

IT Investigation Policy (2008)

1 *Aims*

- 1.1 The purpose of this Policy is to outline the circumstances in which it is permissible for the University to investigate the activity and access the IT accounts, communications and/or other data stored on IT equipment including any peripheral devices or hardware of staff, students, associates and any other authorised users of the University's IT equipment and facilities.
- 1.2 The University respects the privacy and academic freedom of staff and students. However, the University may carry out lawful monitoring of IT systems. Staff, students, associates and other authorised users should be aware that the University may access email, telephone and any other electronic communications, whether stored or in transit to comply with legislation and to ensure appropriate use of the University IT systems. All access and monitoring will comply with UK legislation, particularly the Regulation of Investigatory Powers Act 2000 (RIPA), the Human Rights Act 1998 (HRA) and the Data Protection Act 1998 (DPA).
- 1.3 University staff authorised by the Head of Computing Services may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or maintained by the University and may examine the content and relevant traffic data.
- 1.4 This policy should be read in conjunction with the Canterbury Christ Church University Regulations for the Acceptable Use of University Information Technology ("the AUP").

2 *Principles*

- 2.1 For the purposes of this policy the "Designated Authority" is the Head of Computing Services, or in his absence the Infrastructure Manager or other nominated officer.
- 2.2 The University may access files and communications for the following reasons:
 - 2.2.1 to prevent and detect crime (including, but not limited to, crimes such as fraud and unauthorised access to a computer system under the Computer Misuse Act 1990);
 - 2.2.2 to establish the existence of facts relevant to the business of the institution (for example where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent and with the authority of the Designated Authority.)
 - 2.2.3 to investigate or detect unauthorised use of the systems (for instance, to ascertain whether the user is breaking University regulations);
 - 2.2.4 to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the University's business (i.e. to ascertain whether the University is abiding by its own policies);

- 2.3 For any investigation into a member of staff authorisation must be by **both** their Head of Department and University Solicitor or Assistant University Secretary. The Designated Authority will also require proof that Human Resources are aware of the investigation.
- 2.4 For any investigation into a student, associate or other authorised user authorisation must come from the appropriate Head of Department and University Solicitor or Assistant University Secretary.

3 *Law Enforcement Authorities*

- 3.1 A number of non-institutional bodies/persons may be allowed access to user communications in certain circumstances. Where the University is compelled to provide access to communications by virtue of a Court Order or other competent authority, the University will disclose information to these non-institutional bodies/persons when required as allowed under the Data Protection Act 1998.
- 3.2 Under the Regulation of Investigatory Powers Act 2000 a warrant may be obtained by a number of law enforcement bodies regarding;
- issues of national security;
 - the prevention and detection of serious crime;
 - safeguarding the economic well-being of the UK.
- 3.3 In such circumstances, the University will provide necessary assistance with the execution of a lawful warrant.

4 *Access to Accounts – Suspected Illegal Behaviour*

- 4.1 Where circumstances brought to the Designated Authority's attention constitute grounds for reasonable suspicion that any user is using the University's IT Facilities for the commission or attempted commission of a criminal offence, the University Solicitor will contact the police.
- 4.2 The IT account will be frozen and any associated hardware or peripheral devices will be held pending further investigation by the police. No examination or further investigation will be carried out to ensure that there is no compromise of any future police enquiry.

5 *Access to Student and Other Authorised User Accounts – Suspected Breach of Regulations*

- 5.1 Where there are reasonable grounds to suspect that a breach of the University's regulations has taken place in the first instance the student will be contacted, where possible, to request consent for access. Where consent is given, Designated Authority will record that the student's communications are being accessed.
- 5.2 If it is not appropriate to inform the student or the student is not available to give consent or consent is refused, authorisation will be requested as described in paragraph 2.4 above.
- 5.3 All actions will be taken in line with the Student Disciplinary Procedures.
- 5.4 The relevant communications should be reviewed by the Designated Authority to assess whether the student has breached the University's Rules and Regulations and he will inform the disciplinary investigation.

6 Access to Staff and Associate Accounts – Suspected Breach of Terms of Contract

- 6.1 Where there are reasonable grounds to suspect that a member of staff is using the University's IT Facilities in breach of the terms of their contract of employment in the first instance the member of staff will be contacted, where possible, to request consent for access. Where consent is given, the Designated Authority will record that the member of staff's communications are being accessed.
- 6.2 If it is not possible to inform the member of staff, the member of staff is not available to give consent, consent is refused or access is required under paragraph 2.1 above, authorisation will be requested by the Designated Authority as detailed in paragraph 2.3.
- 6.3 The relevant communications will be reviewed by the Designated Authority to assess whether the member of staff has breached the terms of their contract of employment and the findings passed to the appropriate disciplinary investigation.

7 General Procedures

- 7.1 Any access to the communications of a member of staff, student or authorised user of the University systems will be with as little intrusion and disruption to the communications of third parties that are unconnected to the authorised access as possible.
- 7.2 Any communications collected under this Policy will be treated as confidential and will only be examined by those persons who are so authorised.
- 7.3 Any communications accessed under this Policy will only be retained for as long a period as deemed necessary for the specific purpose and in line with the University's Records Retention Policy.
- 7.4 Any material collected under this Policy will be stored securely and will be labelled accordingly depending on the sensitivity of the material in question. If accessing communications does not uncover any material requiring further investigation of the member of staff, student, associate or authorised user concerned, all material collected will be destroyed 20 working days after the person has been informed.
- 7.5 The Designated Person will maintain a log of all investigations carried out under these procedures.
- 7.6 Any person collecting communications over a period of time under this Policy will ensure that they have continued authorisation to access communications of a member of staff, student or authorised user.

Document control/change history				
Version	Author(s)	Date	Circulation	Comments
1	IE	August 2008	ISC policy T&F group	Taken from JISC model policy, plus local policies
2	IE/RM	Sept 2008	ISC	Minor re-edit and format

Document approval and review	
Approved by:	Information Systems Committee
Date approved:	
Review date:	
Author(s):	Head of Computing Services
Owning Department:	Computing Services