

Fraud Response Plan – IT and Electronic Evidence

1 INTRODUCTION

1.1 This document provides direction to officers who are tasked with investigating suspected theft, fraud, or corruption in an IT environment. It is intended to support the recovery of computer-based electronic evidence. It provides a response framework that enables evidence to be gathered and collated in a timely and appropriate way. It aims to facilitate an informed initial decision and ensure that any evidence gathered is lawfully obtained and will be admissible in Court if the matter proceeds to criminal or civil action.

1.2 Information held on a computer system may provide evidence of either:

- The situation in the records at a specific point in time; or
- A fraud that has been committed or is being committed.

Such evidence may, therefore, form part of the investigation and may be required for any subsequent disciplinary or criminal proceedings.

2 THE PRINCIPLES OF COMPUTER BASED ELECTRONIC EVIDENCE

2.1 When seeking to gather electronic evidence, the senior investigating officer must ensure:

- a) No action taken changes data held on a computer or storage media which may subsequently be relied on in Court.
- b) An audit trail or other record of all processes applied to computer based evidence is collated and preserved.
- c) S/he maintains overall responsibility for ensuring that the law and other principles are adhered to.

2.2 The role of the senior investigating officer is to:

a) Determine the nature of the investigation

Should it be determined that the case is likely to go to Court, where the conduct and results of the examination of equipment will be relied on, then the senior investigating officer should contact a specialist IT forensic company to undertake the investigation.

b) Maintain a record of all actions taken and conclusions reached

The senior investigating officer will regularly update the, Strategic Director of Finance, Policy and Governance, Audit Manager and the External Auditor if appropriate of actions taken and the outcomes of such courses of action.

c) Ensure a consistent approach to the conduct of any investigations

The senior investigating officer will ensure that matters reported and proper records of each action taken are kept from the outset, including accurate notes of when, where and from whom evidence was obtained, and by whom. All actions will be recorded on the IT Fraud Investigation Forms.

3 GATHERING EVIDENCE – EXTERNAL

3.1 The initial objective of gathering evidence is to establish whether or not a detailed examination of computer based evidence is required. External specialist organisations might be used to perform such an investigation if it determined that the evidence requires specialist forensic examination.

3.2 The employment of an external organisation to undertake the examination of evidence must comply with the Council's Procurement Rules.

GATHERING EVIDENCE - INTERNAL

- 3.3 Effectively planning and responding to an investigation requires an investigating officer to know how the relevant computer system(s) is / are structured. The following information should be recorded:
- **System Configuration**
Type of computer and hardware used, desktop and network operating systems, and the type of network and software.
 - **Application software**
The names of all the application systems used on the system.
 - **Back-up procedure and frequency**
The name and version of the back-up software used, the length of time back-ups are kept and how often back up media is used. Details about how the back-up media is indexed and stored should also be noted.
 - **Logons and passwords**
Any encryption programs that are used to lock sensitive information.
- 3.4 Additionally, it is important not to overlook the fact that evidence may be held on an individual's home computer. Data can be transferred to and from the workplace via email, **portable media** or the employee may be able to log into the network from home. Dial in to the Council's network is facilitated by the Council's home working policy.
- 3.5 If material of a criminal nature (for example child pornography) is discovered, the Audit Manager should be contacted immediately in order that liaison with the Police can take place.

Preserving the Chain of Custody

- 3.6 A chain of custody verifies that information copied was not altered either in the copying process or during analysis. To ensure that this is the case, the senior investigation officer must:
- Prove no information was added or harmed – to this end the software the investigating officer intends to use must be virus checked. It also means that before examining any media or making any copies that the originals are 'write-protected' so that no data can be added or changed during inspection and copying.
 - Make a complete copy of the data – An image copy creates a mirror image of the drive being copied, thus capturing all data, including residual data on the drive surface. Simply making a file by file copy will only capture active data and may be inadequate for evidentiary purposes.
 - Use a reliable copying process which meets industry standards. The process used must be capable of independent analysis, and must create tamperproof copies. On completion of the copying process all equipment must be bagged and evidential seals used.
 - Secure all media – All media should be labelled by time, date and source and stored in a secure place. Forensic analysis of the information collected should be undertaken on a working copy of the secure copy.

Appendix A

Checklist

Desktop and Laptop Computers

Where the computer equipment is switched off:

- 5.1 secure and take control of the area containing the equipment
- 5.2 Allow any printers to finish printing
- 5.3 Move people away from any computers and power supplies
- 5.4 Don't switch the computer on
- 5.5 Make sure the computer is actually switched off and not on screen saver by checking monitor activity lights
- 5.6 Remove the battery from laptop computers
- 5.7 Unplug the power and other devices from the sockets
- 5.8 Label and photograph all the components *in situ*
- 5.9 Label the ports and cables so that the computer may be reconstructed at a later date
- 5.10 Carefully remove the equipment and record unique identifiers – the processor, screen, keyboard and other equipment
- 5.11 Search the area for diaries, notebooks or pieces of paper with passwords
- 5.12 Consider asking the user if there are any passwords, and if they are given, record them accurately

Where the computer equipment is switched on:

- 5.13 Secure the area containing the equipment
- 5.14 Move people away from the equipment and power supplies
- 5.15 Disconnect any modems attached
- 5.16 If the computer is believed to be networked seek advice from an external specialist
- 5.17 Label and photograph all the components and label the ports and cables so that the computer can be reconstructed at a later stage
- 5.18 Remove all the connection cables leading from the computer to other wall or floor sockets or devices
- 5.19 Carefully remove the equipment and record unique identifiers – the processor, screen, keyboard and other equipment
- 5.20 Allow the equipment to cool down before removal
- 5.21 Search the area for diaries, notebooks or pieces of paper with passwords
- 5.22 Consider asking the user if there are any passwords, and if they are given record them accurately
- 5.23 Record what is on screen by photograph and by making a written note of the content of the screen
- 5.24 Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present the senior investigating officer should decide if they wish to restore the screen. If the screen restores, photograph and note its content.

