The Newcastle upon Tyne Hospitals NHS Foundation Trust

Digital Forensic Evidence Policy

<table>
<thead>
<tr>
<th>Version No.</th>
<th>2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective From</td>
<td>21 March 2019</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>21 March 2022</td>
</tr>
<tr>
<td>Date Ratified</td>
<td>26 February 2019</td>
</tr>
<tr>
<td>Ratified By</td>
<td>Clinical Policy Group</td>
</tr>
</tbody>
</table>

1. Introduction

Forensic readiness is a key component in the management of NHS information risk. In September 2008 a directive from David Nicholson stated that all organisations are required to have Forensic Readiness Policies in place, therefore Information Governance (IG) forensic readiness must be introduced into the business processes and functions of the Trust.

2. Scope

This policy applies to all information systems, networks, applications, locations and people within the ISMS for the following business processes:

- All wards, departments, laboratories and administrations functions.
- All contractors working within the Trust
- All external services where information is stored or maintained

3. Aims

The aim of the forensic readiness policy is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for a formal dispute or legal process. In this context, forensics may include evidence in the form of log files, emails, back up data, removable media, portable computers and network and telephone records amongst others that are routinely collated on a continuous basis.

- This will maximise the Trusts potential to use digital evidence whilst minimising the costs of investigation.
- The NHS directive reflects the high level of importance placed upon minimising the impacts of information security incidents and safeguarding the interests of patients, staff and the Trust itself.
4. Duties – roles and responsibilities

4.1 **Chief Executive/Trust Board** – have ultimate responsibility for the implementation of this policy including ensuring that the Trust policies comply with all legal, statutory and good practice requirements.

4.2 **Senior Information Risk Owner (SIRO)** – The Trusts’ SIRO is responsible for coordinating the development and maintenance of IG forensic policy, procedures and standards and on-going management of the Trusts Risk Management Programme.

4.3 **Information Asset Owners (IAOs)** - in conjunction with Information Asset Administrators (IAAs) will ensure that this Policy is adequately considered and documented for all information assets where they have been assigned ownership and staff are aware of and adhere to this. This requires IAO to look at the adequacy of audit trails and log provision for systems for which they are responsible.

4.4 **IT Service Management** – is responsible for assisting the Information Security Officer in the safeguarding of all Trust data and the management arrangements in respect of the Trusts electronic data processing assets.

4.5 **Information Governance Manager** – Will be responsible for issuing guidance for implementing and compliance with this Policy and ensuring that the training materials around forensic readiness are kept up to date.

4.6 **Information Security Officer** – Will be responsible for issuing guidance for implementing and compliance with the Digital Forensic Policy.

4.7 **All Staff** – are responsible for co-operating with the implementation of this policy as part of their normal duties and responsibilities.

5. General Principles

5.1 This Policy has been created to:

- Protect the Trust, its staff and its patients through the availability of reliable digital evidence gathered from its systems and processes.
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to Trust business.
- Enable the proactive and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required.
- Demonstrate due diligence and good governance of the Trusts information assets.

5.2 This procedure applies to all departments and functions of the Trust and adherence should be included in all contracts for outsourced or shared services.
5.3 The types of equipment this policy relates to includes PCs, laptops, external hard drives, portable data devices such as memory sticks and removable media such as DVD, CD etc.

6. Process

6.1 Incident Reported

This policy could be instigated by a number of methods these could include:

- Concern raised by a member of staff to their line manager
- Concern raised by a third party to a member of staff
- Concern raised by a manager
- Following a review of audit reports
- Output to a printer – evidence

Staff should feel comfortable raising a concern and know that information would be treated in confidence. The IAO or line manager would then need to follow the actions as outlined in 6.1

6.1 Preliminary Investigation Stage

6.1.1 Consideration should be given by the IAO or line manager as to the strength of case required before proceeding, (log the incident following the Trust incident reporting procedures), therefore a preliminary business/service impact assessment must be made based on information provided and any other information from any reliable source e.g. (a system report or information from other witnesses) whether any of the following are present:

- Evidence of a reported crime.
- Evidence of internal fraud, theft or other loss. If fraud implications refer to the Trust’s Fraud Policy.
- Estimate of possible damages (a threshold may induce an escalation trigger).
- Potential for embarrassment/reputation loss.
- Any immediate impact on patient, partners or profitability.
- Recovery plans have been enacted or are required.
- The incident is reportable under a compliance regime.

6.1.3 If no criminal, civil or disciplinary evidence is suspected or evident following the preliminary enquiry then the support of AuditOne would not normally be required. The initial enquiry is not necessarily restricted to criminal issues; a disciplinary incident would potentially require the evidence to be preserved. If no further action (no internal action is required) then update the enquiry into the incident and close the enquiry.

6.2 Securing of the Data

6.2.1 In all cases the equipment must be secured to ensure that the audit trail and evidence is not altered in anyway either by accident or deliberately.
6.2.2 To ensure this, you must contact the IT Service Desk and arrange for them to send an IT Staff member to secure the equipment. Under no circumstances must the original computer data be accessed as any other interaction or data input will alter any evidence. Where equipment is switched off then please follow the following steps:

- Secure the area containing the equipment – (lock the office) or if an open office do not allow the equipment to be switched on.
- Place the equipment in a sealed container which should be sufficient to contain the following items of equipment for transportation to a secure site:-

  Base of the computer
  any paper print out
  External storage (usbstick, external hard drive etc)

6.2.3 Where the computer equipment which is still switched on is to be left until the authorised IT staff member arrives, you must:

- secure the area containing the equipment – (lock the office)
- Move people away from the computer and power supplies
- If attached, disconnect any modem
- If the computer is attached to the network remove the network cable from the data point
- For laptops the lid should not be lifted as this can cause them to power up. The battery should be removed first before anything further is done
- Do no touch the mouse or keyboard
- Do not take advice from other computer owner/users
- Allow any printers to finish printing (further evidence may be printing)
- Place the equipment in a sealed container and transport to a secure site
- Make full and contemporaneous notes of the entire process, including the date and time that the power cable was removed, details of cables connected to the PC, details of what the cables are connected to and details of the device i.e. make, model and serial number
- Ask the user (if present) for any passwords which they use.

6.2.4 If you have to remove equipment before the IT Staff member arrives, the following steps must be performed:

- Record what is on the screen by taking a photograph if possible
- Switch off the computer by pulling the power cable from the computer, not from the power socket (Note: for laptops, remove the battery before pulling the power cable). When removing the power supply always remove the end attached to the computer and not the socket. This will avoid data being written to the hard drive if an uninterruptable power device is fitted) and label with computer ID Tag code and date and
photograph (if possible) all the equipment in situ. If no camera is available draw a sketch plan.

6.3 Analysis of Evidence

6.3.1 Following consideration of the above and with the approval of the SIRO then the AuditOne investigation team may be contacted for advice or to request a review of the equipment and data.

The service desk must:-

- Store the original data and equipment in a secure location in a sealed and signed container
- Provide a replacement computer to the service in line with the services BCP
- Provide the original of the disk to the authorised investigators
- The authorised and trained member of staff within the computer services department must use a write bloc device, no other method can be used as this would compromise the data and is the only way to guarantee that the data on the original device has not been altered during an investigation.

7. Process for Monitoring and Audit

<table>
<thead>
<tr>
<th>Monitoring/audit arrangements</th>
<th>Methodology</th>
<th>Reporting Source</th>
<th>Committee</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit</td>
<td>Review of processes to ensure comply with policy</td>
<td>Internal Auditors</td>
<td>Sub Groups/IG Sub Committee/IM&amp;T Committee</td>
<td>Annually</td>
</tr>
<tr>
<td>External Assessment</td>
<td>Submission against IG Toolkit and CQC standards</td>
<td>IG Team</td>
<td>Sub Groups/IG Sub Committee/IM&amp;T Committee</td>
<td>Annually</td>
</tr>
<tr>
<td>Continuous Assessment</td>
<td>Quarterly reporting/risk assessments for key systems</td>
<td>Information Asset Owners</td>
<td>Sub Groups/IG Sub Committee/IM&amp;T Committee</td>
<td>Quarterly</td>
</tr>
</tbody>
</table>

Section 8: References

Human Rights Act 1998
BS 27001 Information Security
Data Protection Act 2018
Computer Misuse Act 1998
Section 9: Other Relevant Policies

Fraud, Bribery and Corruption Policy and Response Plan
Disciplinary Policy

X

Matt Carney
Head of Information Governance
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:** 14/01/19

2. **Name of policy / guidance/ strategy / service development / Investment plan/Board Paper:**
   - Digital Forensic Evidence Policy

3. **Name and designation of author:**
   - Matt Carney – Head of Information Governance

4. **Names & Designations of those involved in the impact analysis screening process:**
   - Matt Carney - Head of Information Governance, Julia Scott - Governance & Security Officer

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)*
   - DoH mandates that if required Trusts can isolate and investigate IT equipment while maintaining chain of evidence.
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:

The Policy has no equality issues as it outlines the processes and procedures. This policy is aimed at the preservation of equipment and is independent of staff/users.

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 legal requirements for managing personal data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex (male/ female)</td>
<td>This policy relates to the legal requirements for managing personal data regardless of sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion and Belief</td>
<td>This policy relates to the legal requirements for managing personal data regardless of religion.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual orientation including lesbian, gay and bisexual people</td>
<td>This policy relates to the legal requirements for managing personal data regardless of sexual orientation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>This policy relates to the legal requirements for managing personal data regardless of age.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability – learning difficulties, physical disability, sensory impairment and mental health. Consider the needs of carers in this section</td>
<td>This policy relates to the legal requirements for managing personal data regardless of and difficulties or disabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender Re-assignment</td>
<td>This policy relates to the legal requirements for managing personal data and has no impact on any Gender re-assignment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marriage and Civil Partnership</td>
<td>This policy relates to the legal requirements for managing personal data and has no impact on marriage or Civil partnerships.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maternity / Pregnancy</td>
<td>This policy relates to the legal requirements for managing personal data.</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:
Matt Carney

Date of completion
14/01/19

(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.)