UNIVERSITY OF PORTSMOUTH

HANDLING ILLEGAL MATERIAL

August 2016

Contents

Document title		
Normal text		
Document author and department		
Normal text		
Approving body		
Normal text		
Date of approval		
Normal text		
Review date		
Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		

If you need this document in an alternative format, please email corporate.communications@port.ac.uk

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents/qA43279

Summary

What is this document about?

Occasionally, organisations may have to deal with allegations of serious misuse of computers, where indecent images of children or extreme pornographic images 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.

Who is this for?

This IS advisory is aimed at IS staff of the University.

How does the University check this is followed?

Annual review of this IS advisory will be performed to evaluate its effectiveness.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

1.0 Introduction

These guidelines are intended to help and protect 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 University systems. 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.

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.

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 procedures are described in sections 2.0 and 3.0 of this document.

2.0 Principles for Dealing with Illegal Material

The guidelines aim to implement the following essential principles:

2.1 The police are the appropriate people to be investigating serious crimes.

2.2 The risk of exposing users and staff to potentially harmful material must be minimised.

2.3 As little damage as possible should be done to any evidence of criminal activity.

Therefore:

2.4 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.

2.5 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.

2.6 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.

3.0 Rules for staff when dealing with illegal materials are:

3.1 Staff must only act when they have been given specific written authorisation by Information Services and in accordance with that authorisation and this procedure.

3.2 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 and to preserve it for later investigation.

3.3 Staff must report the presence of suspected illegal material to Information Services (ext 7777 FAO Security Team) and and must follow the directions of the police thereafter. Information Services will inform the police and the Director of Corporate Governance.

3.4 If any delay threatens the University's response to the incident, then the matter must be handed to the police immediately.

3.5 Any information obtained as a result of actions under these guidelines must be treated as strictly confidential.

4.0 Stages in the Process (for authorised investigator only)

4.1 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 Information Services. 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.

Normally, management will report the matter directly to the police and be guided by them in all further activities. If a member of Information Services is not available, call the police and inform Information Services as soon as possible. The contact for the University is the Police Liaison Officer who can be reached by phone on Tel: 023 9284 5989 (ext 5989 on University internal telephones) Mobile: 07793 369726. email: dave.fairbrother@port.ac.uk. 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

4.2 Obtain written authorisation

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. If there is real doubt over the accuracy of a report, Information Services 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 Information Services. 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 Information Services (ext. 7777) 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.

4.3 Perform minimum checks needed to confirm the presence of material

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 the presence of illegal material is confirmed, stop any further actions and report to the member of Information Services who gave the original authorisation.

4.4 Protect evidence

The computer containing the material and its immediate surroundings should be isolated, preventing access and any further use of the equipment. If this cannot be done, the most effective way to protect evidence is to remove power from the computer **(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 the evidence must (e.g. computer, USB stick, external disks etc) be moved then it must be placed in sealed bags, labelled, signed and dated, and placed in a secure, locked location until it can be handed to the police. The Anglesea or James Watson Data Centres are ideal for secure storage. 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.

It is vital to avoid compromising any subsequent police investigation. So, the incident must not be discussed with colleagues. In addition, the material must not be shown to anyone other than the police and, if absolutely necessary, those authorising and performing the investigation.

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.

4.6 Report to the police

When the authorised actions are completed, the results must be reported to the member of staff who authorised them. If the presence of illegal material is confirmed or seems likely, this must be reported immediately to the police.

5. References

The *Sexual Offences Act 2003* is available at: http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1

The MoU is available at: http://www.cps.gov.uk/publications/docs/mousexoffences.pdf

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.opsi.gov.uk/acts2008/ukpga_20080004_en_1

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk