

HEIDS/J-LIS inappropriate use technical investigation process

This document describes an investigation process agreed by HEIDS members (www.heids.ac.uk). It has been compiled in partnership with the JISC Legal Information Service (J-LIS) (www.jisc.ac.uk/legal) and incorporates general guidance notes which set the background against which any process must operate.

This is the first version of the process and is intended to establish a basic framework for use in cases where investigation is likely to focus on desktop equipment. The process provides a starting point for handling the more common type of occurrence as well as providing a foundation on which to build a revised process appropriate for a wider range of circumstances.

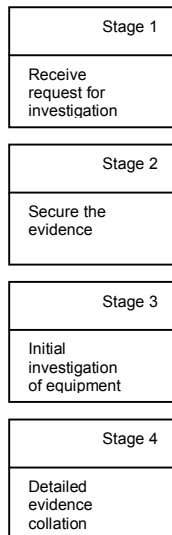
As indicated in the above paragraph, the document does not attempt to provide a prescription for every set of circumstances. A major aim has been to make significant progress towards clear guidance and a process but for a restricted but commonly applicable set of circumstances. That is, the process focuses on staff use of desktop PC equipment. Some general guidance on server related issues is also included. Because of the varied nature of organisations' technical infrastructure and the variety, range and extent of server based information, consideration is being given by HEIDS for a separate document for guidance on a process to apply in this area.

Contents

HEIDS/J-LIS INAPPROPRIATE USE TECHNICAL INVESTIGATION PROCESS.....	1
OVERVIEW OF PROCESS.....	2
Stage 1 – Receive request for investigation	3
Stage 2 – Secure the evidence	3
Stage 3 – Initial investigation of equipment	3
Stage 4 – Detailed evidence collation	4
APPENDICES	4
Stage 1 - Receive request for investigation.....	4
Stage 2 – Secure the evidence	9
Stage 3 – Initial investigation of equipment	10
Stage 4 – Detailed evidence collation and reporting	12
Example of areas for investigation	13
Use of specialist forensic investigation services	14
Summary of ACPO guidelines on evidence collection.....	15
ACPO Principles	15
OVERVIEW FROM J-LIS OF THE LEGAL ISSUES TO BE CONSIDERED.....	16
Inappropriate Use	16
Legal issues	16
Resourcing Issues.....	18
Human Resource Issues.....	18
Conclusion	19

Overview of process

A four-stage process is proposed as illustrated in the following diagram. Each of the stages is described in more detail in the corresponding appendix.



A characteristic of the process is that for various reasons, it may terminate at the end of any one of the stages depending on the outcome of the stage and decisions outside the IT investigation. That is, the process model described is intended to fit within a wider institutional investigation process. This wider process is not under consideration here although some assumptions are made. For example, that there is an appropriate mechanism for authorising investigation and that the need for separating technical investigation and judgement roles is accepted.

Due to the increasing likelihood of investigations resulting in court actions, the process adopts best-practice advice on evidence collection from the outset. There is an overriding need to maintain the chain of custody and to document any investigation so that it can be defended if challenged in court. The recommendations of the Association of Chief Police Officers (ACPO) are summarised in an appendix to this document. The ACPO guide is available as a download at the web site of the National high Tech Crime Unit (<http://www.nhtcu.org/>).

The following definition of evidence recovery staff from the ACPO good practice guide indicates some of the issues -

Evidence recovery staff

Recovery and reproduction of seized computer based electronic evidence by personnel who are trained to carry out the function and have the relevant training to give evidence in court of their actions. Persons who have not received the appropriate training, and are unable to comply with the principles, must not carry out this category of activity.

This means that throughout the process, activities must be handled in a very formal manner. This is the only way in which the integrity of the overall process can be safeguarded. This is a particularly important issue for those technical staff who may be involved in implementing the process. Without the safeguard of the formal process and application of best-practice advice, it is those staff who are at risk in possible subsequent events such as legal action arising out of misuse, criminal prosecution or unfair dismissal actions. That is, investigators should be aware that they need to be prepared to stand up in court and have their actions questioned.

Throughout this document, it may appear that the use of external specialist agencies is encouraged. This emphasis arises out of a pragmatic view with regard to available resources. Institutions might handle all aspects of an investigation themselves but would be advised to ensure that appropriate training is provided to staff and that specialist tools are purchased in order to reduce the overall resource requirement. That is, institutions are able to follow the recommendations of the ACPO good practice guide.

One of the objectives in describing the overall process in the above stages is to help to separate and clarify the roles and responsibilities of professional IT staff. In this way guidance, including training, can be provided to such staff. Of particular concern is that such staff are alert to the possible risks to themselves as well as to the institution. It is considered essential that such staff do not inadvertently become drawn unnecessarily into activities and issues not directly related to their primary roles and responsibilities.

Throughout the process, written records should be maintained. One of the aims in providing this process guidance is to provide with it, a framework for that written documentation. Within the appendices of this document are templates for the recommended documentation for each stage of the process.

Stage 1 – Receive request for investigation

The process commences with a request for investigation. No attempt has been made to define such requests which may be many and varied as well as being subject to institutional variation. For those involved in the investigation the key issue is that they receive a clear written request for initialising an investigation for which an explicit scope is defined. It is an important aspect of stage 1 that investigators are clear as to the extent of the requested investigation and that they do not incur risks in relation to legislation such as the Human Rights Act, RIPA or the Data Protection Act.

The initial request authorises the technical investigation process to proceed through stages 1 and 2. Stages 3 and 4 are authorised by updating the form created in Stage 1. Note that organisations will need to clarify who is the appropriate signatory. It is recommended that this should be the most senior administrative officer of the organisation with responsibility for legal and contractual matters.

In a typical institution such requests might arise through departmental channels, via Human Resources or directly or indirectly through senior management of the IT function. This is an area that individuals may wish to clarify within their own institutions. All requests to individual staff within the IT function should come via designated IT management staff such as the IT Director or their Depute.

Stage 2 – Secure the evidence

The word evidence does not imply guilt of a particular individual. The evidence may prove innocence rather than guilt and identify that accusations were falsely made, perhaps leading to disciplinary action of a different individual. Therefore it is essential that evidence is not compromised in any way.

The main objective is to secure equipment in a way in which minimises the risk of subsequent doubt as to basic use and access to the equipment following notification of a request for investigation. By ensuring that equipment is quarantined in a fair and impartial manner, all parties are protected and a 'breathing space' is provided for the overall investigation.

It is likely that other information should also be secured at this stage such as proxy logs and accounts suspended such as email. This initial version of the process concentrates on the activities associated with desktop equipment and provides only generic guidance on securing other sources of information.

Stage 3 – Initial investigation of equipment

The main objective of this stage is to establish whether or not there is the basis for a further more detailed collection of evidence. That is, the initial investigation is concerned with examining a wide range of technical information sources to detect evidence of misuse. Specialist tools exist to assist with this task and external specialist services might be used to perform such investigation. For many institutions this might be the most cost-effective option.

This stage of the process is halted immediately on discovery of material of a criminal nature such as child pornography and the investigation handed over to the Police.

Stage 4 – Detailed evidence collation

The main objective is to provide the institution process with an independent report on the evidence audit of the equipment and associated activity to admissible evidence standards. This may mean the collation of a considerable amount of material including images. By this stage the institution is likely to have invested a considerable amount of time and effort into the investigation. The likelihood of subsequent use of evidence has increased along with the associated risks to individuals and the institutions. The stakes are high.

Although specialist tools exist to assist with this task, for most institutions it is recommended that external specialist services are used to perform such investigation. For most institutions this is likely to be the most cost-effective option as well as helping to reduce some of the risks inherent with operating a complex process infrequently.

In situations where an organisation considers it desirable to carry out the investigation internally, it may still be advisable to use an external agency to secure the evidence, thereby minimising risks in this area. Similarly, such organisations might wish to consider arrangements for formal training programmes and purchase of specialist software in order to underpin their internal process. Consortium approaches to these aspects might also be considered.

This stage of the process is halted immediately on discovery of material of a criminal nature such as child pornography and the investigation handed over to the Police.

Appendices

Stage 1 - Receive request for investigation

Description: To record receipt of a request for investigation. To ensure that the scope of the requested investigation is accurately recorded. To consider what actions will be necessary as part of stage 2. To record agreement to proceed to subsequent stages.

Four forms are provided; the first provides a record of the receipt and the scope of the investigation; the second identifies the equipment and services to be investigated during stage 2; a third form is used for recording communications relating to the case and a fourth records all actions taken.

Objectives: To ensure an accurate record of the request for investigation, including at subsequent stages. To ensure an accurate record of the scope of the requested investigation. To identify what equipment needs to be secured as part of stage 2. To minimise the risks associated with breaches of existing legislation.

Resources: Two senior IT staff should be designated with one being identified as the Principal Investigator. The Principal Investigator is responsible for establishing and updating appropriate paperwork and retaining this in a secure manner.

Process: The process is described on the accompanying forms.

Hence, complete form 1
 complete form 2
 complete form 3
 complete form 4

Notes: Form 1 includes a section to record the subsequent agreement to proceed to stages 3 and 4. These should be signed by the University Officer with overall responsibility for the investigation. Any subsequent correspondence relating to proceeding to stages 3 and 4 should be retained with form 1.

Strictly Confidential**Stage 1 – Receive request for investigation**

Identify Equipment/Services Used	Ref:	Form 2	
<i>Equipment/Services identification:</i> Check records to identify any equipment and core services known to be used by the individual. Unique identifiers include serial numbers, network IP addresses and user account names.			
Item Ref	Item	Unique Identifier	Location

This form is used as the basis for work authorised under stage 2.

Strictly Confidential

Communications Record		Ref:		Form 3
Date/time	Description	By	Notes	
	Receipt of request for investigation			

Strictly Confidential

Actions Record		Ref:	Page:	Form 4
Date/time	Item Ref	Detailed Description	Witness 1 (sign)	Witness 2 (sign)

Stage 2 – Secure the evidence

Description: To secure desktop equipment according to best-practice guidelines for evidence collection, thereby ensuring no compromise of audit trail from initial notification.

Process: The two designated investigators should be present when the activity is carried out and a record is made of the event by completion of form 4. Where there is more than one item of equipment, the process is repeated for each item.

If equipment is switched on it is not shut down or otherwise accessed – the power is shut off by unplugging the computer at the computer end of the lead, not at the wall (in case of UPS device being present).

Desktop equipment is 'bagged and tagged'. Evidence bags and evidential seals should be used. The unique reference number on the seal should be noted on the form 4 and signed by both investigators by way of confirmation.

On completion of this stage, a breathing space is provided for the investigation process. This is important as the work carried out to date may reveal issues relevant to the overall investigation. For example, matters relating to access of equipment, relationships between individuals associated with the investigation and other risks relevant to the investigation.

Note: It is likely that there may be other server-based information that should also be secured at this stage. Due to the range of infrastructure environments that are likely to be found across institutions, including ancillary log records as well as user maintained file store, no attempt is made within this process to define specific steps for securing evidence etc.

To enable such sources of information to be identified it is necessary to identify any server based storage on which the user has the ability to directly or indirectly store information. This may be a considerable list and will include obvious sources such as home directory file-stores, email servers and also less obvious sources such as web servers and other networked equipment to which the user has some form of write access.

Other server-based information that should be secured might include proxy server logs, web access logging software and other sources of transient records.

Routine backups are may be sufficient and it is appropriate to make separate copies. These should be secured in an identical way as the desktop equipment. That is they should be bagged and tagged and two designated investigators should be present when the activity is carried out. For practical purposes it is likely that an additional individual may be required to provide technical guidance on obtaining the backup thus extending the team of designated individuals. A record should be made of each event by completion of form 4.

Any work that is carried out of a specialist nature, particularly that relating to potential evidence, should be carried out by appropriately trained evidence recovery staff.

Stage 3 – Initial investigation of equipment

Description: This stage is concerned with identification of the existence of any evidence of inappropriate use. The appendix *Example of areas for investigation* provides some indication of the considerable amount of work that may be necessary to assess whether there is any indication of inappropriate use. This stage does not go into the detailed investigation of such indications of evidence but is still likely to be a significant work requirement.

In order to maintain best-practice in evidence collection, any investigation of digital media must take place on a copy of the medium, not the original. Also, the copy must be taken in such a way as to make the least possible change to the original. For example, any inadvertent change to file access dates on the original represents an evidence disaster. Carrying out and documenting the copying process should be done to an agreed standard in which staff are properly trained.

Thus there is likely to be considerable work requirement and there are risks in the technical process. For these reasons it is recommended that external specialist forensic services are considered. As well as being cost-effective it is likely to be more comprehensive and less open to accusations such as conflict of interest than an internally resourced technical investigation.

A key requirement at this stage is to confirm the investigation requirements. This might be done by exchange of correspondence and may vary from case to case. Typical examples might include “to provide a summary of the material on this equipment by an inspection of the live and deleted files”; “to obtain a statement of the internet related activities carried out on this computer by reference to history files, temporary files and other internet access records”. Form 1 should be used to record authority to proceed with the stage and Form 3 should be used to record the receipt of agreed requirements.

Objectives: The main objectives of this stage are to ensure that best practice evidence gathering guidance is adhered to in any initial investigation. Also, to identify whether there is the basis for further more detailed investigation.

Notes: It is important that the initial technical investigation fits with the institutional process and vice versa. That is, there is no scope for reinvention of the investigation process for each use of the overall institutional process. It is imperative that the third stage is not compromised by activities at this stage.

There are a number of issues that need to be considered in choosing how to handle the work at this stage. There is the obvious choice of whether to resource internally or use external services. It is arguable that maintaining confidentiality is more likely through the use of external services than if work is handled internally. For example, for the work to be carried out internally a secure location must be found, two senior staff must be involved and the work is likely to continue for some considerable time. The purchase of specialist tools might be considered but these are expensive. Thus, the very time consuming nature and the fact that two key staff will be otherwise occupied draws attention to the fact that something is going on.

Other issues that may become of concern at this stage are relationships between individual members of staff and the proximity of those carrying out the investigation to those being investigated.

In order to be consistent and fair with the investigation process, incidents should ideally be handled in an identical way. This is very much more difficult to achieve if matters are handled internally due to availability of staff and also there may be the temptation to tailor the investigation to the case in an effort to reduce the resource load.

As there always remains the possibility that investigations will discover something that leads to legal action, adherence to best practice evidence-gathering guidelines is imperative. For many institutions it may be difficult to justify the additional resource load, including training, etc, that this imposes when external services are readily available.

Stage 4 – Detailed evidence collation and reporting

Description: This stage provides the institution process with an independent report on the detailed evidence audit of the equipment and associated activity to admissible evidence standards.

This is likely to require a considerable work effort and may not even be feasible without the availability of specialist tools. For example, there may be hundreds if not thousands of files to be inspected and this may mean the collation of a considerable amount of material including images.

As with stage 3, there is a need to confirm the investigation requirements. This might be done by exchange of correspondence and may vary from case to case. It is recommended that institutions should be guided in the formulation of such statements by the service statements provided through specialist forensic investigation services or their own legal advisers.

Form 1 should be used to record authority to proceed with the stage and Form 3 should be used to record the receipt of agreed requirements.

Objectives: The primary objective is to provide the organisation with an independent detailed report on evidence audit of equipment and activity to admissible evidence standards

Notes: The arguments in favour of the use of external services, as described under the section on Stage 3, are overwhelming for this stage of the work. There is an increased likelihood of the use of evidence as the work is progressed to this stage. This increases the likelihood of the involvement of IT staff in proceedings and there will have been a considerable investment by the institution in the process to date. It is therefore imperative that risks are reduced and for most organisations this may be achieved through the use of external services.

Example of areas for investigation

Specific information requirements

Equipment specification and operating system

External devices configured such as modem, zip drives, etc.

User account information

Network configuration (IP address)

Internet configuration (proxy server or automatic configuration script)

Full internet history including deleted history and criteria entered in search engines

A time-line analysis of activity leading up to date of incident

A time-line analysis of activity from date of incident

Software installed, particularly anything that allows:

- IP tunnelling
- Remote access, eg pcAnyWhere
- Internet chat
- Hacking
- Password cracking
- Keystroke capturing
- Network sniffers
- Port scanners
- Denial of service tools
- Cleaning internet activity
- Permanently erasing deleted files
- File timestamp changes
- Any other suspicious software

Suspicious files and their ownership including:

- Image files
- Audio files
- Movie files
- Files with obscene names

Files and their ownership containing a defined list of keywords

More general information:

- Activity or material relating to possession, making or distribution of child pornography
- Activity or material of an adult nature
- Activity of a discriminatory nature (i.e., sexist, racist, general bullying of other staff)
- Activity or material of a criminal or unethical nature
- Activity or material pertaining to any other digital threat
- Activity or material with potential risk to the University's business
- Activity or material in violation with University policies
- Suspicious internet activity
- Suspicious data (data not authorised to hold)
- Operation of undisclosed private business activities
- Digital piracy
- Evidence of time wasting

Use of specialist forensic investigation services

Benefits in using a specialist forensic investigation service

Independent

Total confidentiality

Procedures strictly in line with legal requirements – evidence admissible in a court of law

Maintain evidential integrity of data throughout

Clear message to staff that misuse will be fully investigated in a proper and legally sound manner

If equipment is found to be clean this is beyond any doubt, i.e. may prove innocence rather than guilt

Issues/risks in not using a specialist forensic investigation service, i.e. using internal staff only

Negative publicity

Assumptions made that those conducting the investigation are not involved

Assumptions made that those conducting the investigation will not favour the suspect

Assumptions made that those conducting the investigation will not discriminate against the suspect

University open to accusations on the above assumptions

Investigating staff open to accusations on the above assumptions

No resource to conduct investigation in a proper and legally sound manner

No resource to capture, preserve and easily manage large numbers of relevant files, including deleted files, file slack and unallocated space

No resource to recover a full internet history including deleted history and criteria entered in search engines

No resource to produce a time-line analysis to define the sequence of events

No trained internal staff

Impossible to maintain evidential integrity of data

Doubt can still exist over equipment that appears clean

Very time consuming to manually investigate equipment with all other work by those involved having to stop for several days

Summary of ACPO guidelines on evidence collection

ACPO Principles

Principle 1

- No action taken by the Police or their agents should change the data held on a computer or other media
- Where possible computer data must be 'copied' and that version examined

Principle 2

- In exceptional circumstances it may be necessary to access the original data held on a target computer
- However it is imperative that the person doing so is competent and can account for their actions

Principle 3

- An audit trail must exist to show all the processes undertaken when examining computer data

Principle 4

- The onus rests with the person in charge of the case to show that a computer has been correctly examined in accordance with the law and accepted practice

Overview from J-LIS of the legal issues to be considered.

Prior to a procedure on the steps to be taken in conducting an investigation, it is essential that the legal implications involved in such an investigation are considered.

The issues highlighted below may aid in general risk assessment and inform the procedures most appropriate for a particular institution as outlined in the investigation process guidelines. However, it should be stressed that the material below is for general informational purposes only. It is recommended that an institution should always seek professional legal advice on specific issues of concern when assessing its own risks.

Inappropriate Use

Inappropriate use of an institution's computer facilities (restricted to desktops for this phase of the guidelines) is divided essentially into two main areas; illegal activity and activity in breach of institutional regulations.

Illegal Activity

The most serious examples of criminal illegal activity are the possession of child pornography, or downloading of pornographic or obscene materials for distribution. These are serious criminal offences, investigation of which must necessarily involve the police not least of all to protect other institution staff and students as well as the institution from the risk of any criminal liability falling on them.

Defamation, and breaches of discrimination legislation may also occur through the circulation of, for example, inappropriate email.

Offences perhaps viewed as less serious by society in general include use of unlicensed software and P2P music downloading involving breach of copyright. These offences involving breach of copyright law have to date not usually been prosecuted in the criminal courts (unless it has involved large scale piracy and sale) and usually incur civil rather than criminal liability. However, the outcome of a breach of copyright law can result in substantial financial loss to an institution as well as damage to its reputation.

Activity in Breach of an Institution's Regulations

Examples of such breaches which an institution might wish to investigate include excessive personal use of email, exchange of 'offensive' email, and viewing pornographic materials in privacy of own office.

Another area of concern for employers is that they may also be held vicariously liable in a court of law for the actions of their employees and may therefore wish to investigate breaches of the obligation of confidentiality or investigate whether, as a result of an employees action, the institution has entered into a contract with a third party.

These activities may not necessarily involve illegal activity, but may involve an institution in internal disciplinary proceedings ultimately resulting in dismissal of an employee. In the litigious society of today this will necessarily require the gathering of evidence which can be confidently presented at such proceedings

In all of the above, legal issues, resource issues and HR issues intertwine when considering what policies and procedures an institution should have in place to investigate this activity.

Legal issues

Criminal Law

The most emotive and potentially damaging investigation for both the investigator and the institution which may have to be carried out is undoubtedly an investigation into child pornography either found on a desktop or alleged to exist there.

If child pornography or obscene materials are found, there is no option but to involve the police. Due to the nature of the crime an institution and its IT department also needs to consider whether anything beyond a superficial investigation is advisable. Current law affecting institutions in Scotland with regard to child pornography is to be found in the Civic Government (Scotland) Act 1982 s 52 and 52A (the Protection of Children Act 1978 is the relevant legislation for the rest of the UK). The current wording of the legislation presents a dilemma for institutions and their investigation teams.

This states that

'any person who ... makes any indecent photograph or is in possession of an indecent photograph or pseudo photograph of a child is guilty of a criminal offence.'

In strict legal terms this means that if an investigator looks at the images on a desktop he is, according to the letter of the law, technically committing a criminal offence. If when investigating he 'makes' a photograph by copying to preserve the evidence he is committing a criminal offence. There is a defence in law of 'legitimate reason' but the damage may very well have been done before getting to the stage of having to defend a course of action.

The logical extension of this is that an institution, in asking that an IT Director or other employee investigates an alleged instance of child pornography, may find itself effectively asking him to unwittingly commit a criminal offence in the course of such an investigation. Although the police have stated that in such circumstances it is highly unlikely that there would be a prosecution, the fact remains that in strict terms of current criminal law a breach has been committed and a risk of prosecution exists.

There is currently an added problem, certainly for those institutions based in England and Wales, in that The Sexual Offences Bill 2003 proposes that it is not an offence to 'make' a photograph if you have been authorised to do so (by the police). The implication is that if you have not been authorised you must not investigate. This Bill is a result of the Government's desire, given the publicity surrounding Operation Ore, to have a robust policy with regard to crimes against children. If the Bill becomes law, as presently drafted, any investigation without authorisation will be a criminal offence. It is currently under review and hopefully lobbying will result in an amendment to the Bill. Although this proposal does not apply to Scotland it could reasonably be expected that similar legislation would be enacted here.

Employment Law

The whole area of using staff to investigate computer misuse by its very nature involves Employment Law and an institution would be well advised to ensure that heed is paid to the requirements of this specialised area of the law.

An institution has a duty of care towards its staff, students, and also third parties which must be considered when developing guidelines for investigating misuse. Some of the law is entrenched in Health and Safety, Employers Liability and Anti-discrimination legislation. Institutions as employers must also be aware that they can be held vicariously liable for the actions of their employees, for example, in concluding contracts and in breaches of confidentiality. It is essential that, as a minimum, an institution ensures that its investigation procedures for computer misuse fit with the institution's other disciplinary guidelines and procedures. Best practice indicates that all requests to investigate should be authorised centrally at a high level and should always be recorded. Practice and procedures for computer misuse investigations must be robust enough to withstand allegations of discrimination, victimisation, and unfair dismissal.

The staff involved in such an investigation may ultimately be required to appear in court or at a tribunal and this possibility must inform an institution when considering appropriate staff to carry out such an investigation. Employers' liability for the health and safety of the investigators is a consideration. These issues may become highlighted in a smaller institution where there is an increased risk that the internal investigators may necessarily be close colleagues of the alleged offender.

Data Protection, Monitoring, and Human Rights

Data protection requirements are important to bear in mind when investigating misuse, especially when investigating without the knowledge of the employee or the student. The Information Commissioner has issued an Employment Code of Practice (Part 3) on monitoring in the workplace

which should be consulted prior to introducing guidelines. It should also be remembered that an individual may make a subject access request under the Data Protection Act for all information being held on him. It is therefore essential that any investigation into computer misuse must pay heed to current legislation regarding monitoring as laid down in the Regulation of Investigatory Powers Act 2000 and subsequent regulations and also that it does not breach the principles of the Human Rights Act 1998.

Law of Evidence

Any evidence gleaned from an investigation must be robust enough to withstand cross-examination and also conform to current admissibility rules. This is not only important when investigating criminal activity but also other misuse activity which may result in disciplinary proceedings ultimately culminating in a claim for unfair dismissal and an appeal to an employment tribunal. The integrity of the evidence gathered is both important to the police in a criminal investigation but also to the institution in an internal disciplinary enquiry. There is an international standard on Legal Admissibility and Evidential Weight of Information Stored Electronically (PD 0008) which sets out the current standards. As the information is stored electronically, and therefore may result in more opportunity for tampering, evidence gathering standards may need to be higher than for paper documents and the person responsible for the computer system and its activities may also be required to state in court that the institution's system itself was operating properly.

We are working in an increasingly litigious society where inadequate standards are frequently and increasingly challenged. It is no longer unusual for a student to have legal representation at an internal disciplinary hearing. Evidence gathered regarding misuse must be robust enough to withstand challenge.

Resourcing Issues

Investigating a breach of university regulations necessarily ties up resources. Due to the potential nature of the 'find', best practice would indicate that the investigator should be a senior member of staff, for example an IT Director who would by the very nature of his position be better placed to handle the outcome of an investigation and involvement in any subsequent proceedings. For the protection of the investigator and of the evidence, an observer should also verify all of his actions.

This may have an impact on the working of IT Services, especially in a smaller institution, and institutions need to consider whether in fact it may be more cost effective to use external forensic investigators. This may have the advantage of ensuring the integrity of the investigation but will have the disadvantage of alerting a wider audience at the allegation stage. However, if the institution promotes this as its standard policy it may have the positive effect of showing the seriousness with which a potential incident is treated and may act as a deterrent.

Investigation of a computer's files by very nature of the technology requires great skill. This is a specialised area which can rapidly develop into a complicated time consuming task and which it may be worth considering whether your staff have the necessary skills to undertake.

Human Resource Issues

These have been referred to above under Employment law but it is worth reiterating from a liability and human perspective, that an institution must consider the welfare of its staff and the position in which they may be placed. It is understood that in practice currently many breaches of acceptable use are carried out by IT services staff and again the means and integrity of the subsequent investigation and impact on staff, especially in a small team, should be considered.

It will also be necessary to ensure that computer misuse investigation procedures fit in with other university procedures and guidelines for example regarding independence and transparency. There may also be union agreements on investigation procedures to consider. The input of the institution's HR department is therefore advisable before drawing up or adopting investigatory guidelines. It is also advisable that contact is made with the local police force to ascertain their approach.

Conclusion

Legal, financial and human resource issues cannot be separated in dealing with computer investigations. The nature of the technology ensures that an investigation can be complicated, lengthy, and fraught with difficulties in evidence gathering and preservation. This may take its toll on staff. Guidelines which have institution wide support are essential to support both the investigators and the alleged perpetrators of computer misuse as well as the institution itself.

Useful Sources of Information

<http://www.jisc.ac.uk/legal/>: JISC Legal Information Service – FE/HE sector specific information on the legal implications of the use of ICT

<http://www.masons.com/> and <http://www.out-law.com/>: general information including guidance on Internet and e-mail policies and privacy guidance

<http://www.dataprotection.gov.uk/index.htm> :The UK Information Commissioner’s website for basic information including the Code of Practice, Employment Part 3 Monitoring at work

<http://www.nhtcu.org/>: ACPO Good Practice Guide for Computer based Electronic Evidence

<http://armed.ilt.bris.ac.uk/>: ARMED – Active Risk Management in Education – the unit titled ‘Student computer use’

<http://www.bsi-global.com/Ways+to+Purchase/BSOL/index.xalter> BSI website which has the standard PD 0008:1999 - A code of practice for Legal Admissibility and Evidential Weight of Information Stored Electronically available to purchase

<http://www.hmso.gov.uk/> : some of the legislation referred to is available on line here.

Acknowledgement

The authors would like to thank Louise Townsend of Masons solicitors and Andrew Cormack of UKERNA for their helpful comments in the preparation of this document.

Copyright

The right of Higher Education Information Directors in Scotland (HEIDS) and the JISC Legal Information Service to be identified as the corporate authors of this work is asserted under the Copyright, Designs and Patents Act 1988. Any UK publicly-funded organisation is welcome to copy or adapt all or part of this work provided that acknowledgement is made to HEIDS/JISC Legal Information Service as the original creator of the work.

© HEIDS and JISC Legal Information Service 2004