Forensic Readiness Policy

DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Version:</th>
<th>0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified By:</td>
<td></td>
</tr>
<tr>
<td>Date Ratified:</td>
<td></td>
</tr>
<tr>
<td>Policy Author:</td>
<td>Essex CSU CCG IG Lead</td>
</tr>
<tr>
<td>Policy Sponsor:</td>
<td>Chief Finance Officer (SIRO)</td>
</tr>
<tr>
<td>Name of Responsible Committee:</td>
<td>Quality and Governance Committee</td>
</tr>
<tr>
<td>Date Issued:</td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td></td>
</tr>
<tr>
<td>Target Audience:</td>
<td>CCG Staff and Members</td>
</tr>
</tbody>
</table>

**Equality Impact Assessment**

This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This Policy is applicable to the Board, every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership, and those who work on behalf of the CCG.
Associated Policy Documents

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Protection and Confidentiality Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>Safe Haven Policy</td>
</tr>
<tr>
<td></td>
<td>Information Sharing Policy</td>
</tr>
<tr>
<td></td>
<td>Information Lifecycle Management Policy and Strategy</td>
</tr>
<tr>
<td></td>
<td>Information Risk Policy</td>
</tr>
</tbody>
</table>

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPO</td>
<td>Association of Chief Police Officers</td>
</tr>
<tr>
<td>CCG</td>
<td>Clinical Commissioning Group</td>
</tr>
<tr>
<td>CMA</td>
<td>Computer Misuse Act</td>
</tr>
<tr>
<td>CSU</td>
<td>Commissioning Support Unit</td>
</tr>
<tr>
<td>IAO</td>
<td>Information Asset Owner</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IGFR</td>
<td>Information Governance Forensic Readiness</td>
</tr>
<tr>
<td>IM &amp; T</td>
<td>Information Management and Technology</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>RAG</td>
<td>Risk Advisory Group</td>
</tr>
<tr>
<td>SIRO</td>
<td>Senior Information Risk Owner</td>
</tr>
<tr>
<td>CONTENTS</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>1  Introduction</td>
<td>5</td>
</tr>
<tr>
<td>2  Policy Objectives</td>
<td>5</td>
</tr>
<tr>
<td>3  Definitions</td>
<td>6</td>
</tr>
<tr>
<td>4  Policy Scope</td>
<td>6</td>
</tr>
<tr>
<td>5  Roles &amp; Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>6  Incident Reporting</td>
<td>9</td>
</tr>
<tr>
<td>7  Forensic Readiness Planning</td>
<td>9</td>
</tr>
<tr>
<td>8  Review and Revision Arrangements</td>
<td>10</td>
</tr>
<tr>
<td>9  Process for Monitoring Compliance &amp; Effectiveness</td>
<td>10</td>
</tr>
</tbody>
</table>

Appendix 1: Forensic Readiness Procedure                                  11

Appendix 2: Computer Investigation - Possessing, Making and Distributing Indecent Images of Children

Policy Ref:
Version: 0.1
Approved
Review date
1. INTRODUCTION

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

This policy provides the framework within which the CCG describes the Forensic Readiness Policy for computer users and sets out the introduction of IG forensic readiness into the business processes and functions of the CCG. The introduction of this policy should maximise the CCG’s potential to use digital evidence whilst minimising the costs of forensic investigation.

This directive reflects the high level of importance placed upon minimising the impacts of information security events and safeguarding the interests of patients, staff and the Trust itself.

The aim of the forensics readiness policy is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required from a formal dispute or legal process. The policy may include evidence in the form of log files, emails, back up data, mobile computing, network, removable media and others that may be collected in advance of an event or dispute occurring.

The CCG acknowledges that IG forensics provides a means to help prevent and manage the impact of important business risks. IG evidence can support a legal defence, it can verify and may show that due care was taken in a particular transaction or process, and may be important for internal disciplinary actions.

2. POLICY OBJECTIVES

This policy sets out the context and process for Forensic Readiness in Castle Point and Rochford CCG.

2.1 Purpose

The purpose of this policy is to ensure that:

- NHS requirements relating to security and confidentiality of equipment and information and the requirements of the Data Protection Act are met.
- 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 CCG business.
• Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required.
• Demonstrate due diligence and good governance of the CCG’s information assets

2.2 Benefits

The benefits to the organisation of creating a forensic readiness policy consist of the following:

• Enterprise defence mechanisms are captured
• Acts as a deterrent to insider threats
• In the event of an incident, this would enable minimum disruption and also link in to the CCG Business Continuity plans.
• Reduced cost and time for internal investigations
• Extends information security to the wider threat from cyber crime
• Demonstrates due diligence and good enterprise governance arrangements
• Compliance with the NHS Information Governance Toolkit and other regulatory requirements.
• Improve the prospects for successful legal action if required
• Supports employee sanctions based on digital evidence.

3. DEFINITIONS

3.1 IG Forensic Readiness

The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisations ability to gather and use digital evidence whilst minimising disruption and/or cost.

3.2 IG Forensic Readiness Planning

Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence, related monitoring and collection processes and capabilities, storage requirements and costs.

4. POLICY SCOPE

This policy applies to all systems and networks used by CCG staff for:

• The transmission of non-clinical data and images
• The transmission of clinical data and images
• Printing or scanning non-clinical or clinical data or images
• The provision of internet systems for receiving, sending and storing non-clinical or clinical data or images

5. ROLES AND RESPONSIBILITIES

5.1 The Accountable Officer

The Accountable Officer will maintain ultimate accountability for the implementation of this policy, although specific responsibility will be delegated to others within the CCG.

The CCG will take all reasonable steps to ensure that staff are aware of policies, protocols, procedures and legal obligations relating to forensic readiness.

5.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of IG forensic policy procedures and standards for the CCG.

The SIRO is responsible for the on-going development and day-to-day management of the IG forensic policy within the CCG’s overall Risk Management Programme.

5.3 Essex CSU Head of Information Governance/Head of ICT

Will be responsible for:

• Issuing guidance for implementing and compliance with the Forensic Readiness Policy.
• Monitoring performance through quality control and internal audits
• Identifying where improvements could be made
• Reporting performance standards to the Information Governance Group.

Defining the business scenarios that may require digital evidence including:

a) Employee internet misuse / abuse
b) Employee Email Misuse / abuse
c) Employee performance issues
d) Electronic bullying / harassment  
e) Formal Police / legal request for digital evidence  
f) Social Networking evidence  
g) Fraud  
h) CCTV  
i) Production of audit logs  
j) Back up data  
k) Removal media  
l) Network intrusion / prevention audit records such as cyber – attacks (hacking attempts etc)  
m) Mobile phone and desk phone investigation  

5.4 Information Asset Owners (IAO)  

CCG information Asset Owners (IAOs) shall ensure that IG forensic readiness planning is adequately considered and documented for all information assets where they have been assigned ‘ownership’. Goals for IG forensic planning include:

- Ability to gather digital evidence without interfering with business processes  
- Prioritising digital evidence gathering to those processes that may significantly impact the Trust, its staff and its patients;  
- Allow investigation to proceed at a cost in proportion to the incident or event;  
- Minimise business disruptions to the Trust.  
- Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action.  

IAOs shall submit their plans for IG forensic readiness, to the SIRO for review along with details of any planning assumptions or external dependencies. Forensic readiness plans shall include specific actions with expected completion dates.

5.5 Heads of Department  

The Heads of Department will support and enable the Heads of to fulfil their responsibilities and ensure the effective implementation of the Information Governance framework.
5.6 **Managers**

Managers are responsible for ensuring that their service operates within the Information Governance framework. They will ensure that:

- There are effective methods for communicating Information Governance related issues within their service.
- Staff complete relevant training, and mandatory updates in relation to Information Governance.
- Staff are aware of and adhere to Information Governance policies.
- Necessary risk assessments are undertaken within their area of responsibility.
- Information Governance issues and risks are discussed in team meetings.

5.7 **All Staff**

Individual staff members will:

- Be aware of and adhere to relevant information governance policies and procedures.
- Complete Information governance training and mandatory updates.
- Assist in identification of information governance issues/breaches and bring them to the attention of the relevant manager.

6. **INCIDENT REPORTING (INCLUDING NEAR MISS)**

Incidents (or near misses) that constitute any actual or potential breach of data confidentiality must be reported directly to the Essex CSU Head of Information Governance immediately. An incident form must be completed and submitted in accordance with the CCGs Incident Reporting procedures.

7. **FORENSIC READINESS PLANNING**

In order to plan for a digital investigation this organisation needs to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. The following steps describe the key activities needed for this process.

- Define the business scenarios that require digital evidence.
- Identify available sources and different types of potential evidence.
- Determine the evidence collection requirement
- Establish a capability for securely gathering legally admissible evidence to meet the requirements
- Establish a policy for secure storage and handling of potential evidence
- Ensure monitoring is targeted to detect and deter major incidents
- Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
- Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
- Document an evidence-based case describing the incident and its impact
- Ensure legal review to facilitate action in response to the incident.

8. REVIEW AND REVISION ARRANGEMENTS

8.1 This document will be subject to review when any of the following occur:

8.1.1 The adoption of the standards highlights errors and omissions in its content

8.1.2 Where other standards/guidance issued by the CCG conflict with the information contained.

8.1.3 Where good practice evolves to the extent that revision would bring about improvement.

8.1.4 2 year elapse after approval of the current version

9. PROCESS FOR MONITORING COMPLIANCE AND EFFECTIVENESS

The Information Governance Steering group will monitor the implementation of this policy, with any supporting procedures, and subsequent revisions.
APPENDIX 1

FORENSIC READINESS PROCEDURE

If you suspect inappropriate usage of computer equipment you should contact your IAO/Line Manager, Essex CSU Information Governance Team. Consideration should be given as to the strength of case required to proceed, therefore a preliminary business impact assessment should be made based on whether any of the following are present:

- Evidence of a reported crime
- Evidence of internal fraud, theft or other loss.
- Estimate of possible damages (a threshold may induce an escalation trigger.)
- Potential for embarrassment/reputation loss.
- Any immediate impact on customers, partners or profitability
- Recovery plans have been enacted or are required.
- The incident is reportable under a compliance regime.
- If fraud is suspected, then contact the Local Counter Fraud Specialist immediately

Following consideration of the above, The Essex CSU Information Governance Team may be contacted for advice or to request an investigation. Where there is a requirement for an investigation to be undertaken you should ensure the following steps are taken:

- If you are able to leave everything as it is until the investigator arrives
- Do not leave equipment unattended
- Make sure it is not accessed by anyone at any time

Where this is not possible the following should be applied.

**Computer equipment which is switched on:**

- Secure the area containing the equipment
- If the user is present, ask them to step away from the computer. Do not allow them to close programs or shut down the machine
- Move people away from the computer and power supplies and do not allow the user or anyone else to touch the machine in any way
- If the computer is directly connected to other computers or equipment (other than via a recognised network data point) then these other machine will need to be dealt in the same manner as outlined in this procedure.
If the computer is attached to the network remove the network cable from the data point.

- Do not touch the mouse or keyboard
- Do not take advice from the computer owner/users
- Allow any printers to finish printing (further evidence may be printing)

**If you have to remove equipment before the investigator arrives, the following steps must be performed:**

- Record what is on the screen and take a photograph if possible (Note: for laptops, be aware that some power up automatically when the lid is lifted – therefore do not open the lid to photograph the screen and keyboard until battery and power cable has been removed).
- Do not attempt to `shut down` the machine or use the power button
- 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).
- Search the surrounding area and locate any memory devices (e.g. CDs, DVDs, USB Memory Sticks) that may be associated with the computer in question. Be aware that such devices can take many forms such as USB memory drives being incorporated into key rings and novelty desk items etc.
- Label and photograph (if possible) all the components in situ. If no camera is available draw a sketch plan
- Label the ports and cables so that the computer can be reconstructed at a later date.
- Carefully remove the equipment and record serial numbers (each component will have a separate number). Also note the identity and serial numbers of any connected devices (e.g. printer, external hard disk or other memory devices)
- Ensure all items have signed and completed exhibit labels attached.
- Search the immediate area for diaries, notebooks or pieces of paper that may contain passwords.
- Consider asking the user if there are any passwords and if these are given record them accurately.
- Make detailed notes of all actions in relation to the seizure of computer equipment
- Remove the equipment to a secure location until the investigator arrives
Upon discovery of computer equipment which is switched off:

- **Do Not switch the computer on.**
- Secure and take control of the area controlling the equipment
- Allow any printers to finish printing (further evidence may be printing).
- Move people away from any computers and power supplies.
- Confirm the computer is actually switched off – some screen savers can give the appearance that some computers are switched off but hard drive and monitor lights may indicate this is switched on.
- Be aware some laptops may power on by opening the lid.
- Remove the battery from laptops
- Unplug the power supply from the computer. A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of data.

**Removable media**

Where removable media i.e. USB pen, external hard-drives etc is found to have been used inappropriately and/or contains inappropriate content you should contact your Line Manager, or Essex CSU Information Governance Team immediately and ensure the device is secured and no longer used until advised otherwise.
Computer Investigation: Possessing, Making and Distributing Indecent Images of Children

Possession of Indecent Photographs / Images of Children

It is important to note that the possession of material depicting indecent images of children is a serious criminal offence. Section 160 of the Criminal Justice Act provides:

It is an offence for a person

- To have any indecent photograph or pseudo photograph of a child in his or her possession

Where a person is charged with an offence under this subsection of the Act, it shall be a defence for them to prove:

- That they had legitimate reason for having the photograph in his possession or;
- That they had not themselves seen the photograph and did know or have cause to suspect it to be indecent or;
- That the photograph was sent to him/her without any prior request made by him/her or on their behalf and that they did not keep it for an unreasonable time.

Making and Distributing indecent Photographs / Images of Children

The Protection of Children Act 1978, section 1 provides:

It is an offence for a person:

- To take a permit to be taken, or to make an indecent photograph or pseudo photograph of a child or;
- To distribute or show such indecent photographs or pseudo photographs or;
- To have in his possession such indecent photographs or pseudo photographs with a view to them being distributed or show by him/herself or other or;
- To publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo photographs or intends to do so
For the purpose of this Act, a person is to be regarded as distributing an indecent photograph or pseudo photograph if he/she parts with the image, or exposes or offers the image for acquisition by another person. Where a person is charged with an offence under this subsection it shall be a defence for him/her to prove:

- That he/she had a legitimate reason for distributing or showing the photographs or pseudo photographs or having them in his or her possession.
- That they had not, themselves seen the photograph or pseudo photographs and did not know, nor had any cause to suspect them to be indecent.

Definition of a pseudo photograph / image: One that is created by image manipulation software so that the overall appearance of any figure is that of a child. Photographs are defined to include data held on a computer that can be resolved into an image.
# Checklist for Approval of Policy – (To be Removed in Finalised Version)

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Title</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the title clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it clear whether the document is a guideline, policy, protocol or standard?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2. Rationale</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are reasons for development of the document stated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3. Development Process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the method described in brief?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are people involved in the development identified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there evidence of consultation with stakeholders and users?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4. Content</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the objective of the document clear?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the target population clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the intended outcomes described?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the statements clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5. Evidence Base</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the type of evidence to support the document identified explicitly?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are key references cited?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the references cited in full?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are supporting documents referenced?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6. Approval</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the document identify which committee/group will approve it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If appropriate have the joint Human Resources/staff side</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Policy Ref:  
Version: 0.1  
Approved  
Review date
<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>committee (or equivalent) approved the document?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. **Dissemination and Implementation**

- Is there an outline/plan to identify how this will be done?
- Does the plan include the necessary training/support to ensure compliance?

8. **Document Control**

- Does the document identify where it will be held?
- Have archiving arrangements for superseded documents been addressed?

9. **Process to Monitor Compliance and Effectiveness**

- Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?
- Is there a plan to review or audit compliance with the document?

10. **Review Date**

- Is the review date identified?
- Is the frequency of review identified? If so is it acceptable?

11. **Overall Responsibility for the Document**

- Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?

12. **Equality Impact Assessment (EIA)**

- Has an equality analysis been undertaken in preparation for this policy?
- Has the equality analysis been quality assured by the Equality and Diversity Group?

**Individual Approval**

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>
### Committee Approval

If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation’s database of approved documents.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

---

Policy Ref:  
Version: 0.1  
Approved  
Review date