SRUC (Scotland’s Rural College)

Information and Digital Services

Acceptable use of IS Facilities

<table>
<thead>
<tr>
<th>Policy Owner</th>
<th>Information and Digital Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by</td>
<td>SRUC Executive Leadership Team</td>
</tr>
<tr>
<td>Date of approval</td>
<td>13 August, 2018</td>
</tr>
<tr>
<td>(by ELT)</td>
<td></td>
</tr>
<tr>
<td>Review date</td>
<td>13/8/2019</td>
</tr>
<tr>
<td>Version</td>
<td>5</td>
</tr>
<tr>
<td>Distribution</td>
<td>IS Intranet policy page</td>
</tr>
<tr>
<td></td>
<td>Moodle IT help page for students</td>
</tr>
</tbody>
</table>
# Contents

1 INTRODUCTION .......................................................................................................................... 3

1.1 Purpose, Scope and Applicability ................................................................................................. 4

2 GENERAL ......................................................................................................................................... 5

3 TELEPHONES ............................................................................................................................... 7

4 E-MAIL ........................................................................................................................................... 8

4.1 Accessing of Email Accounts ........................................................................................................ 8

4.2 Preventing the Spread of Malicious Software (Viruses) ............................................................... 9

4.3 Data Protection and E-mail ........................................................................................................... 9

4.4 Legal Consequences of Misuse of E-mail Facilities .................................................................... 10

5 USE OF THE INTERNET ................................................................................................................. 11

5.1 Use of social networking websites and blogs .............................................................................. 12

5.2 Initiation of social networking websites on behalf of SRUC ....................................................... 12

6 PASSWORD PROTECTION ............................................................................................................ 13

6.1 Sharing of usernames and passwords ......................................................................................... 13

6.2 Clear screen procedures .............................................................................................................. 14

7 MONITORING OF THE USE OF TELEPHONES, E-MAIL AND THE INTERNET ......................... 15

7.1 Interception, monitoring and logging .......................................................................................... 15

8 BREACH OF POLICY .................................................................................................................... 16

9 POLICY REVIEW AND ASSESSMENT ....................................................................................... 17

9.1 Policy approval .............................................................................................................................. 17

10 APPENDIX A – DEFINITION OF SRUC COMPUTING FACILITIES ........................................... 18

11 APPENDIX B – SRUC POLICY REGARDING THE USE OF COMPUTER SOFTWARE ................. 19

12 APPENDIX C – PASSWORD PROTECTION ................................................................................. 20
1 Introduction

The provisions of this Policy apply to all users of SRUC’s computing facilities (as defined in Appendix A), at all SRUC campuses and sites, whether or not they have access to, or sole use of, a telephone, e-mail or the Internet on a personal computer. 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 telephones and e-mail/Internet access in order to safeguard the interests of both members of staff/students and SRUC.

The Policy is not intended to place users under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, fax, telephones and the Internet.

It should be noted that the Policy governs the use of telephones, including mobile phones, fax and e-mail/Internet access provided on Personal Computers, or in computer clusters, to users to allow them to undertake their SRUC employment duties/studies.

The sections of the Policy regarding misconduct and misuse should be read in conjunction with the SRUC Disciplinary Procedure (accessible for staff on SRUC’s staff intranet under the Human Resources Policies and Procedures Section, with hard copies obtainable from the Human Resources Department, or, for students, within the Virtual Learning Environment system).

This Policy has also been designed to safeguard the legal rights of members of staff and students under the terms of both the Data Protection Act and the Human Rights Act.
1.1 Purpose, Scope and Applicability

This policy applies to all employees of SRUC (permanent, fixed term and casual), to all SRUC students, and to guests using SRUC’s computing facilities, including WiFi. Collectively, these are referred to as users of SRUC’s computing facilities.

These facilities include central services such as those provided by the Information and Digital Services Group, Libraries, departmental computers, personal computers and peripherals, networks and all programmable equipment as well as any associated software and data and the networking elements which link the facilities together. See Appendix A for a definition of SRUC’s computing facilities.

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 adhere to a separate agreement for the use of such service in addition to the SRUC policy.
2 General

SRUC’s main purpose in providing Information and Communications Technology (hereafter ICT, or computing facilities) is to support the teaching, learning, research and approved business activities of SRUC.

(a) All authorised users shall be allocated a user name, which, together with any computing facilities authorised, may only be used for the purposes for which they have been allocated.

(b) Users shall abide by SRUC’s Policy Regarding the Use of Computer Software, issued from time to time by the Information and Digital Services (see Appendix A). The policy regarding the use of Computer Software is summarised at Appendix B.

(c) Users shall not attempt to gain access to, copy, or otherwise make use of any other user’s software or data. This includes acquiring knowledge of any other user’s password.

(d) Users shall take all reasonable precautions to protect their software, data and other resources from unauthorised access by other users.

(e) Users shall not disclose their usernames or passwords to any other person, nor shall they use or attempt to use any system which they have not been authorised to use.

(f) Users shall not knowingly introduce any virus or other harmful program or file into any computing facility, nor take deliberate action to circumvent any precautions taken, or prescribed, by SRUC to prevent this.

(g) Users shall not attempt to gain access to systems management facilities or other facilities not available for general use.

(h) Computing facilities shall not be used 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.

(i) No one shall make use of SRUC’s computing facilities to harass any person or group of people.

(j) No one shall produce, use, or promulgate material via SRUC’s computing facilities which could bring SRUC, or any part of SRUC, into disrepute.

(k) No one shall make any use of SRUC’s computing facilities to undertake or assist in a criminal act.

(l) The sending of unsolicited and unapproved bulk e-mail to third parties is not permitted. This includes, but is not limited to, advertisements, political and religious materials. Bulk e-mails must be approved in advance of transmission.

(m) Any use of SRUC’s computing facilities to create, store or disseminate information or to access external computer networks or other computer based communication systems must 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:

(n) Some software and data are provided by agreement with CHEST (Combined Higher Education Software Team). Users must comply with the CHEST code of conduct, available by request or at http://www.eduserv.org.uk/codeofconduct.aspx, and in particular must acknowledge copyright for any products used. Note that a user’s obligations become binding as soon as a person uses licensed software or data regardless of whether or not the form has been signed.

(o) Users shall abide by the information security policies and codes of practice as issued from time to time by the Information and Digital Services (see Appendix A).

(p) 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.

(q) You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. SRUC reserves the right to block or monitor access to such material.
3 Telephones

It is recognised that there will be occasions when users need to make short, personal telephone calls on SRUC telephones, both fixed lines and mobiles, in order to deal with occasional urgent domestic problems. It is considered unlikely that such occasions would arise at weekends, or during periods of leave, and SRUC telephones should not be used for personal calls in those circumstances.

Other non-urgent personal calls should be made using public payphone facilities located in SRUC buildings or by use of personal mobile telephones. Alternatively, the personal charge cards issued by the various telephone companies can be used on SRUC telephones to ensure that the cost of the call is charged to an individual's private account. Where possible, these non-urgent calls should be made during scheduled breaks or outside of the normal working day when they do not interfere with work requirements. Equally, it is legitimate to receive personal calls about domestic crises and arrangements, and occasional, short, non-urgent calls can be received providing they do not interfere adversely with work requirements.

Premium-rate telephone services not directly connected with SRUC related work are not permitted. If such services are used the onus is on the employee/student to show that such calls are for strictly business purposes. The repeated use of such services for non-business purposes shall constitute a disciplinary offence.

The use of SRUC telephones for private purposes, which are in any way excessive (i.e. outside of the limits defined above), and any calls which are defamatory, obscene or otherwise inappropriate, will be treated as misconduct under the appropriate SRUC Disciplinary Procedure.

Where SRUC has grounds to suspect possible misuse of its telephones, it reserves the right to monitor the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of call content, but, in certain rare circumstances, where there are reasonable grounds to suspect serious misconduct, SRUC reserves the right to monitor the duration, source, destination and content of calls.
4 E-mail

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

It is recognised that a personal e-mail account may be used in certain circumstances - as long as such personal use is confined to non-working hours or during break periods and does not interfere with SRUC business.

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

It is legitimate for users to make use of personal e-mail accounts outside of the normal working day or during break periods for personal reasons to send messages, provided that they are in no sense obscene or defamatory or otherwise inappropriate. Personal e-mail use should not interfere, either by its timing or extent, with the performance of the employee’s/student’s duties.

Users should exercise extreme care before they open any attachment to a personal e-mail they receive, and be sure that they are confident that the content is in no sense obscene or defamatory. Equally, if an employee/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 IS Group.

The use of e-mail for either personal or SRUC purposes to send or forward messages or attachments which are in any way 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.

4.1 Accessing of Email Accounts

SRUC also reserves the right to access an employee’s SRUC e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee’s normal role. In normal circumstances, where it is possible to contact the employee concerned, this will be with her/his prior knowledge. Any accessing of employees’ SRUC e-mail accounts must only be done with the express permission of Human Resources Head (or nominee). The request can be made on the ‘Request to Access User’s Account Form’ – a copy of which can be located on the Intranet.

While SRUC reserves the right to access an employee’s SRUC e-mail account, individual staff may not access another user’s SRUC email account without prior written permission from the owner of the email account. In the case of an employee’s unexpected or prolonged absence, this permission must be obtained from the Head of Human Resources as detailed above. If a user has to access someone else’s account to carry out their normal duties (e.g. in the case of a PA to a Group Manager, or Head of Division) then this should be done by setting up a delegated profile. The owner of the email account must clarify this arrangement by completing a ‘Request to Access User’s Account Form’ – a copy of which can be located on the Intranet.

Once the form has been completed it should be sent to the IS Group for filing and future reference.
In circumstances where access needs to be gained to student e-mail accounts, authorisation must be sought via the relevant Senior Tutor (or nominee).

### 4.2 Preventing the Spread of Malicious Software (Viruses)

Users of SRUC’s computing facilities must take all reasonable 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 IS Group);
- must not open e-mail file attachments received from unsolicited or untrusted sources.

### 4.3 Data Protection and E-mail

As members of SRUC, employees and students are covered by the Data Protection Act (2018).

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) Users should not leave a computer physically insecure (e.g. in an unlocked room or not keyboard locked) or in such a state that a third party could inspect e-mail or data and gain access to personal information;

e) 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.

f) 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 IS 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;

g) 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;
4.4 Legal Consequences of Misuse of E-mail Facilities

In a growing number of cases involving the civil or criminal law, e-mail messages (deleted or otherwise) are produced as evidence in a permanent written form.

There are a number of areas of legislation which apply to use of e-mail and 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 1989, the Children Act 2004 and Protection of Vulnerable Groups (Scotland) Act 2007 make 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 Counter Terrorism and Security Act 2015

The above is only designed to be a brief outline of some of the legal consequences of misuse of e-mail facilities.
5 Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information for research purposes in order to enhance the ability of its staff to undertake their SRUC role.

However, as with e-mail, it is legitimate for users to make use of the Internet in its various forms outside normal working hours 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.

It is recognised that there can be occasions where it is sensible for the user to make occasional use of the Internet for personal reasons such as a private transaction, rather than having to spend considerably more time out of SRUC. Examples of this might include a bank transaction or the booking of a holiday. As long as such personal use is confined to non-working hours or during break periods, then it is permissible.

Users may:

- transfer information of a confidential or sensitive nature over the Internet only if protected by an encryption product that is approved by Information and Digital Services, who should be contacted to confirm the details of approved products
- only use Internet access that is provided by centrally managed services
- download software from the Internet, only with the prior written approval of the Group Manager of Information and Digital Services (or nominee) for each download
- make occasional and reasonable use of personal e-mail (e.g. Hotmail) and social networking websites (e.g. Facebook, Twitter) during breaks, outwith working hours, etc.
- not access undesirable information. Undesirable materials include, but are not restricted to pornographic, violent, sexist and racist material, and gambling sites

"Reasonable use" includes occasional use during designated breaks or outside normal working hours of the Internet for personal research, shopping, accessing personal email and social networking sites, etc. Confidentiality of personal information that is given to, or is made accessible to third parties, is not guaranteed by SRUC.

The upper limit of "reasonable use" of SRUC's computer facilities for personal purposes is set at 5 hours per week.

Unreasonable use includes sustained or regular access to the Internet for personal purposes; storage of personal music, video or photo collections; on line gaming; use of SRUC mobile phones for prolonged personal reasons; using facilities to run any form of business that is not part of SRUC.

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

SRUC reserves the right to monitor the use of the Internet from any devices attached to SRUC networks where SRUC suspects misuse of the facility. Internet use shall include personal e-mail accounts, instant messaging, telephones and internet browsers.

SRUC reserves the right to access any user accounts where misuse is suspected.
5.1 Use of social networking websites and blogs

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 accessible space through the internet. 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
- are not expressed during working time, except with prior approval of line management
- in situations where the user acknowledges they are employed by/have a relationship with SRUC, personal comments should include a disclaimer advising that the comments do not represent the views of SRUC

If there is any doubt about the propriety of comments, or of all or part of a website, users should seek guidance from their line managers.

5.2 Initiation of social networking websites on behalf of SRUC

It is appreciated that social networking sites such as Facebook and Twitter 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 use of SRUC-branded sites:

(a) is approved for use before being released by SRUC staff,
(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.

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

As outlined in SRUC’s media relations policy, if a member of the media or non-traditional media (including bloggers) contacts the user about SRUC’s business, the request must be referred to the Communications Unit.
6 Unauthorised release of social networking 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.

Password protection

It is essential that all users (employees/consultants/contractors/students) are aware of the requirements for password selection and usage within SRUC. The following provides a framework for a password management system and provides guidance that must be followed and adhered to.

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;
- never insert a password in an email message;
- not use ‘Remember Password Feature’ in any application (e.g. Internet Browser);
- not keep paper records of passwords;
- change passwords at regular intervals (90 days maximum);
- change passwords whenever there is a suspected password compromise;
- 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 old passwords;
- not share individual user passwords.

Staff should not disclose passwords to any other person, with the exception of authorised personnel in HR and IS Groups where there is a valid business reason for the request being made. Staff must not give their password to their line manager or any other senior member of staff if they are requested to do so.

Where a user has either disclosed passwords or have been negligent in the security of passwords, this will be treated as misconduct under the appropriate disciplinary procedure.

6.1 Sharing of usernames and passwords

Staff must not share usernames and passwords. All staff with access to any of SRUC’s Business Systems should have their own username and login password that should not be divulged to any other person, or used by any other person.

IS staff will never ask for your password. If anyone asks you to reveal your password, you should refuse and report the occurrence to service desk immediately.
6.2 Clear screen procedures

Steps must be taken to avoid accidental disclosure of information to visitors and other non-authorised persons in a user’s work area. Computer screens should be switched off or switched to a display that does not contain sensitive or confidential information when non-authorised persons are able to view that screen. Note that it is not necessary to switch the computer off.

If the user is leaving the room, they should either log off the system completely or lock the screen (by using ‘Ctrl Alt Delete’ and then enter to confirm that you wish to ‘lock’ your workstation).

Locking your screen not only prevents someone else from using your PC, which is logged on in your name, but it also prevents someone from reading information on your screen which may be sensitive.

Users should be aware that they would be accountable for all terminal activity and transactions entered through their User ID whether or not they were present at the time. By locking the screen this will prevent unauthorised access to user’s PCs.

Where a user leaves either confidential or business sensitive documents on their computer screens which are open to scrutiny by a third party, this will be treated as misconduct under the appropriate SRUC Disciplinary Procedure.
7 Monitoring of the use of telephones, e-mail and the Internet

It is SRUC’s policy that no 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. (The only exception is where designated employees are authorised to receive print-outs of telephone call details from particular extensions for recharging purposes).

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

7.1 Interception, monitoring and logging


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.

This policy on the privacy and the interception of electronic communications is intended to achieve a balance between the rights to privacy of individuals and the need to protect SRUC and its users from the consequences of misuse, or of illegal activity.
8 Breach of policy

In circumstances where there is assessed to be a breach of Policy, SRUC will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate member(s) of management, Human Resources and the Information and Digital Services Group.

Subsequent action will be as described below.

- Indications of non-compliance with the provisions of the Communications 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 Communications Policy will lead to appropriate disciplinary action.
- Furthermore, publication of some materials may not only amount to 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 Policy review and assessment

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

9.1 Policy approval

Belinda Haig

Group Manager, Information and Digital Services, SRUC 14 August 2018

Executive Leadership Team, 14 August, 2018

Advice and guidance on the operation of this policy is available. For further information and advice on the implementation of the guidelines please contact Belinda Haig, Group Manager, Information and Digital Services. Telephone 0131 535 4015 or e-mail: belinda.haig@sruc.ac.uk
10 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, Information and Digital Services”, is applied to the person nominated by the SRUC Executive to hold responsibility for all SRUC Information Systems and for the security and integrity of these systems. At this time, (August, 2018) that person is Belinda Haig.

(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 2018. At this time, (August, 2018) that person is Colin Peebles.
11 APPENDIX B – SRUC Policy Regarding the Use of Computer Software

(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) Staff or 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 staff or students who make, acquire or use unauthorised copies of computer software will be subject to disciplinary procedures.
12 APPENDIX C – Password Protection

Password Style

Passwords must be a minimum of 8 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 and you must change your password every 90 days.

Password Selection

To ensure that any password’s integrity 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