**Appendix 3: Computer Misuse Procedure**

# Computer Misuse

Computer misuse is an activity involving NHS Fife computing resources which is illegal or prohibited, and which, not exhaustively, includes:

* compromises the Security of the NHS Fife eHealth Systems or its data; or, whereby affecting the confidentiality, integrity or availability of NHS Fife’s information assets;
* generates a formal complaint from a member of the public or another member of NHS Fife staff;
* results in civil or criminal proceedings being mounted against NHS Fife or a member of NHS Fife staff;
* use NHS Fife’s owned equipment or networks for malicious purposes e.g. hacking, software piracy, software or data theft, copyright contravention etc;
* breaching NHS Fife information security policies or procedures;

# Computer Forensics

Specialist computer forensic services may be brought into NHS Fife where Investigations conducted by the eHealth Security Manager have failed to establish the cause of a major security incident and such involvement is justified, or where other issues come to light which warrant the involvement of specialists in order to take the investigation to its conclusion.

# Initial Action

Where computers/servers etc, have network access and are identified as being compromised, the device shall be removed from the network (wired or WiFi).

The only exception to this is where the compromised machine is listed as a “critical system”. In such case, the person responsible for it will be contacted, notified of the problem and instructed to liaise with the eHealth Department to address the issue immediately.

Where the owner of a compromised machine is a third party supplier, they must be contacted immediately and instructed to address the issue. If the issue is a threat to other critical eHealth systems then the machine responsible shall have its connections blocked.

# Investigative Actions, requesting Help and Reporting Findings

All major security incidents will be investigated by the eHealth Security Manager, in consultation with technical system leads and/or local system administrators.

All minor incidents are to be investigated by technical system leads and/or local system administrators and the results reported to the eHealth Security Manager.

On completion of an investigation the findings are to be recorded on the call management system under the call reference number for the incident.

# Securing Evidence Procedure

To ensure that all potential evidence is secured during computer misuse investigations is admissible in a court of law; all investigations will follow the Association of Chief Police Officers (ACPO) guidelines (Computer Evidence)

[https://www.cps.gov.uk/legal/assets/uploads/files/ACPO\_guidelines\_computer\_evidence[1].pdf](https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5B1%5D.pdf)

To ensure that this is attained, staff shall quarantine the area where the computer is located and report the potential incident to the Departmental Manager and inform the eHealth Service Desk.

eHealth staff will carry out the required steps outline In sections 5.1, 5.2 and 5.3. These basic steps will prevent data loss or corruption and maintain the admissibility of evidence in a court of law.

## Upon discovery of computer equipment which appears to be switched off:

• Secure and take control of the area containing the equipment.

• Move people away from any computers and power supplies.

• Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date.

• Allow any printers to finish printing.

• Do not, in any circumstances, switch the computer on.

• Make sure that the computer is switched off – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine

is switched on.

• Be aware that some laptop computers may power on by opening the lid.

• Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss.

• Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket).

A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of files.

• Label the ports and cables so that the computer may be reconstructed at a later date.

• Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so

may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners.

• Search the area for diaries, notebooks or pieces of paper with passwords on which are often attached or close to the computer.

• Consider asking the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately.

• Make detailed notes of all actions taken in relation to the computer equipment.

## Upon discovery of computer equipment which is switched on:

• Secure the area containing the equipment.

• Move people away from computer and power supply.

• Photograph or video the scene and all the components including the leads in situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that system/s may be reconstructed at a later date.

• Consider asking the user about the setup of the system, including any passwords, if circumstances dictate. If these are given, record them accurately.

• Record what is on the screen by photographing and by making a written note of the content of the screen.

• Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video it and note its content. If password protection is shown, continue as below, without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances.

• Where possible, collect data that would otherwise be lost by removing the power supply e.g. running processes and information about the state of network ports at that time. Ensure that for actions performed, changes made to the system are understood and recorded. See section on Network forensics and volatile data.

• Consider advice from the owner/user of the computer but make sure this information is treated with caution.

• Allow any printers to finish printing.

• If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket. This will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

• Remove all other connection cables leading from the computer to other wall or floor sockets or devices.

• Ensure that all items have signed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners.

• Allow the equipment to cool down before removal.

• Search area for diaries, notebooks or pieces of paper with passwords on which are often attached or close to the computer.

• Ensure that detailed notes of all actions are taken in relation to the computer equipment.

## What should be seized

For the retrieval of evidence (Examples):

• Main unit: usually the box to which the monitor and keyboard are attached.

• Monitor, keyboard and mouse (only necessary in certain cases. If in doubt, seek expert advice).

• Leads (again only necessary in certain cases. If in doubt, seek expert advice).

• Power supply units.

• Hard disks not fitted inside the computer.

• Dongles (see Glossary in ACPO guidelines).

• Modems (some contain phone numbers).

• External drives and other external devices.

• Wireless network cards (see Glossary in ACPO guidelines).

• Modems.

• Routers.

• Digital cameras.

• Floppy disks.

• Backup tapes.

• Jaz/Zip cartridges.

• CDs.

• DVDs.

• PCMCIA cards (see Glossary in ACPO guidelines).

• Memory sticks, memory cards and all USB/firewire connected devices.

N.B. Always label the bags containing these items, not the items themselves.

# Computer Misuse by Staff

All cases of alleged computer misuse by staff will be dealt with in accordance with existing NHS Fife policies.

The user account will be suspended in the initial stages of the investigation when the nature of the allegation is such that this action is considered necessary.

The eHealth Security Manager will report to the appropriate Line Manager cases of actual or suspected computer misuse by staff.

# Recovery of Stolen Equipment

Unless equipment is returned by the police it must not be touched by ungloved hands. It must be bagged and passed to the police for finger printing.