UNIVERSITY POLICY ON THE USE OF COMPUTING FACILITIES AND RESOURCES

Table of Contents

1. Guiding Philosophy

The guiding philosophy of this policy is that the University's computing facilities should be used in a manner which is ethical, legal, appropriate to the University's aims, and not to the detriment of others. The policy sets out the conditions for use of the University's IT facilities and demands that information in electronic format is used and managed according to the same principles as is normally applied to printed materials.

2. Scope

This policy covers the use of all computing facilities and resources administered by the University of Strathclyde, whether on- or off-site, including use by staff and students of the University and by any other person authorised to use these facilities. It covers use on University premises and through any networked links to the University's computing facilities. Any registered user using any kind of computer hardware or software, for any purpose, at the University or connecting and authenticating to the University's network from a remote location, even if it is their own or a third party's equipment, and even if it is only connected to the institution through a network, is required to abide by the terms of this policy. Any equipment owned by the University, is covered, even if used at a remote location.

In this policy computing facilities and resources includes services such as those provided by Information Services or by any other department, faculty or directorate of the University. This includes any services delivered for the University via an external partner. Such facilities and resources include fixed and mobile computing devices; any associated software, data or electronic resource, including data created by others, and the networking elements which link the facilities together.

3. Access to Facilities

- Computing facilities are provided for authorised users, solely for use in connection with the aims and purposes of the University. Computing facilities may be used for limited personal use, so long as that use is not at odds with the underlying philosophy of this policy and does not in any way interfere with the aims and purposes of the University or the responsibilities that individuals have to the University. Such limited personal use must not include use for commercial purposes.

- On special application being made, the University may authorise the use of its computing facilities for work outside the scope of normal University purposes, including by third party organisations. Any charges for provision of such facilities will be determined by the Director of Information Services. Other use may be allowed, by agreement with the Director of Information Services, as a privilege not a right, and if abused may be deemed to be a breach of this policy. Any such special application should be made in writing to the Director of Information Services.

- The majority of University resources will be accessed via individual University accounts. For access to core services this will be automatically created for both staff and students prior to their arrival at the University. For some specialist resources personal accounts are created separately.
- Bona fide visitors to the University, people working for the University temporarily, and third parties who require remote access to University services may be eligible to have accounts created via the IT Temp Access Process or Limited Access Accounts.
- The Director of Information Services may permit other legal entities to connect to the University network under the terms and conditions laid down by JANET (UK).

4. Conditions for Use – Rights and Responsibilities

- All users are bound by the University Policy on the Use of Computing Facilities and Resources as soon as they access such a University resource.
- Users must also comply with relevant legislation. Users should review the Legal Framework for ICT
- Users will be held responsible for any and all activity on computing facilities which is initiated by their user ID. Accordingly, it is forbidden for a user to allow any other person access to their user ID or password. Users should not use another person's user ID or password; or modify or interfere with information belonging to another user without appropriate permission
- If a user suspects that the security of their computing facilities has been breached or compromised it should be reported to the Information Services IT Help Desk.
- It is the responsibility of every user to act in a manner which will not cause damage to computing facilities, communications network, systems programs or stored information, nor adversely affect the performance of any service available on these facilities.
- Users of a resource, service or software (including remote resources) must comply with the licence conditions associated with that facility.
- Users must comply with good Information and Records Management practices, as advised by the University Records Management Guidance.
- No user will connect to the University network any piece of equipment, which by its function could adversely affect the performance of the network. Any user connecting their own equipment to the University network agrees that by doing so the Director of Information Services has the right to audit the equipment and data stored on it at any time. Users connecting their own equipment to the University's network directly or remotely must adopt appropriate security measures for their own equipment, including using encryption when appropriate, setting passwords, and installing anti-virus and firewall software.

- The University of Strathclyde will not permit the use of its computer facilities and resources for the access to or transmission of information which is considered by the University to be unacceptable; illegal; in breach of University policies, such as those on Equal Opportunities and Harassment; in breach of the appropriate research ethics guidelines; wasteful of resources; or not commensurate with the provision of facilities for legitimate purpose relating to the aims of the University.
- The University may actively monitor usage of University computer facilities and resources. This may include monitoring access to publication or receipt of any Internet materials by any user. It reserves the right to remove from the University systems any material which, in the opinion of the Director of Information Services, is considered unacceptable according to the policy. It is University policy to provide information obtained by monitoring, when required to do so by external agencies operating within the Scottish legal framework.
- The University may require access to information stored on the facilities provided by it for legal or business continuity purposes. This will include information stored on accounts issued to individuals for communication or information storage purposes. For more information see Procedure for Accessing Personalised Electronic Storage Resources
- On receipt of an appropriate request from legal or regulatory bodies, or an internal investigator the Chief Operating Officer may require any user holding or transmitting encrypted information to provide appropriate de-encrypting tools/keys to those bodies and/or the University.

5. Misuse – Penalties and Sanctions

- Breaches of this policy by staff or students will be dealt with under the appropriate disciplinary procedures. Where an offence may have occurred under criminal law it will be reported to the police or other appropriate authority. Individuals could also be personally liable for their actions under civil law.
- Where appropriate, staff or students at the University of Strathclyde or other authorised users may have their use of the University's computing facilities immediately suspended pending an investigation by an authorised person in the University. This suspension can be authorised by a member of the management team of Information Services.
- In the event of loss being incurred by the University, or members of the University, as a result of a breach of these regulations by a user, that user may be held responsible for reimbursement of that loss.

6. Ownership, Monitoring and Review

This policy is owned by the University's Information Strategy Committee. The day to day management and monitoring of it is delegated to the Information Services Directorate. It should be reviewed biennially.

7. Further Relevant Information

Legal Framework for ICT

Policy for Providing Access to Personal Allocated Resources

Network Connection Policy

Bring Your Own Device Policy

Policy on IT Access for Leavers

Records Management: Best Practice Guidelines on Information and Records Management

Records Management: Email Management

Records Management: Information Security

Records Management: Determining if Information is Confidential

Records Management: Information & Records Management Top Ten key Points.