Removal of computing devices, for Investigation or Quarantine of Server as Evidence

1. Users and managers should note there are occasions when either a PC may be required to be removed from their normal location, or information held on servers, including the Storage Area Network Systems (SANS) may be required for investigations. As the removal or quarantining of evidence is normally part of a serious investigation, this process is not to be undertaken lightly. It is often the prelude to a disciplinary process which may lead to dismissal or even criminal proceedings. It may also be required where the evidence held may be required by a tribunal or other process. In this latter case it is probable that it will have been preceded by a court or other statutory instrument being served on NHS Lothian. Which ever applies these processes are not to be initiated without the approval of an eHealth Executive Manager or without the permission of the NHS Lothian IM&T Security Manager in their absence.

2. The guidance within this Policy is taken from the Association of Chief Police Officers, ACPO,
3. “Good Practice Guide to Preserving Computer Evidence”
4. The need for removal of evidence may be initiated through three main sources:
   a. Within the IS department from information gathered through routine examinations of the network or servers
   b. When asked by a departmental other senior manager through a suspicion or other evidence of improper behaviour.
   c. Court Order or other legal requirement

5. When the information is discovered through routine monitoring, the member of IS making the discovery is inform the IS Security Manager or Security Officer immediately, they will discuss this with the senior eHealth managers the most appropriate approach.

6. When the request is from a departmental or service manager, it must be stressed that this is a serious matter and that the manager must be prepared to justify that the alleged offence is in clear breach of NHS Lothian policies. That request should be made formally, in writing or by email to the Director of eHealth, one of the eHealth Executive Managers or to the IM&T Security Manager in their absence. As this
sequence of events may lead to disciplinary or criminal action it is essential that the evidence be preserved and that a log of proceedings must be maintained throughout. An IM&T Security Officer will be allocated to the investigation and will have responsibility for initiating and maintaining the log.

7. The location of the staff or group under suspicion will determine the actual process to be followed as due to the differences in the infrastructure throughout NHS Lothian. The process to be adopted must be discussed and agreed prior to any PC or drive being searched or withdrawn from service.

8. That discussion must include the following personnel:
   a. eHealth Security Officer,
   b. Manager of department or of any individual under suspicion of wrong doing,
   c. Staff side representative, member of server or desktop support team responsible for that site and a member of HR department.

9. Where a computer device is involved or suspected of being used illegally the internal cache of that computer device may hold information which can be tied directly to an individuals log in ID and personal profile. Even where no access is routinely granted to the local hard drive by a user this information is cached on the local drive and may remain on that drive for the life of the computer device. It should be considered that where only a suspicion of an illegal process is held or where information is routinely stored on a server drive, removing the device for detailed analysis might be the only course of action. If necessary the member of staff should be informed of the nature of the suspicion by their manager in the presence of the staff side and HR representative. They should be asked about the matter under investigation and whether they have any comments. They should also be asked to disclose any passwords for any files and folders under their control. The device should be removed and if appropriate another connected. The "Home" drive of the member of staff should be frozen and another allocated if the staff member is to be allowed to continue in post whilst investigations are undertaken. Where the decision is taken to suspend a member staff during an investigation, their access to services and systems are to be removed.

10. When a PC is removed or a server drive is involved, no attempt is to be made to check the data held until two copies of those drives have been made. The PC and drive copies should be labelled and secured by the IM&T department. One of the copies will be used for initial forensic examination, the other held should a problem exist on the first or if external forensic specialists are required. The log of proceedings must identify all events and copies where they were made, when and by whom.
11. During the initial forensic examination if, at any time, any evidence of an illegal activity is uncovered, e.g. paedophile pornography or fraud, the investigation is to be halted and NHS Lothian senior managers advised prior to the investigation being handed over to the appropriate authority, police or NHS Fraud investigation unit.

12. Four principles\(^1\) must be followed at all times:

- **Principle 1.** No action should be taken to change data held on a computer or storage media which may subsequently be relied upon in court.

- **Principle 2.** In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, 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 computer based electronic 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 the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

---

\(^1\) “Good Practice Guide for Computer based Electronic Evidence v.3”, Assoc of Chief Police Officers p 6