SRUC
Acceptable Use of IT Facilities Policy - Students

Introduction

This policy is a part of SRUC's wider policy framework and any internal codes of conduct as can be found in the Education Manual.

Purpose

This policy covers the acceptable use of all computing facilities administered by SRUC for the use of students. This policy is a snapshot of standards that govern the use of computing facilities and full details can be found in the links provided at the end of this document.

Scope

This policy applies to all students of SRUC, irrespective of mode of study.

The policy applies to all locations from which SRUC information is accessed including home use.

Lines of responsibility

By using SRUC's compute facilities you agree to:

- SRUC's primary external network is JANET and the acceptable use of this network can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy
- Manage your password in line with the guidance provided, which requires you to keep passwords confidential, with a minimum length of 12 characters and not easily guessable.
- Use the internet and social media within the guidance provided, which prohibits you from accessing undesirable information, downloading software without prior approval, storing personal information on SRUC systems and transferring sensitive information. It also requires you to consider the law around sharing of sensitive information, data protection and not to share information that is pornographic, violent, sexist, extremist and racist. Ensure that you read and understand SRUC's equality, diversity and inclusion policy which can be found at SRUC | Equality, diversity & inclusion
- SRUC licenses the use of computer software from a variety of outside sources. SRUC does not own this software or its related documentation and, unless authorised by the software license agreement, does not have the right to reproduce the software or its related documentation. Software shall

only be used in accordance with the appropriate license agreement. Every user must comply with the terms of any license agreement between SRUC and a third party which governs both the use of software and access to data.

And you will not:

- try to access, copy, or otherwise make use of any other user's software or data without permission. This includes another user's password (passwords should never be shared with others).
- attempt to access any system or data that you have not been given permission to use.
- knowingly introduce any virus or other harmful program or file into any computing facility, nor disable tools that protect against harmful programs.
- tamper with, disable, or work around the security technologies in place to protect SRUC data, its systems, or its staff and students.
- attempt to access secured systems to which you have not been granted access.
- use Computing Facilities to display, print, transmit or store text or images or other data which could be considered offensive such as pornographic, racially abusive or libelous material.
- make use of SRUC's computing facilities/social media to harass or bully any person or group of people.
- produce, use, or pass on material via SRUC's computing facilities/social media which could give SRUC, or any part of SRUC, a bad reputation.
- make any use of SRUC's computing facilities to engage in or assist in a criminal act.
- send unwanted and unapproved bulk e-mails. This includes, but is not limited to, advertisements, political and religious materials.

Monitoring and Evaluation

Under the Lawful Business Regulations (LBR), SRUC draws to the attention of all users the fact that their communications may be intercepted where lawful under RIPA 2000. Details can be found at Regulation of Investigatory Powers Act 2000 Approval to do so will be granted by the Registrar or a nominee.

Related policies, procedures and compliance with law

This policy forms part of the Information Security Policy Framework and it's underpinning policies, standards and SOPs, which are published on the SRUC website.

Standards specifically related to student use of compute facilities are as follows:

- Use of Email
- Use of the Internet and Social Media

- Password guidance and protection

All UK legislation is published at Legislation.gov.uk

Information Security Incident Reporting

An information security incident is any event that has or could result in loss, damage, modification or corruption of the key business functions.

In general, all IS security incidents should be reported immediately by calling Information & Digital Services on the direct line 4444 (Tel: 0131 535 4444).

Security incidents occurring outside normal working hours, including weekends, should be reported to Information & Digital Services Group Duty Manager: 07917 040662

Document Information

Policy owner	Information and Digital Services		
Approved by	SSEC		
Date of approval	25 February 2025		
Next review date	February 2027	Version	1
Distribution	SRUC Internet Pages Moodle IT help page for students		