Information Security Policy

Institutional Access to information within University IT Accounts, Equipment and Networks

1 Introduction

1.1 This Policy outlines the circumstances in which Officers of the University of Sussex may authorise staff to access the IT accounts, communications and/or other data stored on its IT equipment, including any peripheral devices or hardware, of authorised users including staff, students, contractors, consultants, visitors and guests of the University. This Policy should be read in conjunction with the Information Security Policy at http://www.sussex.ac.uk/infosec, any relevant sections of the Ordinances and Regulations as applicable to students and relevant terms of the conditions of employment as applicable to members of staff.

1.2 The University of Sussex respects the privacy and academic freedom of staff and students. Staff, students and any other authorised users should be aware that the University may access files, 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 IT systems. All access and monitoring will comply with UK legislation including the Regulation of Investigatory Powers Act 2000 (RIPA), Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR); the Human Rights Act 1998 (HRA); the Data Protection Act 2018 (GDPR) and in accord with the Employment Practices Data Protection Code (June 2005); the Investigatory Powers Act 2016 and the Counter Terrorism and Security Act 2015 which includes Prevent duty guidance.

1.3 The University will not access files or communications, including email, or disclose personal data except:

1.3.1 at the specific request of the account owner;

1.3.2 when allowed to do so under Data Protection Act 2018 (GDPR) or compelled to do so by law;

1.3.3 when authorisation or permission is sought and obtained as detailed below in paragraph 2.

1.4 Access to another person's communications or data by an individual operating without the University's authority through this Policy or the University's Regulations for the Use of Information and Communications Technology may be considered a disciplinary offence and could lead to criminal proceedings.

1.5 Access to data, communications and voice mail associated with the University telephone system is covered under separate policy.

1.6 Third parties might act as data processors on behalf of the University to allow for delivery of services, but third parties will not have access to personal data for any other purposes.

2 THE UNIVERSITY OF SUSSEX'S POWERS TO ACCESS COMMUNICATIONS AND DATA

2.1 University staff authorised by the Director of IT Services or the Chief Operating Officer may access and monitor files and communications, including electronic mail files, stored on any IT facilities owned, managed or maintained by the University (except where the University acts solely as a service provider for another body) and may examine the content and relevant traffic data in accordance with the terms of this policy. In this document, The Director of IT Services means the post holder or nominee and the Chief Operating Officer means the post holder or one of the Pro Vice-Chancellors in his/her absence.

2.2 **Access for Operational Reasons** The Director of IT Services may authorise University staff to access or monitor files and communications (including email) for an appropriate time limited period for the following operational reasons:

2.2.1 to ensure the operational effectiveness of the service (for example, IT Services may take measures to protect the communications system from viruses and other threats such as hacking or denial of service attacks or to investigate email routing problems);

2.2.2 to investigate anomalies in routinely monitored communication logs;

2.2.3 to access information needed for urgent operational reasons as detailed in section 1.1 and 1.2 of the Annex A;

2.2.4 Retrospective approval may be given by the Director of IT Services in exceptional circumstances where urgent action is needed to protect the integrity of systems or data.

2.3 **Access for Exceptional Reasons** - The Chief Operating Officer may authorise University staff to access and monitor files and communications for an appropriate time limited period for the following exceptional reasons:

2.3.1 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) The Vice-Chancellor's approval must be obtained if access or monitoring relates to one of the named officers;

2.3.2 to establish the existence of facts relevant to the business of the institution (for example, where a case of suspected fabrication of research results 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 Chief Operating Officer;

2.3.3 to investigate or detect unauthorised use of the University's information systems by examining the content of communications (for instance, to check whether the user is breaking regulations);

2.3.4 to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the University's business (e.g. to ascertain whether the University of Sussex is abiding by its own policies).

2.4 Each specific request for the authority to access and monitor files and communications for exceptional reasons under section 2.3 must be made in advance and accompanied by a privacy impact assessment which will document:

2.4.1 the reason for the access and monitoring and an indication of why the action requested is felt to be a proportionate approach;

2.4.2 the scope of the access and monitoring; the intended duration;

2.4.3 the steps to be taken to protect the privacy of any individual(s) .

2.5 Each specific request for the authority to access and monitor files and communications under section 2.3 will be recorded by the Governance Office and reported annually in summary form to the Information Services Committee.

3 The Powers of Law Enforcement Authorities to Access Communications

3.1 Where the university is sanctioned or compelled by legislation to provide access to communications, the University will comply with the relevant legislation through the authority of the Chief Operating Officer.

3.2 A third party acting as a data processor may be required to hand over data and /or meta data to UK or US law enforcement agencies without the University being informed.

ANNEX A

1. Procedure for Access to Staff and Students Accounts by Authorised Persons

1.1. Staff Absence

1.1.1. If a member of staff is absent from work and a planned handover has not occurred 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 will follow the procedure set out below: Authorisation will only be given when access is required for operational reasons and or specific information; it will not be granted for general access to the account in question.

1.1.2. If appropriate, the member of staff will be contacted by their line manager and they will be informed that access to identified role-specific communications and/or documents is being sought. The request will be signed off by the Division Head, Head of School or School Administrator and actioned by IT Services.

1.1.3. Where there is no alternative way to get the required information, permission to access the member of staff's account will be sought under the authority of the Director of IT Services.

1.1.4. After the necessary information has been retrieved, access will be removed and the account holder informed of the access that has taken place.

1.2. **Staff Departures** – Before staff leave University employment, they are expected to make available all University information to their line manager or other member of staff. All personal information that they may have been storing on University systems should be deleted.

1.2.1. Where information has not been made available and access is required, permission to access the account will be sought from the Director of IT Services.

1.2.2. The Director of IT Services is responsible for ensuring as far as is reasonably possible that only University information is accessed and that personal information is not disclosed.

1.3. Access to Student Accounts - Suspected Breach of the University of Sussex's Regulations.

1.3.1. Where there are reasonable grounds to suspect that a breach of University regulations has taken place; in the first instance the student will normally be contacted, where possible, to request consent for access. Where consent is given, the Chief Operating Officer will record that the student's communications are being accessed with consent.

1.3.2. If it is not appropriate or possible to inform the student or the student is not available to give consent or consent is refused, authorisation will be requested from the Chief Operating Officer.

1.3.3. The relevant communications will be reviewed by the Chief Operating Officer to assess whether the student is considered to have breached the University's Rules and Regulations and where necessary the appropriate disciplinary procedures will be invoked.

1.4. Access to Staff Accounts-Suspected Breach of Terms of Contract of Employment

1.4.1. Where there are reasonable grounds to suspect that a member of staff is in breach of the terms of their contract of employment in the first instance the member of staff will normally be contacted to discuss the circumstances and, if necessary, request consent for access. Where consent is given, the Chief Operating Officer will record that the member of staff's communications are being accessed by consent.

1.4.2. 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 section 2.3 above, authorisation will be requested from the Chief Operating Officer.

1.4.3. The relevant communications will be reviewed by the Chief Operating Officer to assess whether the member of staff is considered to have breached the terms of their contract of employment. Where such a breach is suspected to have occurred, the appropriate disciplinary procedures will be invoked.

1.5. Access to Staff and Student Accounts - Suspected Illegal Behaviour

1.5.1. Where circumstances brought to the Chief Operating Officer's attention constitute grounds for reasonable suspicion that a student or member of staff is using the University's IT Facilities for the commission or attempted commission of a criminal offence, the Chief Operating Officer will contact the police.

1.5.2. The IT account and any associated hardware or peripheral devices may be preserved and quarantined pending further investigation by the University or the police.

1.6. General Guidance

1.6.1. Any access to the communications of an authorised user of the University's IT systems will be with as little intrusion and disruption to the communications of third parties that are unconnected to the authorised access as possible.

1.6.2. Those granted access must preserve the confidentiality of any private or personal data that may be viewed inadvertently.

1.6.3. Any material collected and/or summary reports created through this Procedure will be treated as confidential and will only be examined by those persons who are so authorised; be retained for the period deemed necessary for the specific purpose and in line with the University's Records Management Policy and Retention Schedule; be stored securely and marked according to the sensitivity of the material.

1.6.4. 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 copies of intercepted material and processed data will be destroyed after 28 days, but a record of the interception will be maintained.

1.6.5. Any person accessing the communications or data of a member of staff, student or authorised user through this Procedure must ensure that they have continued authorisation for access.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jeremy Maris	Client Services

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
1.1	D	23/05/2009	Document to ISC	JM
1.2	D	27/12/2009	Limited revision , Document to ISC	Iain Stinson
1.3	D	10/02/2010	Approval by ISC	Iain Stinson
1.4	I	09/10/2014	Approved by ISC	PD
1.5	D	06/2015	Reformatted. Add policy control page	SR
1.6	I	20 June 2017	Minor Amendments	MT
1.7	I	22 Mar 2018	Prevent made explicit	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued