

UNIVERSITY OF ULSTER

**Computer abuse by students and others using
University open access computing systems:**

Guidelines for University staff on procedures

Revised May 2004

Computer abuse by students and others using University open access computing systems; guidelines for University staff on procedures

INTRODUCTION

Regulations exist to cover the use of computers by students. (Ordinance 1990/1 Student Discipline, Section 1.2 (p)). In computer laboratories and terminal rooms there are notices which warn against, among other things, the 'downloading, displaying, viewing and manipulation of offensive and obscene material using University IT facilities'. Students are warned that random checks may occur, and that CCTV is in operation. It is important, therefore, that staff who supervise or patrol areas where computers are in use, know what to do in cases where computers are being misused.

WHAT IS ACCEPTABLE USE?

Details of acceptable uses may be viewed at

<http://www.ulst.ac.uk/isd/itus/docs/policies/Compositedoc.html>

or on posters displayed in all open access computing areas. This document is solely concerned with unacceptable use.

WHAT IS COMPUTER MISUSE?

For the purposes of this guidance note, the definition of computer misuse includes the 'downloading, displaying, viewing and manipulation of offensive or obscene material'. This would include pornography or scenes of violence. In extreme cases this may include the criminal act of downloading or displaying indecent photographs of children. Any such occurrences will be investigated by the police and must be reported immediately and dealt with in accordance with paragraph 10 under "Taking Action" and the section on "Reporting the Incident". Misuse also includes other activities: the creation and forwarding of defamatory material, infringement of copyright, transmission of unsolicited advertising or other material to outside organisations, unauthorised access to University network systems, deliberate corruption or destruction of others' data, disrupting the network or systems, introduction of viruses or disrupting the work of others. Although these are harder to detect, staff should remain alert to the possibility of such misuse. It should also be borne in mind that misuse can involve, for example eg in the case of obscene images, not merely offensive material, but also material the viewing of which constitutes a criminal offence.

ROLE OF STAFF

In the course of their duties, University staff may encounter situations where they believe that there is a misuse of computers. In such cases, it will be necessary for staff to act in accordance with the advice given below and to do so in a calm, comprehensive and neutral fashion. Reports of incidents will be essential for your line manager and others to determine what action to initiate.

TAKING ACTION

It is essential to take action, without delay, along the following lines:

- 1 Be alert to the misuse of University computers.
- 2 Scan the screens in a discreet manner to observe if there is any offensive material displayed in the form of pornographic images or images of violent material.
- 3 Before confronting anyone whom you suspect of viewing such images, it is always best to ensure that another colleague is present.
- 4 If you challenge a person, ensure that a careful note is made of the exchange. Ensure that timings are accurately recorded. Note whether others were present in the vicinity. Did other computer users see the images involved? Did you receive complaints from adjacent users? If other users witnessed the offence, record their details as statements may be required.
- 5 Take full details of the person concerned, from their student card, if possible.
- 6 Try to establish if the person concerned is engaged in any form of research, which could account for their action.
- 7 All interviews should be conducted in private, if possible: otherwise use a secluded area. If possible, a third party should be present.
- 8 If you have reasonable grounds to suspect that misuse of computer equipment has taken place, then ask the person concerned to leave the area.
- 9 It is vital that evidence should be preserved and to that end, if possible, you should not leave the scene unattended. If a colleague is present, ask him/her to remain at the scene.
- 10 Only in the most severe cases will it be necessary to remove the PC. If a serious misuse has been observed (Level 3) and especially an offence involving child pornography then the workstation must be preserved as evidence. In the company of your supervisor or another colleague, if possible, the only action you should take is to disconnect the PC from the electricity supply. Avoid touching it, if possible, in any other way. Cover it with plastic or fabric and remove it to the Security Supervisor's area. The Supervisor will be responsible for keeping the PC secure.

Note: The only situation involving child pornography that need not immediately be reported to the police (see Reporting the Incident) is where there is an allegation that a member of the organization 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 may need to perform the minimum of investigations necessary to verify it

Guidelines for Local Investigations.

If an allegation of child pornography is made then the workstation must be secured in accordance with procedures identified above and the Campus Information & Media Technology Consultant informed at the earliest opportunity. The Director of Information Services will be notified and give written consent to perform initial investigations. The Provost will be notified by the Director of Information Services that an initial investigation has commenced.

Do not start an investigation without the written authority of the Director of Information Services, or in his absence, the Provost or other Senior Officer, and especially do not investigate an allegation on your own.

The following rules must be adhered to:

- ~ All investigations should be recorded in writing, with every click and URL recorded.
- ~ Two 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 Director of Information Services.
- ~ As soon as evidence of child pornography is found stop any further investigation and report to the Director of Information Services.
- ~ Do not show the material to anybody, other than authorized personnel. It may compromise you and your colleagues and jeopardise any subsequent police investigation.
- ~ Do not take copies of the material. Taking a backup copy of an image file as evidence is likely to constitute 'making', and not just possession of child pornography and carries a maximum penalty of 10 years.
- ~ Do not discuss the incident with other colleagues.
- ~ 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 they should be viewed with a text-only browser, or at least with all image downloads turned off. The text or filenames of a site will often indicate the nature of the content.

REPORTING THE INCIDENT

It is vital that the following reporting procedure should be followed:

In the case of issuing an oral warning for a Level 1 offence (see Appendix), any member of University staff is authorised to do so.

For more serious offences, submit an immediate report to your supervisor, line manager or other senior staff member on duty.

Your supervisor should, as soon as possible, make a report to the Estate Services Officer and the Campus Information and Media Technology Consultant, and, in the case of a Level 3 offence, to the Provost. The supervisor must ensure that all statements are written up as soon as possible after the incident.

CONTACT WITH THE POLICE

It is the responsibility of the Provost, having regard to the circumstances as reported to him/her, to decide on whether to contact the police. Other staff should not contact the police.

FURTHER ADVICE

If there are issues which are still unclear, the following may be able to help:

The Assistant Estate Services Officer
responsible for your campus:

Coleraine and Magee
Jordanstown and Belfast

Mr J Coulter
Mr D Bagshaw

phone 24565
phone 66436

Estate Services Officer

Mr F Halpin

phone 24525

I and MT Consultant:

(Coleraine & Magee)
(Jordanstown & Belfast)

Mr N Blair
Mr E Courtney

phone 24542
phone 66940

Secretary of Disciplinary Committee

Mr P Quinn

phone 24295

Revised 5/5/04nsm

Computer abuse by students¹ and others² using University open access computing systems; guidelines for University staff on procedures

	Offence	Recommended Level ³
A	Playing games or other non-academic activities on public access workstations, especially when there is a queue of users	1
B	Permitting others to use personal passwords or PINS	1
C	Downloading software on to University computers without authorisation	1
D	Viewing offensive or obscene material – in relative privacy	1
E	Downloading films, music or other very large files which adversely affect the University's networks without permission	1 2, if copyright infringement 3, if child pornography
F	Scanning or probing systems in other institutions using University computers and networks	1
G	Failing to leave the computer lab needed for teaching when requested by a member of University staff	2
H	Viewing offensive or obscene material – others exposed to the material	3
I	Creation or unsolicited forwarding of defamatory, abusive or pornographic material	3
J	Transmission of unsolicited advertising or other material to third parties outside the University	2
K	Gaining unauthorised access to University or third parties' systems (hacking)	3
L	Harassment by sending persistent and unwanted electronic communications to another person, after having been warned to desist	3
M	Deliberate corruption of other parties' data, deliberate circulation of viruses	3
N	Impersonation in electronic communications with intent to mislead or defraud	3
O	Operating a business over the University's data communications systems without permission	3
P	Making copies of copyright material (including software, music, video or other files) for distribution to others without authorisation	3
Q	Persistent infringements of the Policy on Acceptable Use, despite warnings	3
R	Downloading and or viewing indecent photographs of children	3

¹ Defined as infringement of the Policy on Acceptable Use of University Computing and Data Communications Facilities

² There are separate Guidelines where cases involve abuse of computer facilities by members of staff

³ These recommendations are an indication of the appropriate penalty, which can be more or less severe depending on the scale of the infringement

Levels of offence – handling and penalties

- Level 1 Oral warning by any member of University staff discovering the offence; students should cease the activity immediately. If an individual regularly offends, staff would commence to record details of offences and when appropriate refer the student to the Head of School under Level 2
- Level 2 Referral to Head of School, together with a report. In each case the Head of School should interview the student, inform ISD or other reporting Department on action taken and write to the student to confirm the action. An alternative is that the Information Services Department handles the matter and reports to the Head of School.

Level 3 Referral to Provost

- Penalties for Level 1 Oral warning
- Penalties for Level 2 Removal of access to University IT systems (7 days)
Fines suggested range £25 – £150
Reimbursement of costs
- Penalties for Level 3 As decided by Provost. Action may include referral to Student Disciplinary Committee or, in the case of child pornography, to the Police.

Appeals

- Level 1 Appeal for Head of School or Director of Information Services
- Level 2 Appeal to Student Disciplinary Committee
- Level 3 Appeal to Student Disciplinary Committee (in case of penalty imposed by Provost or Director of Information Services) or to Disciplinary Appeal Board (in case of penalty imposed by Student Disciplinary Committee).