Title:	**FORENSIC READINESS POLICY**

1. Policy Summary

1.1 Forensic Readiness is the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a court of law.

1.2 The Forensic Readiness Policy has been created to:

- Allow consistent, rapid investigation of major events or incidents with minimum disruption to Council business;
- Enable the pro-active and comprehensive gathering and storage of evidence in advance of that evidence actually being required;
- Enable the Council to gather computer based evidence for investigative purposes in such a manner that it is admissible for formal dispute or legal process;
- Demonstrate due diligence and good governance of the Council’s information assets

1.3 This policy is to be made available to all Council staff and must be observed by all members of staff, in particular:

- Information Asset Owners and Assistants;
- Data Protection officer(s);
- ICT professionals;
- Internal Auditors; and
- employees who may be involved in the recovery of computer equipment and other electronic devices for investigative purposes and the storage of such equipment and devices

1.4 Related Council Policies include:

- Computer Security Policy
- Mobile Phone Policy
- Server Back Up Procedures
- Data Retention Policy
- Information Governance Assurance Policy
- Data Quality Policy
- Anti-Fraud & Corruption Policy

1.5 Related legislation and national guidance includes:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Criminal Investigation and Procedures Act 1996

1.6 Information on the above Acts can be found on the government website: www.opsi.gov.uk/legislation.gov.uk and guidelines on Information Security can be found on the Information Commissioner's website: www.ico.gov.uk or from the Council's Legal Team.

1.7 This policy is for cascading from the Senior Information Risk Owner to Information Asset Owners and to Information Asset Administrators.

1.8 The Council aims to design and implement services, policies and measures that meet the diverse needs of our borough, stakeholders and workforce, ensuring that none are placed at a disadvantage over others.

1.9 Monitoring compliance and effectiveness will be achieved through annually reviewing Information Asset Owners plans, and ultimately through the auditing of actual incidents where forensic evidence is required.

2. Policy Introduction

2.1 The Council has endorsed the introduction of forensic readiness into the business processes and functions of the Council in order to maximise its potential to use digital evidence. This decision reflects the high level of importance placed upon minimising the impacts of information security events and safeguarding the interests of stakeholders, staff and the Council itself.

2.2 The Council recognises that the aim of forensic readiness 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, digital evidence may include information in the form of log files, emails, CCTV, back-up data, removable media, desktop computers, portable computers, tablets and mobile/smart phones amongst others that may be collected in advance of an event or dispute occurring.

2.3 The Council acknowledges that forensic readiness provides a means to help prevent and manage the impact of important business risks. 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.

3. Policy Definitions

3.1 Forensic readiness is the ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption and/or cost.

3.2 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 either in its own defence or for effective use in all types of disputes – criminal, civil, employment and disciplinary.

4. Policy objectives

4.1 The Forensic Readiness Policy has been created to:

- Protect the Council, its staff and its stakeholders 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 Council business;
- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required;
- Ensure that the council have systems and audit trails in place to allow evidence to be gathered routinely;
- Demonstrate due diligence and good governance of the Council's information assets;
- Enable the Council to gather computer based evidence for investigative purposes in such a manner that it is collected, documented, preserved and examined as evidence suitable for a wide range of scenarios, for example:
    - information compromise;
    - accidents and negligence;
    - corporate disputes;
    - disagreements, deceptions and malpractice;
    - financial crime e.g. fraud, money laundering;
    - content abuse;
    - privacy invasion and identity theft; and
    - employee disciplinary issues

5. Policy Statements

5.1 The Chief Executive has the ultimate accountability for the implementation of this policy.

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

5.3 The SIRO is responsible for the ongoing development and day-to-day management of the Forensic Readiness Policy within the Council's overall information governance regime.

5.4 The ICT team is responsible for providing the technical expertise and resource in forensic readiness, and for supporting the Information Asset Owners (IAOs) in producing robust forensic readiness planning for systems under their control.

5.5 Procedures and process documents will be kept up to date.

5.6 Information Asset Owners will ensure that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned 'ownership'

5.7 Goals for forensic planning include:

- The ability to gather digital evidence without interfering with business processes;
- Prioritising digital evidence gathering to those processes that may significantly impact the Council, its staff and its stakeholders;
- Allowing investigation to proceed at a cost in proportion to the incident or event;
- Minimising business disruptions to the Council;
- Ensuring digital evidence makes a positive impact on the outcome of any investigation, disciplinary, dispute or legal action.

5.8 Forensic readiness plans shall include specific actions with expected completion dates and submitted to the SIRO for review.

5.9 The SIRO shall advise the Chief Executive and the Council on forensic readiness planning and provide periodic reports and briefings on progress as necessary.

6. Forensic Readiness Process

6.1 Each system maintained by the Council will include, as part of its documentation details of its 'Forensic Readiness'. The section on 'Forensic Readiness' will contain:

- Details of the audit logs / system logs maintained including their name & location within the system;
- Who has access to the logs and their level of access;
- How long the log is to be retained and details of archived logs if required;
- Additional evidence that may be used, where it is stored and who has access.

6.2 Forensic readiness evidence for each system will be reviewed either every 12 months as part of the systems risk assessment cycle (high risk systems) and on a rolling three year programme (low risk systems).

6.3 In addition, each time there is a significant incident or event involving the system, this will trigger further assessment to review risk / identify requirements for additional forensic (digital) evidence collection. This will ensure that all systems are kept up to date with evidence that is pro-actively gathered and preserved to support investigation should an incident occur.

6.4 Some incidents are potentially suspicious. It is essential that Information Asset Owners, advised by ICT Services, define to those monitoring the data what they want to prevent and what triggers should provoke suspicion, whether heightened monitoring is required, and whether any additional security measures should be taken as a precaution.

6.5 Suspicious incidents can occur in countless ways, so it is impractical to develop comprehensive procedures with step-by-step instructions for handling every incident. Consequently arrangements should be in place to handle any type of incident and more specifically to handle common incident types. The primary suspicious incident categories are listed below:

- Denial of Service - an attack that prevents or impairs the authorised use of networks, systems, or applications by exhausting resources
- Malicious Code - a virus or other code-based malicious entity that successfully infects a host
- Unauthorised Access - a person gains logical or physical access without permission to a network, system, application, data, or other IT resource
- Inappropriate Usage - a person violates acceptable use of any network or computer policies
- Multiple Component - a single incident that encompasses two or more incidents.

7. Records Management

7.1 To ensure that evidence sources provides assurance to the organisation, records and evidence must provide accurate and reliable information. These need to meet standards and requirements as set out in this policy.

7.2 Audit logs record user activities, exception and information security events. These logs must be produced and kept for an agreed period determined by the SIRO and responsible IAO for each system or network device in accordance with best practice and for a minimum for six months, to assist any investigations and access control monitoring. Audit Logs will typically include, but may not be limited to:

- user IDs
- date, time and details of key events
- successful login / logout,
- unsuccessful login / logout,
- unauthorised application access (where applicable),
- file access attempts to protectively marked information
- privileged system changes.
- network addresses and protocols
- details of where audit logs are stored and their retention period will be found in each system’s documentation.

7.3 All logs must be protected against tampering or alteration and controls will be put in place to ensure this.

7.4 Retention and storage of audit logs needs to be secure. Where personal identifiable data may found within the logs they will be accessed on a need to know basis.

8. Recovery of Digital evidence

8.1 Principles

8.1.1 The Association of Chief Police Officers has developed a Good Practice Guide for Digital Evidence. This incorporates four principles applicable to the recovery of computer-based electronic evidence, which are recognised as the foundation of best practice in this field. The Council acknowledges these principles and seeks to ensure that, as far as possible, practices used by Council employees in the recovery of digital evidence, are consistent with them.

- *Principle 1:* No action taken in securing digital evidence by Council employees or other acting on behalf of the Council should change data which my subsequently be relied upon in criminal, civil, employment or disciplinary proceedings.
- *Principle 2:* In exceptional circumstances, where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- *Principle 3:* An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- *Principle 4:* The person in charge of an investigation has overall responsibility for ensuring that the law and these principles are adhered to.

8.2 Recovery Process

8.2.1 Computer based evidence is fragile and can be altered, damaged or destroyed by improper handling or improper examination. For this reason, special precautions must be taken to document, collect, preserve and examine this type of evidence. The approved process, which must be followed in all cases, is described in Appendix 1 - Guidance for the Collection of Digital Evidence.

9 Evidence Retrieval

9.1 The retrieval and analysis of digital evidence is a specialised field and only to be undertaken by persons with the requisite training, experience and independence. In general, it is not the Council's intention that this should be done in-house.

9.2 The Head of Internal Audit should arrange for the collection, examination and analysis of data and the reporting thereon by suitably qualified forensic practitioners.

10 Training and Awareness

10.1 All users need to be aware of what to do when a suspicious incident happens. Some staff, such as Information Asset Owners and Administrators will require more specialised training to ensure that they are competent to perform their role relating to the handling and preservation of the evidence. They must be able to fully understand the process of any investigations and the relationships and necessary communication with internal and external parties.

10.2 Information governance and security training will be delivered to meet business requirements in relation to forensic readiness.

11 Reviewing the Policy

11.1 The Director of Resources, as Senior Information Risk Owner, will undertake an annual review of the policy to assess the adequacy of its operation and compliance with legislation. The policy will also be refreshed to reflect any changes to the Council’s corporate structure or the responsibilities of individual officers.

APPENDIX 1

GUIDANCE FOR THE COLLECTION OF DIGITAL EVIDENCE

This guide is based on the Association of Chief Police Officers’ Good Practice Guide suggests methods that will help preserve the integrity of such evidence for effective use in all types of disputes – criminal, civil, employment and disciplinary. These general principles must be followed to ensure the best chance of evidence being recovered in an uncontaminated and therefore acceptable manner. Failure to do so may render it unusable or lead to an inaccurate conclusion.

1. Desktop and laptop computers

1.1 Computers to be secured from offices for the purposes of investigation are desktop or laptop PCs. These machines usually consist of a screen, key board and main unit, with slots for storage devices.

1.2 However, most desktop users now make use of a thin client, a network computer without a hard disk drive, which acts as a simple terminal to the server. There is no data storage capacity and no purpose in securing such equipment.

1.3 With desktop and laptop computers the essential concern is not to change the evidence on the hard disk and to produce an image which represents its state exactly as it was when seized.

Devices switched off:

- Secure the area containing the equipment and do not permit anyone to touch the equipment or power supply
- Make sure the computer is switched off
- Don't in any circumstances switch the computer on – some laptop computers power on if the lid is opened
- Remove the battery from laptop computers
- Unplug devices from power points
- Photograph or film all the components *in situ*
- Securely label, sign and date all the components
- Label the ports and cables so that the computer may be reconstructed at a later date
- Record the unique identifiers/IT Asset Numbers for each element of the computer – the main unit, screen, keyboard and any other ancillary equipment
- Search the area for notebooks or pieces of paper with passwords on, which may be stuck close to the equipment
- Ask the equipment user for any passwords that may be relevant and if these are given, record them accurately
- Carefully remove the equipment and place in appropriate evidence bags, which should be secured with a plastic, numbered seal
- Record the contents and seal number for each bag

Devices switched on:

- Secure the area containing the equipment and do not permit anyone to touch the equipment or power supply
- Record what is on the screen by photograph and by making a written note of the content
- Do not touch the keyboard or click the mouse but if the screen is blank or displays a screen saver, move the mouse to test if the screen restores and if so photograph and note its content, and record the time and use of the mouse
- Without closing down any programs, remove the power supply cable from the end attached to the computer and not the end attached to the socket
- Remove all other connection cables leading from the computer to other devices or sockets

- Photograph or film all the components *in situ*
- Securely label, sign and date all the components
- Label the ports and cables so that the computer may be reconstructed at a later date
- Record the unique identifiers/IT Asset Numbers for each element of the computer – the main unit, screen, keyboard and any other ancillary equipment
- Search the area for notebooks or pieces of paper with passwords on, which may be stuck close to the equipment
- Ask the equipment user for any passwords that may be relevant and if these are given, record them accurately
- Carefully remove the equipment and place in appropriate evidence bags, which should be secured with a plastic, numbered seal

1.4 It has to be accepted that the action of disconnecting a computer may mean a small amount of evidence is unrecoverable if it has not been saved but the integrity of the evidence present will be preserved.

1.5 Bear in mind that certain devices may be connected to the network via a conventional network cabling, while other may be connected via a wireless link.

What should be secured?

- Main unit - the box to which the monitor and keyboard are attached
- Monitor, keyboard and mouse
- Leads including power cables
- Hard disks not fitted inside the computer
- Dongles - small connectors with some memory
- Modems
- Other external storage devices
- Digital cameras
- CDs/DVDs
- Memory sticks
- Printed paper
- Anything that may contain a password

2. Tablets and Smartphones

2.1 A tablet computer is a mobile computer with a touchscreen display, circuitry and battery in a single device. Tablets come equipped with sensors, including cameras and microphones, with the touchscreen display substituting for the use of computer mouse and keyboard. A smartphone is a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps. Consult IT to determine which devices are currently in use.

2.2 With a tablet or smartphone there is no hard disk and the concern is to change the evidence in the main memory as little as possible.

Device switched off:

- Secure the area containing the equipment and do not permit anyone to touch the equipment
- Don't in any circumstances switch the computer on
- Where the device is fitted with only a rechargeable battery the mains adaptor should be fitted to the device, which subsequently should be kept on charge
- Place the device in a sealed envelope with the adaptor cable, if fitted, passing through it
- Place the sealed envelope in an appropriate evidence bag, which should be secured with a plastic, numbered seal with the adaptor cable, if fitted, passing through it
- Record the contents and seal number for each bag

Device switched on:

- Secure the area containing the equipment and do not permit anyone to touch the equipment
- Do not press Reset or remove the batteries under any circumstances as this can result in the loss of all information held on the device
- Switch off the device to preserve the battery life
- Make a note of the time and date of the action
- Where the device is fitted with only a rechargeable battery the mains adaptor should be fitted to the device, which subsequently should be kept on charge
- Place the device in a sealed envelope with the adaptor cable, if fitted, passing through it
- Place the sealed envelope in an appropriate evidence bag, which should be secured with a plastic, numbered seal with the adaptor cable, if fitted, passing through it
- Record the contents and seal number for each bag

What should be secured?

- Tablet or smartphone
- Power leads and adaptor cables
- Memory sticks

2.3 Be careful only to seize devices that have been provided by the Council for business purposes.

3. Personnel

3.1 The removal of computer equipment for investigative purposes must be carried out by or in the presence of two members of the Internal Audit team as a minimum. With a planned operation the Head of Internal Audit should consider obtaining the services of persons who have had appropriate formal training and are experienced in the seizure of computer equipment.

3.2 When it is proposed to secure computer equipment, preliminary planning is essential and as much information as possible should be obtained in advance about the type and location of any computer equipment allocated to or used by the employee under investigation.

3.3 It is essential that all personnel attending are adequately briefed, not only in respect of the logistics and equipment expected to be present, but also about this guidance and the means of safeguarding digital evidence.

4. Records

4.1 A record of all the steps and actions taken when computer equipment is secured must be completed contemporaneously, usually by a member of Internal Audit. The information to be recorded includes:

- Details of all persons present where computer equipment is present
- Details of all computer equipment – make, model, serial number, IT asset reference
- Display details and connected peripherals
- Remarks/comments/information offered by user(s) of equipment
- Actions taken at scene showing time

5. What to Take

5.1 The following is a list of equipment that might be useful for the proper dismantling of computer equipment as well as for its packaging and removal.

- Appropriate tools such as screwdrivers (flathead and crosshead), small pliers and wire cutters for the removal of cable ties
- Adhesive labels and tapes to mark and identify individual components
- Tie-on labels for evidence bags
- Paper sacks and envelopes for securing equipment
- Evidence bags capable of being secured with plastics ties
- Plastic ties for securing evidence bags
- Camera to photograph items *in situ* and any on-screen displays

6. Storage

6.1 The computer equipment should be stored at normal room temperature without being subject to any extremes of humidity and free from magnetic influence, such as radio receivers. Equipment powered by batteries should not be allowed to become flat, or internal data will be lost.

6.2 It is essential that equipment stored pending investigation is held securely in a locked receptacle. Only members of the Internal Audit team should have access to the equipment. Under no circumstances should the security seals be removed from evidence bags before the equipment is handed over for evidence removal.

6.3 The equipment should not be passed from the control of Internal Audit unless it is at the request of the:

- Chief Executive,
- Director of Resources

7. Evidence Retrieval

7.1 Generally the retrieval of digital evidence will not be undertaken in-house. The Head of Internal Audit should arrange for the collection, examination and analysis of data and the reporting thereon by suitably qualified forensic practitioners.

7.2 The Head of Internal Audit must brief the person(s) appointed to undertake the recovery process concerning the matter under investigation to the extent that data analysis highlights all pertinent evidence with probative value to the case.