is fully encrypted in line with this policy. Any laptop not encrypted should be reported to the IT service desk and must not be taken off Trust premises until encryption is complete.

8.3 Encryption will be automatic and will run as a background process when the laptop is attached to the Trust Network.

8.4 The hard drive itself will be encrypted so any data transferred to the drive after the encryption process will be protected.

8.5 Portable equipment that is carried in a vehicle should be locked in the luggage compartment and must be removed if the vehicle is to be left unattended.

8.6 The Portable Computer must be placed in a securely locked location when not in use.

8.7 Staff should not leave the Portable Computer unattended in any public place.

8.8 Staff should not leave the Strong Authentication token in the same location as the Portable Computer.

8.9 Staff should not keep password details in the same location as the Portable Computer.

8.10 Portable data storage devices should be kept secure at all times.

8.11 Faulty portable data storage devices should not be returned to the manufacturer or supplier for repair without having all data removed or destroyed.

8.12 Lost or stolen equipment must be reported immediately via the Trust Incident Reporting Procedure and to the IT Helpdesk.

9 User Accountability

9.1 Only equipment supplied or authorized by the Trust should be used to process or store identifiable personal information for Trust business.

9.2 The Trust does not automatically sanction the use of personal mobile devices. Users who do use personal devices, PDA’s, smartphones, etc. must ensure that Trust data transferred to those devices is fully protected in line with this policy. Any patient identifiable data held on these devices must be encrypted to the recommended 256 bit standard. It is the responsibility of the user to ensure the appropriate level of security and access control is in place.
9.3 Staff may not access personal information from Trust files for non business use, to do so would be viewed as a serious breach of privilege incurring disciplinary action which may include dismissal.

9.4 Staff are bound by the Trust Information Security Policy and by the common law duty of confidentiality concerning the information that they use as part of their work for the Trust.

9.5 Backup of the system software and configuration must be made on a regular basis. The portable computer should be connected to the local network and booted from the user domain on the local server as regularly as possible (at least weekly), to maintain the currency of operating systems and virus protection software.

9.6 Disposal or maintenance of portable computer equipment that may hold personal identifiable information must be referred to the IT Helpdesk.

9.7 Staff may not use Trust portable computers or systems to access or attempt to access any systems or networks that they are not authorised to use or are not permissible for Trust business use. Such unauthorized attempts or access will be viewed as serious breach and will result in disciplinary action which may include dismissal.

9.8 Portable computers supplied by the Trust for use on Trust business outside Trust premises may only be connected to NHSnet at a location for which NHSIA code of connection approval exists. Portable computers must not be connected to the Internet through a non NHS Internet Service Provider. Remote access via Dial up to the NUTH network will be possible where permission has been granted.

9.9 **Staff are responsible for ensuring that any portable storage device taken off site is fully encrypted in line with this policy.**

9.10 Staff must comply with the Trust Email and Internet policies.

**10 System and data integrity**

10.1 Staff must not introduce computer viruses or related malignant code into Trust information systems. To do so deliberately will incur disciplinary action that may include summary dismissal and prosecution. The Trust will install virus protection software and will make staff aware of procedures designed to minimise the risk of infection. Disregard of procedure resulting in virus infection of Trust systems will be considered a serious breach of Trust policy.

10.2 The Portable Computer Systems must have an Anti-Virus software package installed. Users are not to alter the configuration of this package. The anti-virus system’s database of virus definitions must be updated on a regular basis, each day if possible, but at least weekly.
10.3 All serious virus infections which have not been automatically eradicated by the system’s antivirus software must be reported to the IT Helpdesk who will in turn report the incident to the NHS Information Authority.

11 Disciplinary process

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

12 Training

It is the responsibility of all staff to complete the annual mandatory information governance training.

13 Equality and diversity

The Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds. This document has been appropriately assessed.

14 Monitoring Compliance

<table>
<thead>
<tr>
<th>Standard / process / issue</th>
<th>Monitoring and audit</th>
<th>Method</th>
<th>By</th>
<th>Committee</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portable devices</td>
<td>Devices attached to the Trust network will have technical policies enforced through the Trust device management system. Devices that have the security standards either removed or altered will generate a management report at the time of next connection and will be blocked from access until investigated.</td>
<td>IT Security Team.</td>
<td>Indigo Committee</td>
<td>Continuous process.</td>
<td></td>
</tr>
</tbody>
</table>

IT Security will use audit tools to regularly monitor device usage and encryption compliance. Suspected breaches will be investigated and reported to HR and the Caldicott Guardian.

15 Consultation and Review

The Head of Information Governance & Security with the IT Security lead and IT manager produced this policy which was reviewed and agreed by the Trust Indigo committee.

The Director of IT, in conjunction with the Director of HR are responsible for the review and amendment of this policy.
16 Implementation (including raising awareness)

Technical changes to Trust infrastructure which may impact on this policy will be implemented through the technical change control process and staff will be advised through IT service management communications.

17 References

- Caldicott Code of Conduct on Confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Freedom of Information Act 2000
- NHS Code of Confidentiality.

18 Associated documentation

- Clinical Records Management Policy
- Disciplinary Policy / Procedure
- Freedom of Information Act Procedure
- Information Security Policy
- Non-Health related Records and Documents Retention Schedules
This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

### PART 1

1. **Assessment Date:** _18/10/17_________________

2. **Name of policy / guidance/ strategy / service development / Investment plan/Board Paper:**
   - Laptop and Portable Computing and Data Storage Policy

3. **Name and designation of author:**
   - Richard Oliver Head of IG

4. **Names & Designations of those involved in the impact analysis screening process:**

5. **Is this a:**
   - Policy [x]  
   - Strategy [ ]  
   - Service [ ]  
   - Board Paper [ ]

   **Is this:**
   - New [ ]  
   - Revised [x]  

   **Who is affected:**
   - Employees [x]  
   - Service Users [ ]  
   - Wider Community [ ]

6. **What are the main aims, objectives of the document you are reviewing and what are the intended outcomes?**
   *(These can be cut and pasted from your policy)*

   Outlines standards for securing Trust electronic data.
7. Does this policy, strategy, or service have any equality implications? Yes ☐ No X

If No, state reasons and the information used to make this decision, please refer to paragraph 2.3 of the Equality Analysis Guidance before providing reasons:

Cannot find Equality Analysis Guidance on Intranet but this policy outlines the technical measures in place for securing data on Trust computers.

8. Summary of evidence related to protected characteristics

<table>
<thead>
<tr>
<th>Protected Characteristic</th>
<th>Evidence</th>
<th>Does evidence/engagement highlight areas of direct or indirect discrimination?</th>
<th>Are there any opportunities to advance equality of opportunity or foster good relations? If yes what steps will be taken? (by whom, completion date and review date)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Race / Ethnic origin (including gypsies and travellers)</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on Sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex (male/ female)</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on Sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion and Belief</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on race or belief</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual orientation including lesbian, gay and bisexual people</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on Sexual orientation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability – learning</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panel</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>difficulties, physical disability, sensory impairment and mental health. Consider the needs of carers in this section</td>
<td>on physical disabilities or impairments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender Re-assignment</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on Sex.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marriage and Civil Partnership</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on marital status.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maternity / Pregnancy</td>
<td>This policy relates to the technical securing of data on Trust devices and has no impact on maternity or pregnancy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Are there any gaps in the evidence outlined above? If ‘yes’ how will these be rectified?

   Section 8 is not applicable to this policy. see response in 7

10. Engagement has taken place with people who have protected characteristics and will continue through the Equality Delivery System and the Equality Diversity and Human Rights Group. Please note you may require further engagement in respect of any significant changes to policies, new developments and or changes to service delivery. In such circumstances please contact the Equality and Diversity Lead or the Involvement and Equalities Officer.

   Do you require further engagement  No

11. Could the policy, strategy or service have a negative impact on human rights? (E.g. the right to respect for private and family life, the right to a fair hearing and the right to education?)

   No
PART 2

Name of author:
Richard oliver

Date of completion
16/01/18

(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified, please refer to the Policy Author identified above, together with any suggestions for action required to avoid/reduce the impact.)