SRUC (Scotland's Rural College)

Information & Digital Services Group

Acceptable Use of IDS Facilities Student Edition

Policy Owner	Information and Digital Services		
Approved by	SRUC Executive Leadership Team		
Date of approval (by ELT)	**1st March, 2019**		
Next review date	1/12/2023	Version	1
Distribution	IS Intranet policy page Moodle IT help page for students		

Contents

1 INTRODUCTION 3

2 ACCEPTABLE USE POLICY 4

3 E-MAIL 6

4 PERSONAL USE OF THE INTERNET 9

5 USE OF SOCIAL NETWORKING SITES, BLOGS AND OTHER PUBLIC FACING DIGITAL COMMUNICATIONS 10

6 PASSWORD PROTECTION 11

7 INTELLECTUAL PROPERTY AND SOFTWARE POLICY 12

8 MONITORING OF THE USE OF E-MAIL AND THE INTERNET 13

9 COMPLIANCE 14

10 POLICY REVIEW AND ASSESSMENT 15

11 APPENDIX A – DEFINITION OF SRUC COMPUTING FACILITIES 16

12 APPENDIX B – PASSWORD GUIDANCE 17

1 Introduction

This Policy applies to all student users of SRUC's information and digital services (as defined in *Appendix A*), at all SRUC campuses and sites. These facilities are provided for SRUC's business purposes and it is recognised that SRUC should provide guidance to users about the appropriate use of computing facilities, information and digital services (like software, programs, e-mail/Internet access, internal websites, etc.), and computing devices.

The sections of the Policy regarding misconduct and misuse should be read in alongside the SRUC Disciplinary Procedure.

1.1 Purpose, Scope and Applicability

This policy applies to the following people with legitimate access to SRUC data:

- SRUC Students

These facilities include central services such as those provided by the Information & Digital Services Group, Libraries, departmental computers, personal computers and peripherals, networks and all programmable equipment. Also included are any associated software and data and the networking elements which link the facilities together.

Any person wishing to use the computing services of associated Universities or Colleges (e.g. University of Edinburgh, University of the West of Scotland) will be required to follow their agreements for the use of their services in addition to the SRUC policy.

2 Acceptable Use Policy

SRUC's main purpose, in providing information and digital services, is to support the teaching, learning, research and approved business activities of SRUC.

(a) All authorised users shall be given a username and access to computing facilities, which may only be used for the purposes for which it was given.

By using SRUC's information systems and software, you agree to:

(b) abide by this and any other information security policies and codes of practice, issued from time to time.

(c) protect your software, data, passwords, and other resources from access by other users without your permission. Note passwords should never be shared.

(d) when using SRUC's computing facilities to create, store or share information or to access other computer networks or other computer-based communication systems, conform to the policies on acceptable use of these networks. SRUC's primary external network is JANET and a link to its policy is below:

- JANET Acceptable Use Policy: https://community.jisc.ac.uk/library/acceptable-use-policy

You agree that you will not:

(e) 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).

(f) attempt to access any system or data that you have not been given permission to use.

(g) knowingly introduce any virus or other harmful program or file into any computing facility, nor disable tools that protect against harmful programs.

(h) tamper with, disable, or work around the security technologies in place to protect SRUC data, its systems, or its staff and students.

(i) attempt to access secured systems to which you have not been granted access.

(j) 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 libellous material.

(k) make use of SRUC's computing facilities to harass or bully any person or group of people.

(l) produce, use, or pass on material via SRUC's computing facilities which could give SRUC, or any part of SRUC, a bad reputation.

(m) make any use of SRUC's computing facilities to engage in or assist in a criminal act.

(n) send unwanted and unapproved bulk e-mails. This includes, but is not limited to, advertisements, political and religious materials. Bulk e-mails must be approved by the Communications Department before being sent.

It is the responsibility of all SRUC users to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats to systems or services (observed or suspected) as soon as possible. These should be sent to the Group Manager of the Information & Digital Services Group. Investigations of system intrusions and other information security incidents are the responsibility of the Information & Digital Services Management Team.

SRUC has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

3 E-mail

SRUC e-mail accounts should not be used for personal e-mail communications.

E-mail should be treated like any other form of written communication and what is normally seen as unacceptable in a letter is equally unacceptable in an e-mail.

Use of personal e-mail or other internet services should not interfere with the performance of the student's duties.

Users should use extreme care before they open any attachment to an e-mail they receive and be sure that they are confident that the content is not obscene or defamatory. Equally, if an student receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, except to an investigator in the IDS Group.

The use of e-mail for either personal or SRUC purposes to send or forward messages or attachments which are defamatory, obscene or otherwise inappropriate would be treated as misconduct under the appropriate SRUC Disciplinary Procedure.

Where SRUC has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to monitor the destination, source and content of e-mail to and from a particular address.

3.1 Accessing of E-mail Accounts

In circumstances where access needs to be gained to student SRUC e-mail accounts, authorisation must be sought via the relevant Dean (or nominee).

3.2 Preventing the Spread of Malicious Software (Viruses)

Users of SRUC's computing facilities must take steps to prevent the receipt and transmission (by e-mail), of malicious software e.g. computer viruses. In particular, users:

- must not transmit by e-mail any file attachments which they know to be infected with a virus;
- must ensure that an effective anti-virus system is operating on any computer which they use to access SRUC computing facilities (advice on the level and types of effective anti-virus systems should be obtained from the Information & Digital Services Group);
- must not open e-mail file attachments received from untrusted sources.

3.3 Data Protection and E-mail

As members of SRUC, students are covered by the Data Protection Act.

This prescribes a number of further rights and responsibilities in using e-mail.

a) Personal data is subject to the Act. Under its terms, personal data includes any information about a living identifiable individual, including his/her name, address, phone number, and e-mail address. If users include such information in an e-mail or an attachment to an e-mail, they are deemed to be 'processing' personal data and must abide by the Act. Personal information includes any expression of opinion;

b) Users should be cautious about putting personal information in an e-mail. In particular, they should not collect such information without the individual knowing this is proposed; users may not disclose or amend such information except in accordance with the purpose for which the information was collected; and should ensure the information is accurate and up to date;
c) SRUC is permitted to process data for the following purposes: staff, agent and contractor administration; advertising, marketing, public relations; accounts and records; education; research; staff and student support services; other commercial services; SRUC bulletins/ magazine and journal publication; crime prevention, investigation and prosecution of offenders; alumni relations;
d) SRUC has by law to provide any personal information held about any data subject who requests it under the Act. This includes information on individual PCs in departments and users have a responsibility to comply with any instruction to release such data made by the Data Protection Officer. E-mails which contain personal information and are held in live, archive or back-up systems or have been 'deleted' from the live systems, but are still capable of recovery, may be accessible by data subjects. In certain circumstances, defined in the Act, SRUC may not be required to provide personal information held about a data subject. An example is where responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.
e) The law also imposes rules on users in retaining personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected. The Information & Digital Services Group has a retention procedure for deleted e-mails to allow for accidental loss or any other later requirement by the user for it to be retrieved;
f) Users should take care when sending e-mails containing personal information to countries outside the European Union, especially if those countries do not have equivalent levels of protection for personal data;

3.4 Legal Consequences of Misuse of Electronic Communications

In a growing number of cases involving the civil or criminal law, e-mail and instant messages (deleted or otherwise) can be produced as evidence.

There are a number of areas of legislation which apply to use of e-mail, instant messages, and other electronic communications which could involve liability of users or SRUC. These include the following.

1. ***Intellectual property:*** Anyone who uses e-mail to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.
2. ***Obscenity:*** A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly, the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.
3. ***Defamation:*** As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the e-mail and may lead to substantial financial penalties being imposed.
4. ***Data Protection:*** Processing information (including photographs) which contains personal data about individuals requires the express written consent of those individuals. Any use of personal data beyond that registered with the Data Protection Commissioner will be illegal.
5. ***Discrimination:*** Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 where it involves discrimination on the grounds of sex, race or disability.
6. ***Terrorism:*** Any material disseminated which is glorifies, incites or encourages terrorist acts may be unlawful under the Terrorism Act 2006, or the Anti-terrorism, Crime and Security Act 2001.

The above is only designed to be a brief outline of some of the legal consequences of misuse of e-mail facilities and electronic communications.

4 Personal Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for research purposes and access to relevant tools and materials in order to enhance the ability of its students to undertake their studies.

However, as with e-mail, it is legitimate for users to make use of the Internet in its various forms for personal purposes as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Users may:

- transfer information of a confidential or sensitive nature over the Internet only if protected by an encryption product that is approved by the Group Manager of Information & Digital Services (or nominee), who should be contacted to confirm the details of approved products
- download software from the Internet onto SRUC systems, only with the prior written approval of the Group Manager of Information & Digital Services (or nominee) for each download
- not access undesirable information. Undesirable materials include, but are not restricted to pornographic, violent, sexist, extremist and racist material, and gambling sites.
- not use SRUC systems for storage of personal music, video or photo collections or other data of a personal nature.

IDS will routinely block sites which appear on national information security databases as malicious or inappropriate for business use.

Unauthorised use of the Internet will be treated as misconduct under the appropriate SRUC Disciplinary Procedure.

5 Use of social networking sites, blogs and other public facing digital communications

All policies and guidelines that apply to spoken and written communication, whether face-to-face, or by telephone and e-mail, and to use of the internet, apply equally to social networking sites and blogs, personal web pages, and other public facing digital commuications channels. These include such as Facebook, LinkedIn, Instagram, Twitter, and other services that make personal views available to the general public.

Misuse of these services may constitute misconduct (or gross misconduct) in the same way as misuse of any other medium of communication and is therefore subject to appropriate disciplinary procedures.

Users of such services should ensure that personal views:

- do not make any comment about SRUC, its staff, or its students that is libellous, racist, sexist, or is otherwise abusive, threatening, defamatory or disparaging
- do not make any comment about SRUC, its staff, or its students that brings some, or all, of these into disrepute
- do not disclose confidential, or commercially sensitive material relating to SRUC, its staff, or its students
- do not include text or graphical material (e.g. logos or photographs) that may imply that the views expressed represent those of SRUC, its staff, or its students

If there is any doubt about the propriety of comments, or of all or part of a website, users should seek guidance from Information and Digital Services.

5.1 Initiation of social networking, cloud facilities or other SRUC business related web sites on behalf of SRUC

It is appreciated that social networking sites such as Facebook and Twitter or other Internet-accessible sites may have a business utility for SRUC. While it is not possible to control the external site content that may subsequently be displayed by non-SRUC personnel, it is essential that the creation or use of SRUC-branded sites:

a) is approved for use before being created.
b) provides sufficient identity regarding responsible SRUC staff, and
c) has mechanisms in place to regularly monitor and edit content in the interests of SRUC.
d) has mechanisms in place to ensure underlying technology is secure and regularly patched.

Permission for the use of such sites will require authorisation by the Head of Communications and the Group Manager of Information & Digital Services (see Appendix A).

If a member of the media or non-traditional media contacts the user about SRUC's business, the request must be referred to the Communications Unit.

Unauthorised creation of sites that are branded as, or could be interpreted to be, Institutional or supported by SRUC staff will be treated as misconduct under the appropriate SRUC Disciplinary Procedure.

6 Password protection

It is essential that all students are aware of the requirements for password selection and usage within SRUC.

Users are required to follow good security practice in the selection and use of passwords on IT systems operated by or on behalf of the SRUC.

Users must:

- keep passwords confidential
- not share individual user passwords
- not keep records of passwords on paper or digital means unless using a tool approved by IDS
- change passwords whenever there is a suspected password compromise or if a password has been disclosed
- ensure that passwords allocated or re-set by a system administrator must be changed on the first occasion that the users subsequently access the system
- avoid re-using passwords from the past or other systems or accounts

Students should not disclose passwords to any other person, with the exception of authorised personnel in HR and Information & Digital Services Groups where there is a valid business reason for the request being made.

Password Guidance may be found in Appendix B.

7 Intellectual Property and Software Policy

The information, data and programs developed or produced by employees or provided by the organisation are assets belonging to SRUC. They must not be altered, transmitted, removed or deleted without proper authorisation.

All users are responsible for ensuring that viruses are not introduced into SRUC computers.

Only authorised software can be used on any computer owned by SRUC.

a) 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.
b) Software shall only be used in accordance with the appropriate licence agreement. Every user must comply with the terms of any licence agreement between SRUC and a third party which governs both the use of software and access to data.
c) Students learning of any misuse of software or related documentation shall notify their tutor or Group Manager as soon as possible.
d) According to UK Copyright law, persons involved in the illegal reproduction of software can be subject to unlimited civil damages and criminal penalties. SRUC does not condone the illegal duplication of software. SRUC students who make, acquire or use unauthorised copies of computer software will be subject to disciplinary procedures.

8 Monitoring of the use of e-mail and the Internet

It is SRUC's policy that no unauthorised member of SRUC is permitted as a matter of routine to monitor a fellow employee's or student's use of SRUC's telephone or e-mail services, or of the Internet via SRUC's networks.

Authorised monitoring includes

a) normal network and systems monitoring by IDS in order to enforce the rules outlined in this document

However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, a senior HR Manager (or their duly authorised nominee), may grant permission for the monitoring of a student's use of e-mail or the Internet. Managers who suspect misuse should in the first instance advise, in confidence, a Human Resources Manager.

8.1 Interception, monitoring and logging

SRUC may make interceptions for the purposes authorised under the *Regulation of Investigatory Powers Act 2000*.

The provisions of this Act are essential information to users of SRUC's computing facilities about what does, and does not, constitute acceptable use.

All inappropriate use of computing facilities, including e-mail and the Internet, no matter how encountered, will be investigated. SRUC reserves the right to investigate and inspect electronic communications, under the terms of the Act.

Electronic communications include files, access logs, e-mail, messaging and similar "chat" services, blogs, and social networking websites – for example, Facebook, Twitter, etc.

Electronic communications relating to individuals may be monitored in the following circumstances:

a) in the investigation of an incident – for example, alleged contravention of SRUC's rules, regulations, contracts, codes of practice, etc - or alleged criminal activity

b) investigation of abnormal systems behaviour in an operational context – for example, abnormally high network traffic from a particular device, degradation of systems for other users resulting from the activity on a particular device, etc

c) problem-solving – for example, ensuring that a data transfer takes place. In normal circumstances, the responsible user would instigate such actions, but, on occasions, the intended recipient may raise the query when the sender is unavailable

d) to establish charges where these are based on utilisation of electronic resources.

9 Compliance

Where there is a breach of Policy, SRUC will act promptly to stop the breach or correct the problem, and to prevent the breach from happening again. This action may involve the appropriate member(s) of management, Human Resources and the Information & Digital Services Group working together.

Subsequent action may include:

- Indications of non-compliance with the provisions of the Policy will be investigated, as appropriate, in accordance with the provisions of the appropriate SRUC Disciplinary Procedure.
- Subject to the findings of any such investigation, non-compliance with the provisions of the Policy may lead to appropriate disciplinary action.
- Some breaches of policy may be more than just a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action.

9.1 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**

10 Policy review and assessment

This Policy may be amended by SRUC from time to time and will be reviewed after 12 months to consider changes in legislation and best practice.

10.1 Policy approval

This Policy is endorsed by the Executive Leadership Team.

Group Manager – Information & Digital Services

Advice and guidance on the operation of this policy is available. For further information and advice on the implementation of the guidelines please contact the Group Manager – Information & Digital Services.

11 Appendix A – Definition of SRUC Computing Facilities

(a) The phrase, "**computing facilities**", as used in this, and in all other SRUC policies and regulations, shall be interpreted as including:

- any computer hardware or software owned or operated by SRUC
- any rooms or other accommodation managed by SRUC that contain computing equipment
- any allocation of time, memory or other measures of space on any of SRUC's computer hardware, software, rooms, networks or links to networks
- any of SRUC's computer networks or other communications systems involving computers
- any of SRUC's connections to external computer networks or information or communication systems involving computers
- any computer hardware or software connected to SRUC's networks, either on campus, or elsewhere

(b) The phrase, "**SRUC computing facilities**" shall be interpreted as including the computing facilities of any part of SRUC and its associated campuses, regional offices, local offices, farms, and other sites, etc.

~~(c)~~ The designation, "**Group Manager of Information & Digital Services**", is applied to the person nominated by the SRUC Executive to hold responsibility for all SRUC Information & Digital Services and for the security and integrity of these systems.

(d) The designation, "**Data Protection Officer**", is applied to the person nominated by the SRUC Executive to ensure that SRUC fulfils its obligations under the terms of the *Data Protection Act*.

12 APPENDIX B – Password Guidance

Password Style

Passwords must be a minimum of 12 characters long and require a mix of the following:

- lowercase letter;
- uppercase letter;
- number;
- special character (examples: ! £ $ % & *).

Three of these four options above must be included within your password. Passwords must only be changed under instruction from IDS support.

Password Selection

Longer passwords are safer than shorter passwords. Passwords based on sentences or phrases with punctuation can be long and easily include the mix of options in the password style while still remaining memorable.

To reduce the chance that a password is not compromised, users should **not** base their passwords on any of the following:

- the last 3 passwords used
- logon name;
- surname, first name, initials or car registration numbers;
- birthdays, addresses or phone numbers;
- months of the year or days of the week;
- names of friends, family or pets;
- telephone numbers or number patterns (e.g. 345543).

End of Document