

Institutional Access to Staff and Student IT Accounts and IT Equipment - MODEL POLICY



Guidance Note for Users

The purpose of this Policy is to outline the circumstances in which it is permissible for an institution to access the IT accounts of staff members or students.

Your institution should already have in place an Acceptable Use Policy or Communications Policy (referred to below as AUP). This AUP should apply to both your staff and students who have access to IT systems and should set out the institution's policy on the acceptable use of those facilities. It may already set out the circumstances in which it is permissible for an institution to access the IT accounts of staff members or students. If not then this policy may be of assistance in updating your existing AUP. If you wish to use this Model Policy, you will need to make some amendments so that it suits your institution, so read it carefully. In particular, look out for the highlighted sections in square brackets.

Nothing in this Model Policy constitutes legal advice. You should consult a suitably qualified lawyer on any specific legal problem or matter.

This Model Policy is licensed by Pinsent Masons and JISC Legal for use by the UK further education, higher education and specialist college sectors. It may be copied and adapted by your institution and the adapted version published in order to increase awareness. This may include publishing on an intranet or on the internet. If substantive adaptations are made to this MODEL Policy these should not be attributed to Pinsent Masons or JISC Legal. The MODEL Policy must not be re-sold or distributed further without the express permission of Pinsent Masons and JISC Legal.

One of the requirements of the legislation is that an institution must make reasonable efforts to inform users of its systems that an interception may take place. In addition the requirements of the Data Protection Act 1998 to provide information to those whose data are processed will come into play.

It is not normally appropriate for University or College staff to investigate suspected criminal behaviour.

Detailed guidance on monitoring and interception is available on the website of the Information Commissioner in The Employment Practices Code - Part 3 – Monitoring at Work - online at - <http://www.ico.gov.uk/>.

Specific guidance on the powers of law enforcement agencies to require an institution to disclose communications information is contained in the document "Monitoring and Encryption - the Powers of Law Enforcement Agencies" on the JISC Legal website at - <http://www.jisclegal.ac.uk/publications/MonitoringGS.htm>.

Authorised Person

In order for this Model Policy to operate as it should, your institution ought to appoint persons who will be authorised to access information. These persons act on behalf of the institution and may be members of the institution's management team. They should be appointed in accordance with the appropriate management procedures within your institution which may, for example, take the form of a Scheme of Delegation.

Recording Access

In each case where access is authorised a standard form should be adopted that records the specific authorisation (with the reasons for the access) and which identifies the particular information (in so far as possible) required from an account. This completed authorisation form should be retained by the institution for an appropriate period determined by the Records Retention Policy of your institution.

Institutional Access to Staff and Student IT Accounts and IT Equipment

1. POLICY

- 1.1 The purpose of this Policy is to outline the circumstances in which it is permissible for the institution to access the IT accounts, communications and/or other data stored on IT equipment including any peripheral devices or hardware of staff members or students.
- 1.2 This Policy applies to all [University/College] staff, students and any other authorised users of [the University/College]'s IT equipment and facilities.
- 1.3 [The University/College] respects the privacy and academic freedom of staff and students. However, [the University/College] may carry out lawful monitoring of IT systems. Staff, students and any other authorised users should be aware that [the University/College] may access email, telephone and any other electronic communications, whether stored or in transit. This is in order to comply with the law and applicable regulations and to ensure appropriate use of [the University/College] IT systems. All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000 (RIPA), the Human Rights Act 1998 (HRA) and the Data Protection Act 1998 (DPA).

2. [THE UNIVERSITY/COLLEGE]'S POWERS TO ACCESS COMMUNICATIONS

- 2.1 Authorised [University/College] staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or maintained (except where the [University/College] act solely as a service provider for another body) by [the University/College] and may examine the content and relevant traffic data.
- 2.2 [The University/College] may access files and communications for the following reasons:
 - 2.2.1 to ensure the operational effectiveness of the service. (for example, [the University/College] may take measures to protect the telecommunications system from viruses and other threats such as hacking or denial of service attacks);
 - 2.2.2 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);
 - 2.2.3 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 an authorised person. Another example may be checking email accounts when staff are absent on holiday or on sick leave to access relevant communications); **[Note to user]** - Your institution must notify staff and students in the AUP that your institution may access files and communications for such purposes.]
 - 2.2.4 to investigate or detect unauthorised use of the systems (for instance, to check whether the user is breaking regulations);
 - 2.2.5 to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to [the University's/College's] business (i.e. to

- ascertain whether [the University/College] is abiding by its own policies);
- 2.2.6 to ascertain or demonstrate standards which are achieved or ought to be achieved by persons using the system (for instance, staff training or quality control, but not for market research);
- 2.2.7 to monitor whether or not communications are relevant to the business of [the University/College] (for example, to check an email account to ensure that it is not being used for personal or private purposes but not to look at the contents of the emails unless this is required to confirm the use of the email account);
- 2.2.8 to monitor (but not log) communications to a confidential, free, telephone counselling or support service run by [the University/College], provided that users are able to remain anonymous if they so choose. This is to enable help-line workers to receive appropriate supervision and support.

3. THE POWERS OF LAW ENFORCEMENT AUTHORITIES TO ACCESS COMMUNICATIONS

- 3.1 A number of non-institutional bodies/persons may be allowed access to user communications in certain circumstances. Where [the University/College] is compelled to provide access to communications by virtue of a Court Order or other competent authority, [the University/College] will disclose information to these non-institutional bodies/persons when required as allowed under the Data Protection Act 1998.

For example, 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.

In such circumstances, [the University/College] will provide reasonable assistance with the execution of a lawful warrant.

4. POLICY ON ACCESS TO STUDENT ACCOUNTS BY OTHER STUDENTS

- 4.1 Students must not access the IT accounts of any other person, and must only use the institution's facilities in compliance with the [the University/College] Acceptable Use Policy.

5. POLICY ON ACCESS TO STAFF AND STUDENT ACCOUNTS BY AUTHORISED PERSONS

5.1 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 University/College] will follow the procedure set out below:

- 5.1.1 If appropriate, the member of staff will be contacted and consent sought for access to specific communications and/or documents.

- 5.1.2 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 an authorised person. Authorisation will only be given for access to specific information and not for general access to the account in question.
- 5.1.3 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.
- 5.1.4 After the necessary information has been retrieved, the password to the absent member of staff's IT account will be reset and the new password will be communicated only to that member of staff.
- 5.2 Access to Staff and Student Accounts – Suspected Illegal Behaviour**
- 5.2.1 Where circumstances brought to the authorised person's attention constitute grounds for reasonable suspicion that a student or member of staff is using [the University/College]'s IT Facilities for the commission or attempted commission of a criminal offence, the authorised person should contact the police.
- 5.2.2 The IT account and any associated hardware or peripheral devices should be frozen pending further investigation by [the University/College] or the police. [**Note to user** - A 'Good Practice Guide for Computer Based Electronic Evidence' produced by the Association of Chief Police Officers (ACPO) is available online at - <http://www.acpo.police.uk/>.]
- 5.3 Access to Student Accounts – Suspected Breach of [the University/College]'s Regulations**
- 5.3.1 Where there are reasonable grounds to suspect that a breach of [the University/College]'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, an authorised person will record that the student's communications are being accessed.
- 5.3.2 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 an authorised person.
- 5.3.3 The relevant communications should be reviewed by an authorised person to assess whether the student has breached [the University/College]'s Rules and Regulations [and where necessary the appropriate disciplinary investigation should be begun].
- 5.4 Access to Staff Accounts – Suspected Breach of Terms of Contract of Employment**
- 5.4.1 Where there are reasonable grounds to suspect that a member of staff is using [the University/College]'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, an authorised person will record that the member of staff's communications are being accessed.
- 5.4.2 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 under clause 2.2 above, authorisation will be requested from an authorised person.

- 5.4.3 The relevant communications will be reviewed by an authorised person 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].
- 5.4.4 All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000, the Human Rights Act 1998 and the Data Protection Act 1998.

5.5 General Guidance

- 5.5.1 Any access to the communications of a member of staff, student or authorised user of [the University/College] systems will be with as little intrusion and disruption to the communications of third parties that are unconnected to the authorised access as possible.
- 5.5.2 Any communications collected under this Policy will be treated as confidential and will only be examined by those persons who are so authorised.
- 5.5.3 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/College]'s Records Retention Policy.
- 5.5.4 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/content which would warrant further investigation of the communications of the member of staff, student or authorised user concerned, all material collected will be destroyed after [28] days.
- 5.5.5 Any person collecting communications under this Policy will ensure that they have continued authorisation to access communications of a member of staff, student or authorised user.

This Policy should be read in conjunction with [the University/College]'s Communication Policy and with any other relevant sections of [the University/College]'s Rules and Regulations as applicable to students and relevant terms of [the University/College]'s conditions of employment as applicable to members of staff.

USE OF THIS MODEL POLICY

If you wish to use this Model Policy, you will need to make some amendments so that it suits your institution, so read it carefully. In particular, look out for the highlighted sections in square brackets.

This MODEL Policy is licensed by Pinsent Masons and JISC Legal for use by the UK further education, higher education and specialist college sectors. It may be copied and adapted by your institution and the adapted version published in order to increase awareness. This may include publishing on an intranet or on the internet. If substantive adaptations are made to this MODEL Policy these should not be attributed to Pinsent Masons or JISC Legal. The MODEL Policy must not be re-sold or distributed further without the express permission of Pinsent Masons and JISC Legal.