Information Services Computer Misuse/Abuse Procedures for Students, Staff, Alumni and External Users

1. Introduction

1.1 This document describes the procedures for handling suspected cases of computer misuse/abuse that breach the *Regulations for the Use of IT Facilities at the University of Kent* (referred to as the *Regulations* throughout). A number of roles are explained in terms of specific functions within these procedures. These procedures also indicate the actions to be taken in the event of suspected computer misuse/abuse.

1.2 For the purpose of these procedures misuse is an unintentional action while abuse is a deliberate action.

1.3 This procedure will be applied fairly and equitably, in accordance with the University's Equality and Diversity Policy and the principles of 'natural justice' [see General Context – The University's Disciplinary Framework – Regulations on Student Discipline in relation to non-academic matters].

2. Definition of roles

2.1 IT Regulations Implementation Officer

The IT Regulations Implementation Officer is normally the Deputy Director of Planning and Administration and is charged with responsibility for the implementation of the *Regulations.* In his/her absence, the Director of Information Services will have responsibility.

2.2 Investigating Officer

The Quality and Standards Manager in Information Services will normally act as the Investigating Officer and will assess cases of suspected computer misuse/abuse and will initiate such investigations and actions as are appropriate under these procedures. In his/her absence, the Operations Manager in Information Services will fulfill this role.

2.3 Other roles

The Network Controller has been identified by the University as the person designated as having the authority to perform interceptions on the University data network in accordance with the Regulations of Investigatory Powers (RIP) Act 2000 – (Communications Data) (Additional Functions and Amendment) Order 2006.

The Compliance Officer is the person with responsibility to ensure that the University data network is operated within UK law: principally the RIP Act and the Computer Misuse Act 1990 but also other relevant legislation.

The Systems Administrator is the person with responsibility for and privilege to perform the technical management of a computerised system. Specified Systems Administrators will be explicitly authorised by the Network Controller to perform particular types of monitoring

within the scope of these procedures. These Systems Administrators may be from Professional Services or Academic Schools.

The University's IT Security Team is headed by the Network Controller and has responsibility for the security of the University data network and attached systems. The Team will report suspected misuse/abuse to the Investigating Officer and liaise with Systems Administrators.

3. Withdrawal of access

3.1 The Investigating Officer may require Systems Administrators to withdraw specific computing facilities during an investigation of a suspected case of misuse/abuse:

- A user's access to IT facilities may be suspended;
- Computing equipment may be disconnected from the network;
- Computer equipment or files may be physically removed to a secure location;
- Access to specific services may be withdrawn.

3.2 In all cases other than the circumstances listed in paragraph **3.3** below, the case of misuse/abuse should be reported to the Investigating Officer **before** any action is taken (by telephone and or email – and a FootPrints ticket created and assigned to the Quality & Standards team).

3.3 A member of the IT Security Team may temporarily withdraw access to IT facilities or disconnect equipment from the University's network in the following circumstances:

- To ensure the security and continued operation of IT systems.
- To prevent the spread of malware (computer virus, worm, etc.)
- To preserve evidence for an investigation.
- To prevent the University being brought into disrepute.

4. Investigation of suspected misuse/abuse by students

4.1 If a complaint about misuse/abuse of IT facilities is reported to a member of Information Services, or a member of Information Services detects suspected misuse/abuse, the case and any actions taken must be reported on FootPrints and the ticket assigned to the Investigating Officer.

4.2 On receipt of a complaint about, or a report of, a suspected case of misuse/abuse, the Investigating Officer will:

- Acknowledge the complaint, where appropriate.
- Initiate an appropriate investigation.
- Ensure that records are kept of all evidence collected, and actions taken, during the investigation, along with other relevant materials.

4.3 The Investigating Officer will collect evidence of the alleged offence. The Investigating Officer can make a formal request to the Network Controller that further investigations are conducted. The Network

Controller will then authorise the relevant Systems Administrator (in the Operations team or another team in Professional Services or Academic Schools) to perform the requested investigation, including looking through relevant log files for evidence. This will be done in compliance with the RIP Act (2000). For further information see *Security Procedures for Systems Administrators*.

4.4 If there is evidence of any IT misuse/abuse, the Investigating Officer will normally withdraw the user's access to all University and departmental IT facilities or to specific IT facilities or servers pending the completion of an investigation.

4.5 The user suspected of misuse/abuse may be invited to an interview with the Investigating Officer, or may be contacted and presented with the evidence collected (suitably anonymised where appropriate in sensitive cases) and given the opportunity to comment. This may include an adjournment if the user requests time to review the evidence before commenting.

4.6 Following the investigation and interview/contact, the Investigating Officer will come to one of the following conclusions:

4.6.1 If the Investigating Officer is of the opinion that there has been a breach of UK legislation he/she will notify the IT Regulations Implementation Officer who will review the case. The matter may then be reported to the Director of Information Services or other senior officer of the University to discuss how to proceed.

4.6.2 The Investigating Officer will make a decision on whether an offence against the Regulations has been committed and, if so, will then decide on the appropriate action as described in paragraph **4.7** below (if necessary) with the guidance of the IT Regulations Implementation Officer.

4.6.3 If there is evidence that the Guidelines for using various facilities (email, forums, blogs, MyFolio etc)
http://www.kent.ac.uk/web/services/bulletin-boards/index.html;
http://www.kent.ac.uk/web/services/blogs/index.html
have not been followed but it is not evident that the Regulations have been breached then an email warning may be sent. If the warning email message(s) are ignored, then the suspected offender can be considered as having breached the Regulations.

4.6.4 If, following the investigation, there is no evidence of IT misuse/abuse, then:

- All access to IT facilities will be restored and if necessary an apology for any inconvenience will be given.
- All materials collected during the investigation will be immediately destroyed.
- No further action will be taken.

4.7 Appropriate action

The following actions are available to the Investigating Officer according to the nature of the alleged conduct.

4.7.1 Guidance: minor and/or inadvertent misuse

- The Investigating Officer will give the user **advice and guidance** on the appropriate use of IT facilities.
- The user's access to IT facilities (if temporarily suspended) will then be restored.

4.7.2 Informal warning: minor and deliberate misuse/abuse

- The Investigating Officer will give the user **an informal warning in writing**.
- The user will be required to write and sign a letter acknowledging his/her breach of the IT Regulations, agreeing not to re-commit the offence, and agreeing to abide by the IT Regulations in future.
- On receipt of the letter, the user's access to IT facilities (if temporarily suspended) will be restored.

4.7.3 Repeat minor and deliberate misuse/abuse following informal warnings in writing

- The Investigating Officer will refer the matter to the College Master and may inform the user's tutor [see Regulations on Student Discipline in relation to non-academic matters].

4.7.4 Referral in the case of significant breaches of the IT Regulations: Referral to University Disciplinary Procedures for Students [See Regulations on Student Discipline in relation to non-academic matters].

- The user's access to IT facilities will not normally be restored until the formal disciplinary procedures have been completed.
- All evidence and relevant materials are prepared for presentation to the appropriate University authorities.
- The user's tutor and Head of School and College Master will be notified.
- The Director of Information Services will refer the case to the appropriate University authorities.

4.8 All appeals by students against the decision of the Investigating Officer will be referred to the Director of Information Services who will forward the case to the College Master.

5. Investigation of suspected misuse/abuse by external users

5.1 If a complaint about misuse/abuse of IT facilities by an external user is reported to a member of Information Services, or a member of Information Services detects suspected misuse/abuse, an investigation as described in section **4** will be conducted. Note that "external users" are all users of the University's IT facilities who are **not** members of the University of Kent (i.e. staff, students, and alumni) who have been given a Kent IT account after signing the *Regulations.*

5.2 If there is evidence that the *Regulations* have been breached, then all access to IT facilities will be withdrawn immediately, although mitigating circumstances may be taken into account.

5.3 All appeals by external users against the decision of the Investigating Officer will be referred to the Director of Information Services, or, in the case of his/her prior involvement in the case, to the Pro-Vice-Chancellor responsible for Information Services. In either case the decision will be final.

6. Investigation of suspected misuse/abuse by alumni

6.1 If a complaint about misuse/abuse of IT facilities by alumni is reported to a member of Information Services, or a member of Information Services detects suspected misuse/abuse, an investigation as described in section **4** will be conducted. Note that "alumni" are all users with a live@edu account that have agreed to abide by the *Regulations.*

6.2 If there is evidence that the *Regulations* have been breached, the Investigating Officer will email the account holder reminding him/her that they are bound by the IT regulations; they will be asked to respond to the Investigating Officer acknowledging the breach in regulations and asked to give an undertaking that regulations will be respected in the future. He/she will be reminded they risk losing their IT account if the regulations are breached in the future.

6.3 Any subsequent breach will lead to the email account being withdrawn, although mitigating circumstances may be taken into account.

6.4 All appeals by alumni against the decision of the Investigating Officer will be referred to the Director of Information Services, or, in the case of his/her prior involvement in the case, to the Pro-Vice-Chancellor responsible for Information Services. In either case the decision will be final.

7. Investigation of suspected misuse/abuse by staff

7.1. If a complaint about misuse of IT facilities by a member of staff is suspected and or reported to a member of Information Services, or a member of Information Services detects suspected misuse an investigation as described in section **4** will be conducted.

7.1.1 If the complaint about misuse of IT facilities by a member of staff has a basis the Investigating Officer may give the user **advice and guidance** on the appropriate use of IT facilities. The user's access to IT facilities if suspended will then be restored.

7.1.2 If there is evidence that the Guidelines for using various facilities (email, forums blogs, MyFolio etc) have not been followed but it is not evident that the Regulations have been breached, then an email warning may be sent. If the warning email message(s) are ignored, then the suspected offender can be considered as having breached the Regulations.

7.2 Where suspected abuse by a member of staff is reported to Information Services by Professional Services/Academic Schools or Human Resources (HR) (where HR are not already involved the Investigating Officer will notify HR). A full investigation will be carried out as described in section **4.** This will be undertaken by the Investigating Officer with support from HR. In all cases the relevant Professional Service/Head of Academic School will be informed by HR.

7.3 If it is deemed appropriate based on the allegations made, action may be required to ensure that the investigation can be undertaken in a full and unhindered way. Action taken may include review or suspension of part or all of the user's access to IT facilities, and/or suspension of employment on full pay.

7.4 If, following the investigation, there is no evidence of IT abuse then

- All access to IT facilities will be restored, apologies given and suspension of employment lifted, as necessary.
- All materials collected during the investigation will be immediately destroyed.
- No further action will be taken.

7.5 If, following the investigation, there is evidence of IT abuse a disciplinary interview will be arranged by HR. All investigatory action and, where appropriate, disciplinary action will be undertaken in accordance with the appropriate University disciplinary procedure, namely the Disciplinary and Dismissals Procedure Agreement for Staff in Grades 1-6 or the Code of Practice under Statute 7.

7.6 Advice from Information Services, via the Investigating Officer, will be sought at all stages of any such investigation/disciplinary interview and in the case of the latter, it is likely that he/she and or other officers within IS may be required to attend as an expert witness.

7.7 Cases of serious and/or repeated misuse may be deemed by the University as gross misconduct, and/or result in dismissal in accordance with the appropriate University disciplinary procedure.

8. Retention of evidence

8.1 All relevant data will be retained during the investigation and data collected during an investigation will be retained as supporting evidence in any disciplinary process.

8.2 Evidence used in a formal staff disciplinary action will be retained in accordance with University data retention policy.

8.3 Evidence used in an informal or formal student disciplinary action will be retained for up to four years and then destroyed. This information will be kept for the purpose of informing decisions on repeat offences.

8.4 All retained evidence will be held securely. It will only be accessible by the Investigating Officer, the IT Regulations Implementation Officer and the Director of Information Services.

8.5 Copies of any personal data held on individuals will be supplied under the provisions of the *Data Protection Act (1998).*

9. Review

9.1 This procedure will be reviewed annually or in the light of any new or amended relevant legislation.

Approved 23 March 2012