Guidelines for Handling Illegal Material

Occasionally, organisations may have to deal with allegations of serious misuse of computers, where indecent images of children (as defined by the Protection of Children Act 1978 [1] and subsequent amendments) or extreme pornographic images (as defined by section 63 of the *Criminal Justice and Immigration Act 2008* [2]) may be present on the organisation's computers. The possession of such images is a serious criminal offence and must be reported to the Police as soon as possible. Until the material can be handed to the Police, organisations need to act very carefully to avoid harm to their users or potential criminal liability for the organisation or its staff. JANET(UK) has developed the following Guidelines, with assistance from JANET sites and the Home Office, to assist sites in this situation. General information on investigating computers [3] is available elsewhere on this website.

NOTE: Names in this document are deliberately left within square brackets so that the relevant organisations - universities, colleges, research councils etc. - and departments can fill in their own details for internal circulation.

Introduction

These guidelines are intended to help and protect computer support staff who may be requested by [the University] to respond to reports of the presence of illegal images (whether indecent images of children or extreme pornographic images) on computers at [the University of Erewhon]. The Protection of Children Act 1978 and subsequent legislation makes the possession, making or publishing of indecent images of children a serious criminal offence; the *Criminal Justice and Immigration Act 2008* introduces a similar crime of possession of extreme pornographic images. Images of either type must be reported to the police as soon as possible, with the minimum interference, for them to investigate. However, there may occasionally be an urgent requirement to confirm an allegation, to secure evidence or to remove material from view, and in these cases authorised site staff may be best placed to do the minimum necessary to achieve this. Any such action, and any information obtained as a result, must be handled in strict confidence both to protect the evidence and those persons involved: malicious allegations have sometimes been made against innocent parties.

Viewing or handling indecent images of children will normally be a serious criminal offence. However, section 46 of the Sexual Offences Act 2003 provides a limited defence for those who can prove that they needed to do so for the purposes of the prevention, detection or investigation of crime. The CPS (Crown Prosecution Service) and ACPO (the Association of Chief Police Officers) have agreed an MoU (Memorandum of Understanding) setting out the factors they will consider when deciding whether this defence may be available in any specific case.

The *Sexual Offences Act 2003* is available at: http://www.legislation.gov.uk/ukpga/2003/42/contents [4]

The MoU is available at: https://www.cps.gov.uk/publication/memorandum-understanding-between-crown-prosecution-service-cps-and-association-chief [5]

Sections 63 and 68 and Schedule 14 of the *Criminal Justice and Immigration Act 2008* provide a similar "good reason" defence to possession of extreme pornographic images and it is expected that this would be subject to similar tests.

The *Criminal Justice and Immigration Act 2008* is available at: http://www.legislation.gov.uk/ukpga/2008/4/contents [6]

Staff who have been properly authorised and instructed to respond to reports of the presence of illegal images and who satisfy all the tests should not have to fear that they will be prosecuted. The MoU recommends that organisations adopt written procedures for such activities to protect their staff.

These guidelines set out a procedure that is believed to be in accordance with the ACPO/CPS Memorandum of Understanding. Following this procedure should therefore give authorised staff some protection against prosecution by demonstrating that they have acted reasonably and professionally (MoU principle 5).

Principles for Dealing with Illegal Material

The guidelines aim to implement the following essential principles:

- The police are the appropriate people to be investigating serious crimes.
- The risk of exposing users and staff to potentially harmful material must be minimised.
- As little damage as possible should be done to any evidence of criminal activity.

Therefore:

- Allegations of the presence of illegal material on systems connected to the [university] network must be reported to and dealt with by authorised staff as soon as possible (MoU principles 1 and 2).
- As soon as the likely presence of such material is confirmed, the matter must be handed to the police with the minimum delay, with the evidence in the best condition that can be achieved (MoU principles 3 and 4).
- These guidelines must be followed, or any departure from them documented with reasons for doing so, to demonstrate that staff have acted responsibly and professionally (MoU principle 5).

Rules for staff

The basic rules for staff when dealing with illegal materials are:

- Staff must only act when they have been given specific written authorisation by [computing service management] and in accordance with that authorisation and this procedure.
- The role of the organisation's staff is only to confirm the presence of illegal material, to prevent further access to the material and to do the least possible damage to evidence.
- Staff must report to the police as soon as the presence of illegal material is confirmed and must follow the directions of the police thereafter. The police should normally be contacted by a member of the [computing service management], but if they are not available then the police should be called direct and management informed as soon as possible.
- If any delay threatens the organisation's response to the report then the matter must be handed to the police immediately.
- Any information obtained as a result of actions under these guidelines must be treated as strictly confidential.

Stages in the Process

1) Receive report

Any report or allegation of the presence of illegal material on a [university] system must be immediately recorded in writing and passed to a member of [computing service management]. Only they can authorise further action. The written record must include how the presence of the material was detected: in particular staff must never proactively seek out illegal material.

Do not start an investigation without authorisation from [computing service management]. Authorisation will be given in writing. In particular, do not investigate an allegation on your own.

Normally, management will report the matter directly to the police and be guided by them in all further activities. If a member of [computing service management] is not available, call the police and inform [computing service management] as soon as possible. The contact for [the University] is the Police Liaison Officer who can be reached by phone on [NNNN]. Reports of material elsewhere on the Internet, for example on public websites, should normally be passed to the Internet Watch Foundation: http://www.iwf.org.uk [7]

2) Obtain written authorisation (MoU principle 1)

The only situation involving illegal material that need not be immediately reported to the police is where there has been an unverified allegation that a member of the organisation has been accessing such material. Unfortunately there have been cases where such allegations have been made falsely and maliciously. If there is real doubt over the accuracy of a report, [computing service management] may need to authorise appropriately skilled members of staff to perform the minimum checks necessary to confirm the presence of such material on [university] systems or elsewhere.

If you are authorised to deal with an allegation, you will be informed in writing by a member of [computing service management]. The authorisation should identify you, and the authorising manager, by name and job title. All actions to deal with the allegation must always be

performed by two authorised staff working together.

As soon as it seems likely that illegal material is present, this must be reported to [computing service management] for them to contact the police. No further investigation must be done unless authorised by the police and then following their instructions to the letter. Staff must not attempt to identify how material came to be on the system, or which users may have accessed it, as doing so is almost certain to damage the credibility of evidence that may need to be presented in court.

3) Perform minimum checks needed to confirm the presence of material (MoU principles 3 and 4)

The purpose of the organisation's actions is only to confirm whether illegal material is likely to be present on a computer. This should involve the least possible handling of computer files and disks, both to reduce the risk of exposing staff to harmful material and to do the least possible damage to evidence.

Every action taken must be recorded in writing (ink, not electronic), with every mouse click, command or URL recorded. Where a complex command needs to be recorded this may be printed out in addition to writing it down but the printout must be signed and dated immediately and inserted into the written record.

Two staff must be present at all times. Both must sign and date every sheet of the record. If possible they should also initial each entry in the record.

If possible, these checks should be performed with the computer disconnected from all networks, to prevent external interference.

Often, checking a list of filenames or URLs visited will be sufficient to confirm suspicions: viewing files or visiting websites should be regarded as an absolute last resort. If it is necessary to visit a suspect web site then this should be done with a text-only browser, or at least with all image downloads turned off (ensure you know how to do this before starting the investigation). The text or filenames of a site will often indicate the nature of the content.

As soon as evidence of the presence or absence of illegal material is found, stop any further actions and report to the member of [computing service management] who gave the original authorisation.

4) Protect evidence (MoU principles 3 and 4)

The most effective way to protect evidence is to remove power from the computer on which the illegal material is stored (pull the power lead out of the back of the computer, not the mains socket: do not perform a shutdown as this may overwrite evidence).

If, however, the computer cannot be taken out of service for an indefinite period then a backup copy of at least some of the illegal material must be taken before making it inaccessible to users. Ideally this should be a forensic-quality copy of the disk using, for example, the UNIX® 'dd' command or a recognised commercial forensic package. If this is not possible for reasons of space or skill then a directory listing and a selection of files should be copied to a secure

medium, e.g. CD-ROM. Such copying should be the minimum necessary to indicate the scale and nature of the illegal material.

In either case the evidence - computer, disk or backup copies - must be sealed, labelled, signed and dated, and placed in a secure, locked location until it can be handed to the police. Details of the location and its security measures must be recorded in writing. All those with access to the location must be identified and any actual entry into the location recorded and signed.

The incident must not be discussed with colleagues. The material must not be shown to anyone other than, if absolutely necessary, those authorising and performing the investigation. Doing so may compromise the individual and jeopardise any subsequent police investigation.

5) Make minimum change to prevent access (MoU principle 3)

If the computer containing the material is not taken out of service, then action must be taken to prevent deliberate or accidental access to the material. Such action must make the least possible change to any remaining evidence; advice should normally be taken from the police on appropriate measures. These may include changing the permissions on directories or files to make them inaccessible, or deleting them.

6) Report to police (MoU principle 2)

When the authorised actions are completed, the results must be reported to the member of [computing service management] who authorised them. If the presence of illegal material was confirmed or seems likely, this must be reported immediately to the police.

Version 1.1 (added extreme pornography law to introduction)

Links
[1] http://www.legislation.gov.uk/ukpga/1978/37/contents
[2] http://www.legislation.gov.uk/ukpga/2008/4/part/5/crossheading/pornography-etc
[3] http://193.60.199.196/development/legal-and-regulatory/regulated-activities/network-monitoring-and-investigation.html
[4] http://www.legislation.gov.uk/ukpga/2003/42/contents
[5] https://www.cps.gov.uk/publication/memorandum-understanding-between-crown-prosecution-service-cps-and-association-chief
[6] http://www.legislation.gov.uk/ukpga/2008/4/contents
[7] http://www.iwf.org.uk