SOP Title Reference: **ISP Guidance**	Last Reviewed: **12/10/2017**	Last Revised: **29/03/2017**	St George's University of London
Author: **IT Services**			

IT Services
IT Policies and Procedures

Information Security Policy
Guidance on proper & improper use of IT Services

(see also related documents 'Information Security Policy' and 'Information Security Policy Technical Annex')

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

Contents

1. Introduction

Personal computers with access to local networks, email facilities and the Internet are widely used in the Institution. Many members of staff depend on their use for teaching, research and for the administration of the everyday business of the Institution. Similarly students and others members of the Institution use personal computers for learning and research. Recent developments in legislation relevant to the use of computers bear on the Institution as an employer and on employees and students. The principal aim of this guidance is to disseminate a clear understanding of what constitutes acceptable use and unacceptable use; the guidance is not intended to limit or discourage use of computing facilities throughout the Institution.

In addition to this guidance, all users should be aware of the IT Conditions Of Use policy which is applicable to all users of systems and networks provided by the Institution, and the rules of the wider network provided by JANET (http://www.ja.net/company/policies/aup.html).

Acceptable use facilitates the purposes and aims of the Institution as an academic institution. With regard to all electronic communication, the Institution is committed to: -

- Encouraging and facilitating access to and dissemination of knowledge where that is appropriate

- Ensuring that computer usage does not breach either legislation or the IT Conditions Of Use or other requirements issued by the Information Services Department

- Protecting
    i. research data, including personal data collected for research purposes, held on computer or transmitted via email or the Internet.
    ii. the intellectual property of others.
    iii. the right of staff and students not to be subjected to discrimination.
    iv. staff, students and other members of the Institution community against any harm or mischief which might be inflicted on them by the misuse of computer systems by others.
    v. computer systems and data against any damage which might be caused by virus or other forms of contamination or misuse by individual members of staff
    vi. the Institution's resources.

- Protecting the privacy of communication by members of staff with their representatives, professional associations or trades unions, students, if appropriate, or any other third parties

- Respecting the rights of staff and students under legislation.

This list is not necessarily exhaustive.

2. Required Standards

2.1 General

- Reasonable personal use may be made of any computing facilities provided by the Institution. However, this personal use should not interfere with the performance of duties or cause any damage or difficulty to computers or to local networks, or any difficulty or distress to other members of the Institution’s community.

- Only properly licensed software may be installed on computers used within the Institution. Users have a responsibility for licensing and supporting software which is not issued by IT Services.

- Only IT Services’ staff may configure or modify PC network and security settings. The use of any software whose purpose is to disable or circumvent SGUL IT security settings and policies is additionally prohibited

- The institution’s computer facilities must not be used for private business purposes without the permission of the Director of Information Services or for private purposes which have more than a minimal impact on the Institution’s resources.

2.2 Email and the Internet

- Limited use of the Institution system is permissible for personal emails, provided that it does not have more than a minimal impact on resources and does not adversely affect work or that of others.

- If an email message is personal, it should be identified by the word ‘personal’ in the subject line.

- Email must not be used for trivial or frivolous purposes (such as circulating jokes to mailing lists).

- Institution email systems must not be used for the transmission of messages which could be regarded as harassment or which could be deemed defamatory or which are otherwise unlawful.

- Occasional internet access for other than strictly work purposes is permitted on condition that it does not adversely affect work and the work of others and has a minimal effect on the Institution’s resources.

2.3 Safeguarding University business data

- Important SGUL business information, operational documentation and data considered to be valuable University intellectual property should be stored on the appropriate SGUL central network drive where it will be routinely backed up.

- Cloud-based storage made available through the University's Microsoft Office 365 service, for example OneDrive, must not be used to store the *sole* copy of key University data. OneDrive may be used to collaborate on / share business documents and data with colleagues, either within or outside of the institution.

- Personally-owned devices, including removable media, should not be used to store confidential University data, personal or sensitive personal data for which the University is the data controller, or other business-critical data.

2.4 Staff absence and staff leavers

- Staff either leaving the University's employ or taking scheduled absence must make arrangements for handing over work-related files and email messages and any other important business information to colleagues *before* they go.

- Staff leaving the University's employ must also make sure they download and save information they wish to take with them *before* they leave. Staff who no longer work for the University and whose IT account has been closed will not be granted access to their data once they have left.

2.5 Data protection and security

All SGUL members must comply with the institution's Data Protection Policy, https://portal.sgul.ac.uk/org/lis/computing-services/policies/

In particular:

- Personal information and other confidential material must be guarded by the proper use of passwords and other security measures.

- If there is a concern about the inadequate protection of data, the Institution's Data Protection Officer must be informed so that any necessary steps can be taken to safeguard the data.

- The same standards of confidentiality must be observed for electronically-held or generated information as for information held on paper.

All members of the Institution have an obligation to protect data and systems by following up-to-date recommendations to avoid virus contamination. Guidance is available from the IT Services Department.

Any breach of confidentiality may be treated as misconduct or, if sufficiently serious, as gross misconduct.

3. Monitoring

In normal circumstances the confidentiality of files and email communications is guaranteed. However, the Institution reserves the right to listen to or have access to read any communication made or received by a member of the Institution using the Institution's computers or the telephone system without notice. The Institution has an obligation to ensure that all computer systems in the Institution are operated in accordance with internal regulations, with contractual agreements, with UKERNA and with legislation. Monitoring will only be carried out for the following purposes:

- to establish the existence of facts
- to ascertain compliance with regulatory or self regulatory practices
- for quality control and staff training purposes
- to prevent or detect crime
- to investigate or detect unauthorised use of the Institution's telecommunication system
- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding e mails to correct destinations
- to check email and voicemail systems when staff are on holiday or on sick leave.

The Institution also reserves the right to make and keep copies of telephone calls or emails and data documenting use of the telephone, email and/or the Internet systems, for the purposes set out above, and if it sees fit to use the information in disciplinary proceedings.

4. Misuse of Computing Facilities

The following examples of misuse are likely to be considered as gross misconduct and will be dealt with under the relevant disciplinary procedure:

- Hacking - attempts to access systems or data within or outside the Institution without authority, or encouraging others to do so.

- Deliberately accessing from the Internet material which is counter either to legislation or to commonly accepted standards, is likely to be offensive to reasonable people, or breaches the Institution's equal opportunities policy, e.g. racist material or pornography. Such access is permitted only for bona fide academic and related purposes. If an Internet site which contains offensive or unacceptable material is accessed accidentally, the matter should be reported immediately to the Director of Information Services.

- Email communications with others which constitute bullying or harassment as defined in the Institution's policies on bullying and harassment.

This list is not exhaustive.

5. Investigation of Misuse

Normally the privacy of members of the Institution's personal computers will be protected. However, an investigation into misuse of computing facilities may require the inspection of any files held on any of the Institution’s computing systems. In such cases, the Director of Information Services is authorised to give permission for such access. Access will only be allowable in so far as it is necessary for the Institution to comply with national legislation, e.g. the Regulation of Investigatory Powers Act 2000 and the Lawful Business Regulations.

In such cases the consent of the individual member of the Institution will normally be sought. However in certain circumstances access may be obtained without consent, e.g.

i. if member of staff is absent and it is impossible to contact him/her and access is needed to provide information crucial to the Institution

ii. if there is prima facie evidence that a member of staff may be misusing facilities to an extent, or in ways which would be considered serious or gross misconduct or there is a need to initiate an investigation and there is a possibility that evidence might be destroyed.

The procedure will not be used to breach privacy in situations other than those where the Network Conditions of Use and the Required Standards (section 2) have not been respected. The privacy of members of the Institution will be respected in other situations, and that privacy will be protected especially in connection with the areas defined in the Introduction.

As part of normal procedures, computers linked to networks may be scanned automatically for virus and similar contamination and the Director of Information Services may authorise the routine monitoring of email traffic (but not content) and of Internet access within the Institution's networks.

6. Misuse and Disciplinary Action

The Principal in consultation with the Head of Human Resources (HR) or Academic Registrar as appropriate should decide in the light of the outcome of an investigation of possible misuse of computing facilities whether disciplinary action is appropriate, and if it is judged appropriate, instigate necessary action in accordance with the relevant disciplinary procedure.

Heads of Divisions should consult with the relevant HR Officer or the Academic Registrar as soon as any instance of apparent misuse comes to his or her attention.