Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Policy Title: Joint Forensic Readiness Policy

Reference	POL/IG/009
Version	V1.0
Date Ratified	19/03/2019
Next Review Date	March 2022
Accountable Director	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)
Policy Author	Trust Information and Cyber Security Officer

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Cumbria Partnership NHS Foundation Trust | North Cumbria University Hospitals NHS Trust

Policy On A Page

SUMMARY & AIM

This Policy provides guidance on how to deal with the gathering, interpretation and preservation of digital evidence. It is directly pertinent to Senior Managers, Information Asset Owners & Administrators and those concerned with management led investigations regarding the requirements for Forensic Readiness in line with legal requirements, NHS Information Risk Management and Governance.

TARGET AUDIENCE:

- All Trust employees, consultants, third parties, contractors and temporary workers using Trust systems
- All Partner Organisations delivering services on behalf of the Trust and using Trust systems and others who have been given access to internal Trust systems in support of service delivery.

TRAINING:

- Mandatory Data Security Awareness training using the Trusts' TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1
- Local training in Incident Awareness, the individual's role in the digital evidence process and the sensitivities of forensic evidence.

KEY REQUIREMENTS

1. Managers must ensure that employees, agency staff and partners comply with the Trust's Information Security Acceptable Use Policy.

2. Managers must also ensure that any potential disciplinary action with regard to the use or misuse of information processing facilities is investigated with this Policy in mind.

3. Commencement of any investigation where forensic evidence may be required is to be preceded by gaining permission to proceed from HR and with a discussion with the Trusts' Cyber Security Managers on what evidence may be permissible and available.

4. Detailed forensic investigation is at present the sole responsibility of the Audit One Forensic Computing Service and the Local Counter Fraud Specialist

TABLE OF CONTENTS

1. INTRODUCTION 4
2. PURPOSE 4
3. POLICY DETAILS 4
4. TRAINING AND SUPPORT 5
5. PROCESS FOR MONITORING COMPLIANCE 6
7. REFERENCES: 6
8. ASSOCIATED DOCUMENTATION: 7
9. DUTIES (ROLES & RESPONSIBILITIES): 7
9.1 Chief Executive / Trust Board Responsibilities: 7
9.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates): 7
9.3 Senior Information Risk Owner (SIRO) Responsibilities: 7
9.4 Caldicott Guardian Responsibilities 8
9.5 Business Managers & Heads of Service 8
9.6 Trust Cyber Security Managers' Responsibilities 8
9.7 Information Asset Owners' (IAOs) Responsibilities 9
9.8 Approving Committee Responsibilities: Joint Information Governance Board 9
9.9 Audit One Forensic Computing Service 10
9.10 Local Counter Fraud Specialist 10
9.11 Staff Responsibilities 10
10. ABBREVIATIONS / DEFINITION OF TERMS USED 10
APPENDIX 1 – FORENSIC READINESS PROCESS 12
For computer equipment which is switched on: 12
For computer equipment which is switched off: 13
Incident Management Process 14
DOCUMENT CONTROL 15

1. INTRODUCTION

Forensic readiness is a key component in the management of NHS information risk. The forensic process reflects the high level of importance placed upon minimising the impacts of information & cyber security events and safeguarding the interests of patients, staff and the Trusts themselves.

A forensic examination of digital evidence is commonly employed as a post event response to a serious information or cyber security incident or computer related crime. In fact there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs.

The aim of the forensic process is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for disciplinary processes, formal disputes or legal cases. In this context, forensic evidence may include, but is not limited to, material in the form of web access and other system log files, emails, back up data, removable media, portable computers and network access records.

2. PURPOSE

This policy has been created to:

- Protect the Trusts, their staff and their 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 Trusts' 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.
- Ensure that the Trusts have systems and audit trails in place to allow evidence to be gathered routinely.

3. POLICY DETAILS

It is the policy of the Trusts that, in the event of an incident requiring investigation, any and all relevant forensic evidence will be collected, preserved and examined as part of that investigation.

The Forensic Readiness Policy is designed to help protect the information assets of the Trusts through the application of best practice in IT Forensic Investigation and to minimise the costs of such an investigation.

It aims also to ensure investigations are carried out in a systematic and structured manner that digital evidence has a positive impact on the outcome of any investigation.

Preparing to use digital evidence may involve enhanced system and staff monitoring; technical, physical and procedural means to secure data to evidential standards of admissibility; processes and procedures to ensure that staff recognize the importance and legal sensitivities of evidence; obtaining appropriate legal advice and interfacing with law enforcement.

The evidence from a forensic investigation 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 investigations.

Forensic readiness addresses a number of key business risks by providing evidence to detect and deter crime such as fraud, information theft, internet abuse, and by preparing an organisation for the use of digital evidence in its own defence.

The Trusts recognise that the aim of forensics is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for 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, network and telephone records amongst others that may be collected in advance of an event or dispute occurring.

Digital systems and distributed computing offer the Trusts great advantages in terms of efficiencies and cost saving. However our increased reliance upon these systems has proportionally increased risk, something the adoption of good practice and controls can help to reduce or eliminate. However, it is necessary, as part of incident response, to have the ability to collect and analyse data held on a variety of electronic devices or storage media that may be used as evidence in some future investigation.

Proactive forensic monitoring comprises of those systems and practices in place at the Trusts for monitoring computers, users, groups or systems. Examples of such practices include, but are not limited to: computer security logs, email logs, internet traffic monitoring and telephone exchange logs.

Reactive forensic investigations will normally be requested by an Executive Director or the Head of Information Governance within the organisation.

4. TRAINING AND SUPPORT

In order to ensure the correct implementation of this policy all managers are required to ensure that all their staff members are aware and have understood its content as part of approval of registration applications.

The following training requirements are specific to this policy:

- Employee Induction
- Mandatory Data Security Awareness training using the Trusts’ TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1
- Incident Management & Forensic Awareness for Managers (locally delivered & if applicable)

5. PROCESS FOR MONITORING COMPLIANCE

The process for monitoring compliance with the effectiveness of this policy is as follows:

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Cyber Security Incidents	Ulysses and SIRI reports relating to cyber security incidents	Head of Information Governance	Joint Information Governance Board	Quarterly or as deemed necessary by the seriousness of the incident

Wherever the above monitoring has identified deficiencies, the following must be in place:

- Action plan
- Progress of action plan monitored by the Joint Information Governance Board minutes
- Risks will be considered for inclusion in the appropriate risk registers

7. REFERENCES:

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

Public Records Act 1958
http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51/contents

Public Records Act 1958 (Admissibility of Electronic Copies of Public Records) Order 2001
http://www.legislation.gov.uk/uksi/2001/4058/contents/made

Regulation of Investigatory Powers Act 2000 (RIPA)
http://www.legislation.gov.uk/ukpga/2000/23/contents

Employment Practices Code
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Audit One Forensic Computing Service
https://www.audit-one.co.uk/forensic-computing

Forensic Readiness Guidance for Health & Social Care Organisations
https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-

health-and-care/forensic-readiness-guidance-for-health-and-care-organisations

8. ASSOCIATED DOCUMENTATION:

Information on the topics listed below can be found on individual Trust Intranet pages. Direct hyperlinks have been removed due to accessibility issues during the integration. If in doubt please contact the relevant IT Service Desk or IG Officers.

CPFT Intranet: http://cptportal.cumbria.nhs.uk/Pages/Home.aspx
NCUHT Intranet: http://nww.staffweb.cumbria.nhs.uk/index.aspx

- Information and Cyber Security Guidance
- Information and Cyber Security Policy
- Information and Cyber Security Acceptable Use Policy
- Information Risk Policy
- Incident Reporting Policies and Procedures
- Disciplinary Procedures
- Policy for the Use of Social Networking Sites.

9. DUTIES (ROLES & RESPONSIBILITIES):

9.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trust, including ensuring that Trust policies comply with all legal, statutory and good practice requirements.

9.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates):

The Executive Director of Finance & Strategy is responsible for ensuring the development and sign off of this Policy. They ensure the policy is kept up to date by the relevant author and approved at the appropriate committee.

9.3 Senior Information Risk Owner (SIRO) Responsibilities:

The SIRO has responsibility for ensuring that a Mobile Computing & Remote Access Policy is in place, and for assuring the Joint Trust Board of compliance with relevant legislative and mandated requirements. The SIRO has overall responsibility to ensure an Information & Cyber Security Policy framework is in place, including processes to monitor such use, thereby providing assurance that management of threats to security is in place, and that all employees are aware of their responsibilities

The role of the SIRO:

- Is accountable for approving all Information Assets.
- Fosters a culture for protecting and using data.
- Provides a focal point for managing information risk and incidents.
- Is concerned with the management of all information assets.

- To provide a focal point for the resolution and/or discussion of information risk issue.
- Ensure that all care systems information assets have an assigned Information Asset Owner.
- Ensuring the Organisation has a plan to achieve and monitor the right Information Governance culture, across the organisation and with its business partners.
- Approval of all information asset business continuity plans.
- Document a plan for information security assurance that identifies the support necessary to ensure work related to information security management is appropriately carried out.
- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Review and agree action in respect of identified information risks.

9.4 Caldicott Guardian Responsibilities

The Caldicott Guardian is appointed by the Trust Board and registered with NHS Digital. They ensure that the Trust achieves the highest standards for handling patient information. They represent and champion patient confidentiality issues within the Trust’s overall Information Governance Framework

9.5 Business Managers & Heads of Service

All Managers are responsible for ensuring:

- That their service works within the Information Governance framework.
- There are effective methods for communicating Information Governance related issues within their service.
- Information Governance responsibilities are reflected in staff objectives and discussed during the appraisal process.
- Staff members attend relevant training, induction and mandatory updates in relation to information governance.
- Staff members are aware of and adhere to information governance policies and procedures.
- Staff members are briefed and made aware of the requirements of Forensic Readiness in relation to incidents and their responsibilities to the preservation of any incident site.
- Ensuring that Incident reporting is integral to the operational activities within their areas and all incidents are reported and investigation in accordance with Trust Incident Reporting policy
- Where necessary, appropriate investigations are conducted, reports produced and action plans agreed and monitored.

9.6 Trust Cyber Security Managers’ Responsibilities

The Trust Cyber Security Managers along with selected members of the Trust IT Department will be allocated responsibility for assisting the **Audit One Forensic Computing Service** in the safeguarding of all Trust data and the management arrangements in respect of the trust's electronic data processing assets.

These responsibilities also include but are not limited to:

- Maintenance of Information & Cyber Security Policies in support of the forensic process
- Ensuring forensic evidence is available where possible
- Assisting IAOs in system security reviews in support of the forensic process
- Increasing management awareness of forensic evidence processes through this Policy and training sessions
- Specialist Information & Cyber Security investigations

9.7 Information Asset Owners' (IAOs) Responsibilities

Trust Information Asset Owners (IAOs) will ensure that Forensic Readiness Planning is adequately considered and documented for all information assets.
IAOs will submit their plans for Forensic Readiness to the SIRO for review along with any details of any planning assumptions or external dependencies.
Forensic Readiness plans must include specific actions with expected completion dates.

9.8 Approving Committee Responsibilities: Joint Information Governance Board

The Joint IG Board is the oversight committee for all items relating to information governance and reports into the Joint Clinical Governance Group and Quality and Safety Committee (Board Sub Committees) as required. In terms of policy responsibilities the role of the Joint IG Board is to ensure that local policies compliment the national policy, strategy and guidance relating to information governance and that it is implemented and evaluated appropriately within the Trust. The Joint IG Board are responsible that regular review of information governance policies and procedures takes place and monitors policy compliance at each of its meetings.

The Joint Information Governance Board (JIGB) is responsible for reviewing this Policy, ensuring it is fit for purpose and that it is ratified and passed for publication. The Chair of the JIGB will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

The Head of Information Governance reviews Information Governance incidents reported through the Trusts' Risk Management systems with this Policy in mind. The Head of Information Governance reports Serious IG Incidents to the JIGB. To further support the tenets of this Policy the Head of Information Governance reviews the Trusts' Information Flow Mapping on an annual basis, and reports any 'high risk' flows to the JIGB.

9.9 Audit One Forensic Computing Service

Expert forensic computing services are provided via the **Audit One** and are used to recover and/or review digital evidence for use in investigations.

These services include but are not limited to:

- Collection and preserving electronic data.
- Forensic examination of computers and digital media.
- Analysis of extracted data.
- Advice and assistance on computer related investigations in terms of legal requirements
- Support in disciplinary/court proceedings.

9.10 Local Counter Fraud Specialist

The Local Counter Fraud Specialist will provide direction for the processes to be followed in forensic work related to counter fraud in accordance with the Trust Incident Management Policy

9.11 Staff Responsibilities

All staff members are responsible for reading and co-operating with the contents of this Policy as part of their normal duties and responsibilities. They are responsible for ensuring that they maintain up to date awareness of Information Security practices with regard to their own and their staff roles and responsibilities.

10. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
AUP	Acceptable Use Policy
HR	Human Resources
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
JIGB	Joint Information Governance Board
SIRO	Senior Information Risk Owner

TERM USED	DEFINITION
Data communications	Networks and systems used to process, store and move electronic data
Forensic Readiness	The ability of an organisation to make use of digital evidence when required. The aim is to maximise the organisation’s ability to gather and use digital evidence whilst minimising disruption and cost.

TERM USED	DEFINITION
Forensic Readiness Planning	Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence related monitoring, collection processes & capabilities and storage requirements & costs.

APPENDIX 1 – FORENSIC READINESS PROCESS

Normally, where an incident has been deemed serious, the Investigating Officer will be from the Audit One Forensic Computing Service assisted by the Trust Cyber Security Manager or nominated deputy. All evidence provided as part of an investigation must be recorded and securely stored in such a way as to maintain its integrity until such time as the case, any hearings and appeals have concluded.

Any investigation which presents a suspicion of fraud should be notified to the appropriate Trust Director to engage the Local Counter Fraud Team. Any investigation which presents a suspicion of criminal activity should be notified to the SIRO to engage the police.

If you suspect, or are informed of, inappropriate usage of computer equipment you must contact your IAO/Line Manager and notify your Trust Cyber Security Manager immediately. If it is determined that this is suitably serious to require an investigation under SIRI regulations you must also inform the Data Protection Officer in order that an entry may be made in the Data Security & Protection Toolkit (DSPT) incident reporting tool.

Consideration must be given as to the strength of case required to proceed. In order to determine this, a preliminary investigation will be carried out by the IAO/Line Manager using advice and guidance from the Trust Cyber Security Manager based on assessment of:

- Indications of a potential breach of the Trusts' Acceptable Use Policies(AUP)
- Evidence of a reported crime (e.g. internal fraud, theft or other loss)
- Evidence of a Serious Incident Requiring Investigation (SIRI) or any other incident reportable under a compliance regime
- Any immediate threat to, or impact on, patients and third parties.

Following consideration of the above, in the case of a potential breach of the AUP, managers can request digital evidence via the IT Service Desk after having gained permission from HR. A discussion must also take place with the Trust Cyber Security Manager to determine what may be achieved. There is a formal process for the retrieval and interpretation of digital evidence.

Where there is a requirement for an investigation to be undertaken by the Audit One Forensic Computing Service staff members should ensure the steps in this Policy are followed.

If you are able to leave everything as is until the Audit One Forensic Computing Service investigator or Trust IT Technician arrives do so. However, equipment should not be left unattended or be accessed by unauthorised personnel at any time. Where this is not possible the following should be applied:

For computer equipment which is switched on:

- Contact the Trust Cyber Security Manager

- Where practical secure the area containing the equipment.
- Move people away from the computer and power supplies.
- 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). Secure documents when printing is complete.

N.B. Computer equipment involved in an investigation must only be moved in the event of a direct and immediate emergency.

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.
- 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 uninterruptible power device is fitted).
- 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).
- 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 Audit One Forensic Computing Service investigator or Trust IT Technician arrives.

For computer equipment which is switched off:

- Do not switch the computer on.
- Secure and take control of the area containing the equipment.
- Allow any printers to finish printing (further evidence may be printing). Secure documents when printing is complete.
- 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.

N.B. As with computers which are switched on, computer equipment involved in an investigation can be moved only in the event of a direct and immediate emergency. If you have to remove equipment before the investigator arrives, the following steps must be performed:

- 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).
- 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 Audit One Forensic Computing Service investigator arrives.

Incident Management Process

Further forensic investigation may be required as part of the incident management process defined for Counter Fraud, Major Incidents, Serious Incidents Requiring Investigation or Information & Cyber Security Incidents. This may involve assessment of damages, reputation loss and required recovery processes.

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	Joint IG Board 15/03/2019

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published
NCUH IG14 Cyber Security Forensic Readiness v4.0	8/8/2018	Aug 2021	Not published
CPFT POL/002/003 Forensic Readiness VFeb16	10/2/2016	Mar 2019	Not published

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1 Draft	07/09/2018	• Moved content of both existing Trust Policies into the new, joint template. • Restructured all sections for readability. • Moved Forensic Process into Appendix A. • Amended Forensic Process to reflect new NHS Digital Guidance. • Updated Roles and Responsibilities. • Updated Monitoring process.
0.2 Draft	08/01/2019	• Removed redundant requirements • Added Audit One information where required • Updated Abbreviations and Definitions
0.2 Draft	25/01/2019	• Stakeholder amendments added for typos and syntax where applicable
0.3 draft	12/03/2019	• Reference to previous trust policies in Doc Control section
0.4 draft	19/03/2019	**Amended following Policy Management Group meeting:** • Added Joint IG Board approval date to Policy front page and document control section, and Policy Checklist • Section 8.5 Joint IG Board Responsibilities added clarification that this is the approving committee for the Policy. • Section 8.3 Removed Associate Medical Director and left as Caldicott Guardian • Added SIRO responsibilities

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Michael Smillie	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)/Senior Information Risk Owner	10/01/2019
Robin Andrews	Interim Executive Director of Finance	10/01/2019
Andrew Brittlebank	Medical Director	10/01/2019
Graham Putnam	Associate Medical Director/Chief Clinical Information Officer	10/01/2019
Dave Dagnan	Consultant Clinical Psychologist	10/01/2019
Farouq Din	Associate Director of Digital Health	10/01/2019
Daniel Scheffer	Associate Director for Corporate Governance/Company Secretary	10/01/2019
Lesley Paterson	Associate Director of Quality & Nursing (Specialist Services)	10/01/2019
Lyn Moore	Associate Director of Operations	10/01/2019
Mandy Annis	Employment Services Bureau Manager	10/01/2019
Julie Thompson	Head of Workforce Services	10/01/2019
Elizabeth Klein	Head of Nursing - Clinical Standards	10/01/2019
Jacky Stockdale	Joint Business Manager - Corporate Services	10/01/2019
Paula McBride	Deputy Business Manager	10/01/2019
Kirsty Jay	Deputy Business Manager	10/01/2019
Laura Parkinson	Head of PMO	10/01/2019
Yvonne Salkeld	Head of IG	10/01/2019
Steve Johnstone	Joint Interim Head of IT	10/01/2019
Sarah Sproat	Clinical Nurse Specialist in Palliative Care	10/01/2019
Natalie Karam	Head of Performance	10/01/2019
David Franklin	Financial Systems Manager	10/01/2019
Kath Watts	Network Manager - First Step	10/01/2019
Katherine McGleenan	Clinical Quality Manager	10/01/2019
Anne Gadsden	Information Governance Officer	10/01/2019
Paul Corrie	Information Governance Compliance Manager	10/01/2019
All NCUH Business Managers		10/01/2019