Policy on access to staff and student accounts by authorised persons

School of Informatics

19th March 2009

1 Preamble

This policy is based on section 5 of the JISClegal model policy on Institutional Access to Staff and Student IT Accounts and IT Equipment. This Policy should be read in conjunction with the University of Edinburgh's Computing Regulations and with any other relevant sections of the university's rules and regulations as applicable to students and relevant conditions of employment as applicable to members of staff. The term "data" will be used to cover communications and documents.

2 Staff Absence

Where a member of staff is absent from work and access is required to that member of staff's IT account for a specific reason (for example to access correspondence in order to complete an item of work), the School of Informatics will follow the procedure set out below:

1. Where possible, the member of staff will be contacted and consent sought for access to specific data.
2. Where consent is not or cannot be given and there is no alternative way to get the required information, permission to access the member of staff's account will be sought in writing from the Head of School. Authorisation will only be given for access to specific information and not for general access to the account in question.
3. The person authorised to access the account is responsible for ensuring that only the specific information authorised is accessed and that other information is not read or disclosed.

3 Access to Staff and Student Accounts – Suspected Illegal Behaviour

1. Where circumstances brought to the Head of School's attention constitute grounds for reasonable suspicion that a student or member of staff is using the School of Informatics's IT Facilities for the commission or attempted commission of a criminal offence, the Head of School should contact the police.
2. The IT account and any associated hardware or peripheral devices should be frozen pending further investigation by the School of Informatics or the police.

4 Access to Student Accounts – Suspected Breach of the University's Regulations

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, the investigating computing officers will record that the student's data is being accessed.
2. If it is not appropriate to inform the student or the student is not available to give consent or consent is refused, authorisation should be requested from the Head of School.
3. The relevant data should be reviewed by the Head of School to assess whether the student has breached the university's rules and regulations [and where necessary the appropriate disciplinary investigation should be begun].

5 Access to Staff Accounts – Suspected Breach of Terms of Contract of Employment

1. Where there are reasonable grounds to suspect that a member of staff is using the School of Informatics'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 investigating computing officers will record that the member of staffs data is being accessed.
2. If it is not possible to inform the member of staff or the member of staff is not available to give consent or consent is refused or access is required with legitimate reason by the School of Informatics, authorisation will be requested from the Head of School.
3. The relevant data will be reviewed by the Head of School to assess whether the member of staff has breached the terms of their contract of employment [and where necessary the appropriate disciplinary investigation should be begun].

6 General Guidance

1. All access and monitoring will comply with UK legislation including the Human Rights Act 1998, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000 (pursuant to this policy).
2. Any access to the data of a member of staff or student by an authorised user of the School of Informatics systems will be with as little intrusion and disruption to third parties that are unconnected to the authorised access as possible.
3. Any data collected under this Policy will be treated as confidential and will only be examined by those persons who are so authorised.
4. Any data 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.
5. 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 data does not uncover any material/content which would warrant further investigation of the data of the member of staff or student by the authorised user concerned, all material collected will be destroyed after 28 days.
6. Any person collecting data under this Policy will ensure that they have continued authorisation to access the data of the member of staff or student concerned.
7. The School of Informatics Computing IT Facilities include any computing equipment (eg laptop) which has been loaned to a member of staff or student as part of their employment or studies.