Investigating alleged and actual Child Pornography and other illegal material on Computers

These guidelines are intended to help computer support staff who may be called upon to investigate allegations of child abuse pictures[1] being held on computers in their own institution at the University of Cambridge. They have been approved by the Information Technology Syndicate, the Personnel Division and the University's Police contacts.

If you **know** that there is such material on a computer in the University, you should notify your Authorized Officer[2] and seek advice from the Cambridge Computer Emergency Response Team (Cambridge CERT), who will liaise with the Police. The major concern of the police is currently child abuse pictures, however the guidelines may be used to cover other illegal material.

Cambridge CERT,which is a part of the Computing Service, is the single point of contact with the Police force for computer related crime. The preferred method of contacting Cambridge CERT is by e-mail to cert@cam.ac.uk. Mail to this address is monitored regularly, including outside working hours. During working hours, members of CERT may be contacted via UCS Reception, 34600.

In investigating illegal material the basic rule is simple - it is the police that should be investigating such material and as soon as it seems likely that indecent photographs of children are involved, they should be contacted immediately via CERT and the investigation handed over to them. You should preserve all evidence including log files and server backups, if necessary, by seizing the machine or related equipment.

The only situation involving child abuse pictures that need not immediately be reported to the police is where there is an 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 doubt over such an allegation then authorized staff (see below) may need to perform the minimum of investigations necessary to verify it using the following guidelines.

Guidelines for Investigations

If an allegation of child pornography is made, contact the Authorized Officer immediately. He or she has the necessary authority to order an investigation.

Do not start an investigation without the authority of the Authorized officer and especially do not investigate an allegation on your own. Do not start to investigate until you have read all of these guidelines.

If you are authorized to investigate an allegation, the Authorized Officer will inform you in writing. The following rules must be adhered to:

. All investigations should be recorded in writing, with every click and URL recorded. Caching should be turned off. Record sheets should be numbered.

. Two authorised staff should be present during all such investigations: both should then sign and date every sheet of the record of the investigation. The result of the investigation should be reported to the Authorized Officer who should contact CERT if necessary

. As soon as evidence of child pornography is found, stop any further investigation and report to the Authorized Officer. You should preserve all evidence including log files and server backups, if necessary, by seizing the machine or related equipment.

. Do not show the material to anybody, other than authorised personnel. It may compromise you and your colleagues and jeopardise any subsequent police investigation.

. Do not take copies of the material. Although the law[3] does include an exemption for investigating crime, we do not recommend that you do so without specific instruction. If backups have inadvertently been taken, as part of a routine backup, these should be quarantined along with the computer at least while the investigation proceeds.

. The investigation should be treated as confidential; do not discuss the incident with anyone other than those immediately involved, CERT, your Head of Institution and line manager. Do not discuss details unless absolutely necessary.

. Often checking a list of URLs visited will be sufficient to confirm suspicions, so actually visiting sites should be regarded as an absolute last resort. If it is necessary to visit a suspect web site then it should be viewed with a text-only browser, or at least with all image downloads turned off and caching turned off. The text or filenames of a site will often indicate the nature of the content. The important thing is not to put yourself in any danger of prosecution and not to cause yourself distress or embarrassment.

This note deals with matters in connection with potential criminal offences. However it should be borne in mind that computer misuse is also an offence in terms of the University's disciplinary procedures for staff. It is important that the Head of Institution is made aware of any allegation made against a member of staff that is being investigated. The Personnel Division will be able to advise on the employment aspects of the investigation.

---

[1] Child abuse pictures concern images of children who are or appear to be under 18

[2] The Information Technology Syndicate rules define the Authorized Officer to be the Director of the University Computing Service in the case of services under the supervision of the ITS, or in other cases the relevant University or College officer (in the case of University institutions, the Chairman of the Council of the School, the Chairman of the Faculty Board or the Head of the Department; in the case of Colleges, a person appointed by the College for the purpose).

[3] Sexual Offences Act 2003 section 46