Walton Centre

Incident Response (Legal & Forensic)

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain	

Table of Contents

1. Introduction

Information and information systems are important assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust .

The Trust acknowledges that we must demonstrate to our stakeholders our commitment to, and delivery of, effective information governance.

The aim of the Trust Governance Policy, Standards and Guidelines is to maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within the Trust. These policies, standards, guidelines are used as part of the information security management system (ISMS) within the Trust.

The Trust places great reliance upon the robust application of the policies and standards that make up the ISMS and has, therefore, developed processes to self assess compliance and for independent review, by its internal auditors.

This standard applies to all staff, whether permanent, part-time or temporary with responsibilities defined below.

2. Responsibilities Within This Standard

All employees using IT equipment, the internet or e-mail have responsibilities with regard to this standard. Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line managers (in scope)
Compliance	All staff and contractors (in scope)
Monitoring	Information Security Officer Information Security Auditor

3. Incident Response

3.1 Background

Incidents fall, broadly, into two categories, those that can be investigated and resolved internally and those which require external expertise to support a forensic investigation. Forensic investigation is necessary where computer based electronic evidence may exist to support disciplinary or legal action.

Where forensic investigation is or may be required the Trust will abide by the guidance provide by the Association of Chief Police Officers and the National High Tech Crime Unit and, where there is a suspicion of fraud, in accordance with the requirements of the Directorate of Counter Fraud Services guidance.

In such circumstances the Trust should take no action in respect of the investigation before contacting its internal auditors and/or Local Counter Fraud Specialist who will facilitate the investigation process.

3.2 Initial Actions

3.2.1 Context

When an information security incident occurs there are a number of things that need to be done in a formal manner so that the incident is properly documented and channelled into the process of incident management.

3.2.3 Verify the incident

When an incident occurs there are a number of things that need to be done to put the initial investigation on a good footing viz:

- Formally record that an incident has happened
- Record what the incident is believed to be
- Record the potential impact from the incident
- Make a case for an initial investigation

- Report to senior management
- Allocate or apply for funds to complete the initial investigation
- Register the requirement for further funding if the initial investigation is positive.

This process should be undertaken using the Trust ‘s standard incident reporting process.

3.2.3 Involve all interested parties

It is essential to ensure that all parties that will be required to take action are involved as early as possible. Only involve essential parties at this stage, such as:

- Senior management sponsor
- Internal Audit
- HR
- Legal
- IT
- Security
- Press office.

Discussion of the event or knowledge of the occurrence of the incident should be kept strictly to only those that have a clear need to know. The more people who are aware of the incident, the more opportunity there is for people to interfere, hamper or compromise the investigation. This helps to ensure the suspect (if there is one) does not become aware of the investigation and does not get any access through which they might be able to delete evidence or cover tracks.

Investigators should be aware of collusion, there might be more than one miscreant working alone.

It is also advisable to consider the need for a media response should the incident be leaked either by the Trust, a member of staff or the perpetrator.

3.2.4 Identify an incident manager

An incident manager should be identified, to manage the investigation team. This may be either a manager from a non-related business area or, where appropriate, an individual from a

specialist area that carries out investigations, such as internal audit or the Local Counter Fraud Specialist.

The incident manager should be aware of, or have direct access to other who are aware of, the prevailing laws such as the Data Protection Act, Regulation Investigation Powers (RIP) Act and the Human Rights Act so that he is able to ensure that an individual's privacy and human rights are maintained. This is especially important because the investigation may prove the suspect's innocence.

3.2.5 Prepare investigation documentation

An incident management log should be established to record all actions taken in the investigation, the results and the evidence secured as a result.

It is critically important that all actions taken within an investigation can be accounted for within a chronological sequence in case the incident results in legal action. This is especially important in relation to the access and recovery of IT based evidence. The Incident Manager is responsible for ensuring that the incident log is current and accurate.

3.2.6 Prepare media management

The Trust should carry out its investigation in the expectance that the incident will, at some stage, become public knowledge and it should prepare itself for reaction in case of a leak.

Staff involved in the investigation should be advised not to speak to the press or any individuals directly involved in the investigation.

The corporate services manager should be involved as the rumours inside the organisation need to be controlled as much as the rumours outside.

3.2.7 Decide on the course of the initial investigation

The first task of the investigation team is to consider what could be done to investigate the incident in a passive manner without alerting the instigator(s). The objective should be to collect enough evidence to make a decision about further active investigation. It is important that the team documents what will be undertaken as a part of the initial investigation in as much detail as possible to avoid criticisms of bias or 'fishing'.

3.2.8 Identify specialist skills required

It is important to identify early on whether specialist skills will be required, such as computer imaging, computer forensics or network monitoring, and where those skills will come from.

Where forensic skill are required the first port of call should be the Trust's internal auditors who will facilitate this process.

Additionally it is essential to provide training, for the people who are likely to be involved in an incident, such as evidence identification and preservation for first responders, evidence gathering and the need for scrupulously accurate logs.

3.2.9 Activate the Incident Response Team

If necessary an incident response team should be called together to conduct the investigation and the Incident Manager should ensure that they are properly supported.

Where members of the team are tasked with evaluation of inappropriate data and/or images that contain the more extreme areas of pornography and violence, they should be appropriately managed and offered support, which includes counselling.

3.2.10 Estimate budget requirements

Investigation of incidents can be a costly exercise given the need for specialist resources etc. and it is not always possible to gauge the extent of such costs at the outset.

However, it is essential that there is initial indication of potential costs and agreement that these can be funded in order that the investigation can be progressed.

3.2.11 Create incident control room (if required)

Where an investigation is particularly sensitive, or where the investigation could disturb normal business it is essential that a “secure” are is established for conducting the investigation.

Where such an area is a secure room, access should be restricted to only those involved in the investigation. Alternatively, it may be possible to undertake the investigation in a less secure area with all sensitive documents and equipment etc be looked away in secure cupboards etc when not required. Again, in such circumstances, access should only be granted to those involved in the investigation.

3.3 Preliminary Investigation

3.3.1 Context

This is a high level investigation to establish the facts of the incident and whether or not it requires detailed investigation. It is a passive and non-destructive assessment to confirm whether there has been an incident that requires further investigation and if so what level of further investigation is required.

3.3.2 Establish the objectives of a preliminary investigation

The initial investigation of an incident can be both difficult and hazardous. It can be difficult because in the early minutes of an incident only the tip of the iceberg will be visible, and it is easy to misjudge what is really going on. It is hazardous because an incorrect analysis in the

early stages can lead to the investigation going off in entirely the wrong direction, not only wasting valuable time, but also possibly hindering any later full-scale investigation.

There are some critical judgements that need to be made in the early stages including:

- What is the severity/criticality of the incident
- Has this incident crossed any significant boundaries
- Geographic differences, cultures and different laws
- Criminal versus corporate policy breach – if a crime is being or has been committed, the response might be handled differently than if it is purely an internal policy violation
- Regulatory impact.

When conducting an investigation it is important to make sure that the full range of contextual information is available and ask the question, is there another explanation of what is being seen that might be innocent or benign? Always be aware that the individual(s) under investigation may be innocent and ensure that their privacy and human rights are not violated

3.3.3 Request technical support

Technical resources required to complete the investigation should be ascertained at the earliest opportunity and agreement should be reached to receive this support. Typically such resources may include:-

- Technical IT staff
- Internal Auditors
- Counter Fraud Specialist

3.3.4 Gather preliminary evidence

Evidence can be sought from as many areas as possible without externally affecting them. Likely areas that are worth considering are:

- E-mail
- Internet usage
- Memory caches
- Voice recording

- Network monitoring
- CCTV
- Access controls systems
- System logs
- Time sheets
- Building access logs
- Eyewitness accounts (e.g. what was seen on the screen).

It should be ensured however, that evidence collection is not in breach of legal requirements such as the Regulation of Investigatory Powers Act and the Human Rights Act etc.

WARNING Even if a prosecution is not planned, it is important to preserve evidence. The organisation may be taken to a tribunal or court even if that was not the original intention.

3.3.5 Analyse preliminary evidence

During an investigation it is important to keep an open mind and not to jump too quickly to conclusions, things might not necessarily be as they first appear because there have been instances where evidence has been falsified to discredit someone. Likewise it is always best practice to check that assumptions are accurate before they are relied upon.

Where appropriate, get an impartial technical expert to review the evidence so they can give a second opinion.

3.3.6 Present summary of preliminary evidence to management

It is important to liaise with and present evidence to management at an early stage.. It is important to ensure that all parties understand what the object of the presentation is and the decisions that need to be made, such as:

- Whether there will be a full investigation
- Objectives/scope of the full investigation
- Whether to inform the authorities (e.g. police, regulators).

Care should be taken not to prejudice any future hearing by ensuring that those who may be responsible for hearing a disciplinary case are not involved in any such briefings.

3.3.7 Update the media management response

As there may now be a better indication of the impact of the incident on TRUST's reputation, the media response should be readdressed. The Corporate Services Manager should also reconsider the internal impact of the incident.

3.3.8 Plan the full investigation

It is essential at this stage to set out the objectives of the full investigation and plan its implementation. Care should be taken not to widen the scope of the investigation to cover areas where there has been a suspicion of wrongdoing in the past or where there are inter-related systems etc. as this may dissipate resources for little reward.

Keep the scope of evidence collection within defined bounds. Investigators should always be aware that people might sometimes use an incident as an opportunity to further any personal vendettas they might hold against others.

3.3.9 Notify authorities or other NHS bodies (if appropriate)

The decision whether to notify the authorities or other NHS bodies, such as the NHS Information Authority or the National Patient Safety Agency, will in most cases be decided when the evidence is presented to senior management and they can see the full implications of the incident. However, such decisions should be made not on the basis of Trust's opinions but rather on the reporting requirements incumbent upon them.

Where there is evidence of paedophilic images the Trust must report the incident immediate to the police, describing the circumstances of the investigation as failure to do so may leave the Trust open to prosecution for holding such images.

3.3.10 Re-assess the risk

From the analysis of the preliminary evidence it may be possible to identify control weaknesses that allowed the incident to occur. These control weaknesses should, in normal circumstances, be addressed quickly to prevent the incident occurring again. However, the implementation of additional controls could alert someone who is under observation and the risks should be assessed to decide whether they are acceptable.

Where possible the information should be shared with other areas of business to ensure they are not vulnerable, provided that it does not affect the investigation.

3.4 Formal Evidence Gathering

3.4.1 Context

This is the part of the process where the most detailed evidence is gathered together from all of the sources available, and in particular from computer systems and networks.

It is particularly important that any computer investigation should be conducted by a computer forensics specialist with a good knowledge of the systems under investigation. The Trust's internal auditors should be a first point of contact in such instances

3.4.2 Identify sources of evidence

Before starting to collect evidence it is important to identify the sources of evidence and the methods by which it may be obtained. This will help to establish the specialist resources that may be required and for how long. There are a number of steps that need to be taken in the management of incident evidence:

- Identification
- Preservation
- Recovery
- Analysis
- Presentation

3.4.3 Engage forensics skills (if required)

Where computer forensics expertise is required early contact should be made with Trust's internal auditors.

The internal auditors will facilitate the forensic examination, working with respected organisation in the security industry and within the NHS to undertake the imaging and analysis.

3.4.4 Gather and secure evidence

There are a number of disciplines that need to be applied to a detailed investigation and these should be part of a rigorous process for carrying out the tasks required for a successful investigation and possible prosecution. This is necessary because every case should be treated as if it is going to court because it may only be during analysis that the incident is identified as a crime.

It is essential to ensure that computer systems are not checked by enthusiastic amateurs, whether they are authorised or not, because even turning a machine on or off could destroy or contaminate data, which may otherwise prove the subject's guilt or innocence.

When carrying out a preliminary check of any data ensure it is done from an account with read only access. It is important to ensure that you have the right people doing the right job and use people who have the ability to access and recover potential evidence correctly, Data collection for Computer Forensics can be performed in two ways:

- Overtly – openly acquiring the equipment to be used in an investigation
- Covertly – allowing the activity to continue whilst gathering evidence and identifying the conspirators.

Wherever possible covert monitoring should always be considered in cases of employee misuse, to ease their return to work if the allegation is found to be untrue. Where an allegation of a policy breach is investigated, only sufficient evidence to support the case should b e captured and retained.

Evidence of employee misuse should be collected in the same manner as that for a criminal act, as at the outset it may not be clear which direction an investigation may take and other offences may come to light. It is also important that the non-IT sources of evidence are not overlooked as they might shed valuable light on what is happening.

When writing reports to be circulated within the organisation it is advisable to ensure that they are simple and technical terms are clearly defined.

As few people as possible should be involved, to prevent leakage of the evidence collection, and only people in the organisation that are known to be trusted should be informed of the progress of the investigation.

3.5 Analysis of Evidence

3.5.1 Context

This is where all of the available evidence is assessed for accuracy, quality and reliability and then set against the background of the incident so that the investigation team can identify what has happened in detail.

3.5.2 Produce and agree analysis plan

The way in which the evidence is analysed may depend on the type of incident involved, for example whether it is a policy breach or a criminal act. The way in which the evidence is treated should be determined at the beginning so that the appropriate level of rigour can be applied.

3.5.3 Execute analysis plan

The analysis of the evidence should proceed according to the analysis plan, although there should be sufficient flexibility to allow for exceptions.

3.5.4 Identify areas for further investigation

There will often be areas where the evidence is weak and a judgement will need to be made whether to seek more evidence or to rely on what is available, and to seek further evidence if a decision is made to prosecute.

3.5.5 Present evidence to management

When the evidence has been analysed it should be presented to senior managers for a decision to be taken on whether to proceed and in which direction. When presenting evidence to managers there is a possibility that they may not understand the technical intricacies of the process and/or the collection methods. Care should be taken to present evidence in a manner that is understandable to its audience but which is supported by appropriate technical information.

3.5.6 Inform the authorities

If a decision has not previously be taken as to whether to inform / involve the authorities or other HS bodies a decision should be taken at this stage.

3.6 Human Resources Action (where no legal action takes place)

3.6.1 Context

Where the preliminary investigation has obtained evidence of a breach of company policy or rules and legal action is either not appropriate or not considered to be the best way forwards, the HR function may be expected to take action in line with normal disciplinary procedures.

This section sets out where the incident management process supports HR in its disciplinary actions. It is not intend to replace the Trust's HR policies and procedures but rather to complement them.

3.6.2 Establish the chronological sequence of events

It s important to provide the HR function with a chronological sequence of events that led up to the incident, which may be established from the analysis of the preliminary evidence, The HR function should also have access to the investigation log so that the methods of securing the evidence are understood (in case o f appeal etc.) and so that it is also able to demonstrate (to employee representatives etc.) that the appropriate evidence has been collected.

3.6.3 Secure access to systems and evidence

Where the alleged perpetrator is still in on site, it is important to ensure that evidence cannot be destroyed before the interview with HR. During the interview with HR the IT function may be requested to secure all system access such as:

- Network access
- E-mail
- Privileged access
- Remote access
- Physical access.

It is important to ascertain whether the employee has access to a laptop, PDA or documents and organise their retrieval.

3.6.4 Present evidence to the individual(s)

The HR interview with the individual will be more productive if the investigation results are presented clearly and concisely, and steps have been taken to explain the implications of the suspect's actions.

This process should be undertaken in accord with the Trust's documented disciplinary processes.

3.7 Risk Management – Learning the Lessons

3.7.1 Context

This part of the process is where any control weaknesses that led to the incident are considered within an overall risk assessment and any new or alternative controls are implemented.

This is also where changes, based on experience, are made to the incident management process.

3.7.2 Identify actions required to mitigate risks

It is important that any control weaknesses that were discovered during the analysis of evidence should be documented and the appropriate controls identified.

An implementation plan may then be proposed to fill in the gaps in controls and manage the risks effectively.

3.7.3 Review and agree policy

Following the incident senior management should be encouraged to critically review the incident management policy to confirm that the current incident has not identified that there are deficiencies and that a change needs to be made.

3.7.4 Identify awareness raising activities

There is a possibility that the incident may be used as a warning to others as a part of an awareness programme, provided that appropriate safeguards concerning the subject's privacy and human rights are implemented.

Often an unofficial disclosure of an (sanitised) incident can have a positive effect in raising awareness.

3.7.5 Incident management process review

Following the conclusion of the incident investigation a post incident review of the incident management process should be held to identify what went right and what went wrong. This will often ensure that lessons learnt during the incident are fed into the incident management process and mean that the process may be better the next time.

3.7.6 Archive materials/evidence

The information collected during the process will need to be dealt with and often it will need to be retained for a certain length of time, either in case of a future appeal or for regulatory purposes.

It is important to create a secure archive of all of the material collected during the incident investigation and subsequent analyses, which is only available on a need to know basis. Retention periods of documents should be in accordance with NHS guidance and the Data Protection Act.

3.7.7 Re-instate user access/equipment

Where the incident has proven the subject to be innocent or where no further action is to be taken, the subject's access to systems and services should be resumed. However, a review of access rights may be necessary if they contributed to the incident.

Where action has been taken against the subject the equipment may need to be retained as evidence pending a court case or possible appeal.

3.7.8 Corporate risk register

It is intended that Information Security incidents should feed corporate incident reporting and as such all incidents will also be recorded in the corporate risk management system (which is outside of the scope of this ISMS)

4. Compliance

4.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

4.2 Review and Monitoring

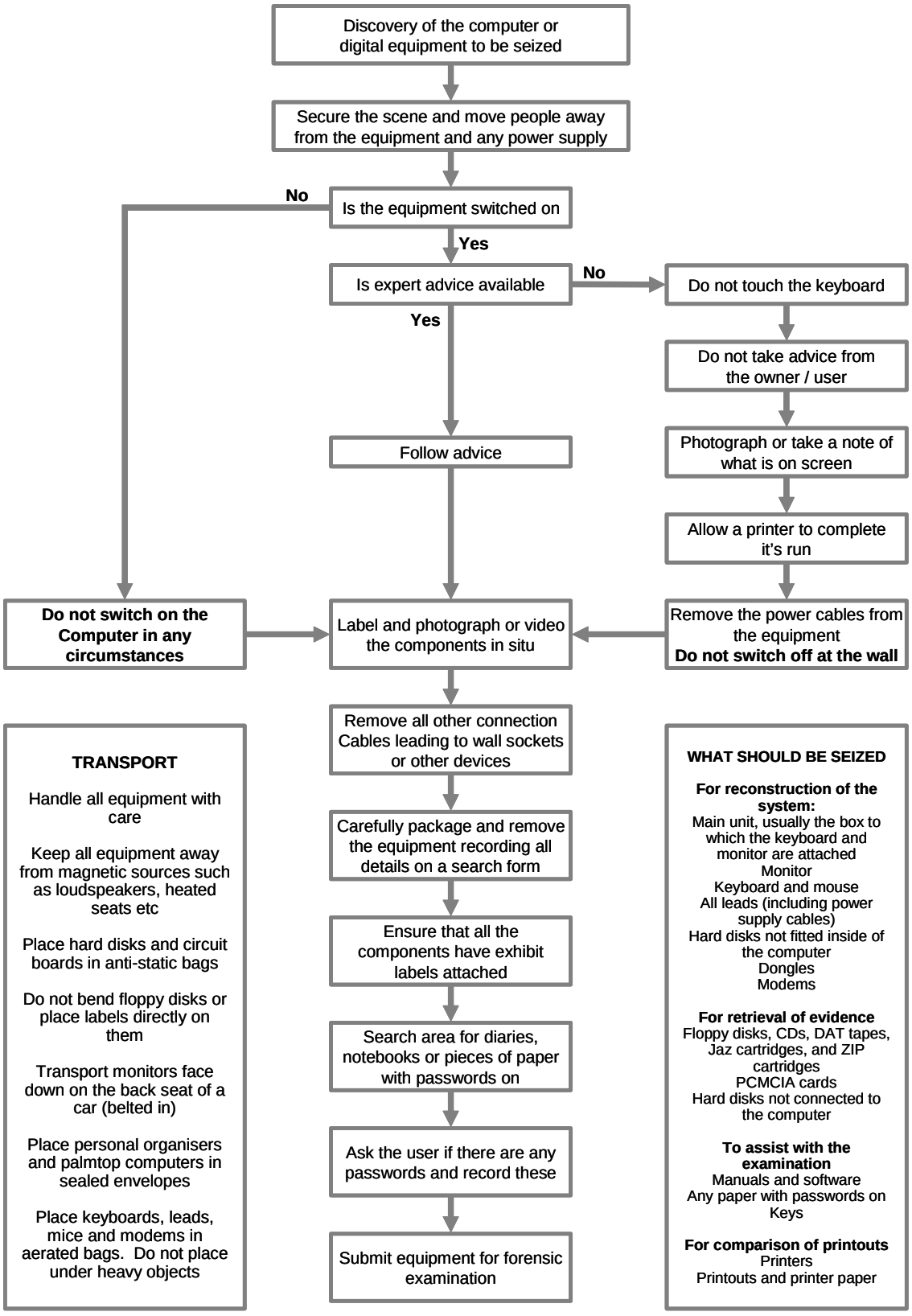
The Trust has in place routines to regularly audit compliance with this and other standards.

Appendix A

Best Practice Flow Diagram

Seizure of Electronic Evidence

Best Practice Flow Diagram Seizure of Electronic Evidence



Appendix B

Best Practice Flow Diagram

Seizure of Personal Digital Assistants

Best Practice Flow Diagram Seizure of Personal Digital Assistants