SOP Title Reference: **Account Access**	Last Reviewed: **12/10/2017**	Last Revised: **22/09/2014**
Author: **IT Services**		

St George's
University of London

IT Services
IT Policies and Procedures

Institutional Access to Staff and Student IT Accounts and IT Equipment

IT Services, St George's, University of London, Jenner Wing, Cranmer Terrace, London SW17 0RE

Contents

1. Introduction

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.

This policy applies to all St George's University of London staff, students and any other authorised users of SGUL's IT equipment and facilities.

SGUL respects the privacy and academic freedom of staff and students. However, SGUL may carry out lawful monitoring of IT systems. Staff, students and any other authorised users should be aware that the University 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 University 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).

The policy was approved by the University's Strategy Planning and Resources Committee (SPARC) on 19th October 2011.

This document is based on a template prepared by JISC Legal, in conjunction with Pinsent Masons law firm, for use in the UK education sector.

2. SGUL'S powers to access communications

Authorised University staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or maintained (except where SGUL acts solely as a service provider for another body) by the University and may examine the content and relevant traffic data.

SGUL may access files and communications for the following reasons:

a) to ensure the operational effectiveness of the service. (for example, SGUL may take measures to protect the network systems from viruses and other threats such as hacking or denial of service attacks)

b) 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)

c) 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)

d) to investigate or detect unauthorised use of the systems (for instance, to check whether the user is breaking regulations)

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

f) 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)

g) to monitor whether or not communications are relevant to the business of the University (for example, to check an email account to ensure that it is not being used for excessive 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)

Requests for access must be authorised by one of the role holders specified on the front of the official request form.

3. The powers of law enforcement authorities to access communications

A number of non-institutional bodies / persons may be allowed access to user communications in certain circumstances. Where SGUL 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.

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, SGUL will provide reasonable assistance with the execution of a lawful warrant.

4. Policy on access to student accounts by other students

Students must not access the IT accounts of any other person, and must only use the institution's facilities in compliance with the SGUL Conditions of Use Policy.

5. Policy on access to staff and student accounts by authorised persons

For the purposes of this policy authorisation for access to staff or student accounts must come from one of the following people:

- a senior member of Registry (for student accounts)
- a senior member of HR (for staff accounts)
- the Director or a Head of Section for Corporate Services
- the Director or a Head of Section for Learning & Institutional Services
- an Institute Director or the Institute Head of Operations

Authorisation for account access requests will not be accepted from any other SGUL staff member and must be provided using the official request form.

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), SGUL will follow the procedure set out below:

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

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.

3) The person authorised to access the account is responsible for ensuring that only the specific authorised information is accessed and that other information is not read or disclosed.

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

Where circumstances brought to the authorised person's attention constitute grounds for reasonable suspicion that a student or member of staff is using SGUL's IT Facilities for the commission or attempted commission of a criminal offence, the authorised person should follow the relevant procedure(s) as laid out in the University's Information Sharing Protocol.

The IT account and any associated hardware or peripheral devices should be frozen pending further investigation by the University or the police.

5.3 Access to Student Accounts - Suspected Breach of SGUL's Regulations

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, an authorised person will record that the student's communications are being accessed.

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.

The relevant communications should be reviewed by an authorised person to assess whether the student has breached the University's rules and regulations (and where necessary the appropriate disciplinary investigation may be initiated).

5.4 Access to Staff Accounts - Suspected Breach of Terms of Contract of Employment

Where there are reasonable grounds to suspect that a member of staff is using SGUL'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.

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 a) above, authorisation will be requested from an authorised person.

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 may be initiated).

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

Any access to the communications of a member of staff, student or authorised user of SGUL systems will be with as little intrusion and disruption to the communications of third parties that are unconnected to the authorised access as possible.

Any communications collected under this policy will be treated as confidential and will only be examined by those persons who are so authorised.

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 policy on records retention.

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.

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 SGUL's Network Conditions Of Use Policy and the SGUL Information Sharing Protocol, and with any other relevant sections of the University's rules and regulations as applicable to students and relevant terms of SGUL's conditions of employment as applicable to members of staff.