SRUC (Scotland's Rural College)

Information & Digital Services Group

Acceptable Use of IDS Facilities
Staff & Contractors Edition

Policy Owner	Information and Digital Services		
Approved by	SRUC Executive Leadership Team		
Date of approval (by ELT)	**1 March, 2019**		
Next review date	1/12/2023	Version	7.1
Distribution	IS Intranet policy page Moodle IT help page for students		

Contents

1 Introduction

This Policy applies to all 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 anyone with legitimate access to SRUC data and systems, including but not exclusively to:

- Employees working for, or on behalf of, SRUC (both permanent, temporary or agency)
- SRUC Students
- Guests, Visitors and Contractors using SRUC's computing facilities, including WiFi. Together, these are referred to as users of SRUC's computing facilities.
- Associates or other third parties

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.

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:

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

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

(c) 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:

(a) 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).

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

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

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

(e) attempt to access the administrative or management portals to systems unless you are the owner or administrator of that system.

(f) 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.

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

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

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

(j) 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.

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 Chest - User obligations. The must acknowledge copyright for any products used.

> Note - 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.

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 Mobile Devices and Home Working Guidance

Laptops, tablet computers, smartphones, and other mobile devices provide users greater access to SRUC e-mail and data. All policies and guidelines that apply to computers apply equally to mobile devices.

You should ensure that the confidentiality of information is not disclosed when using mobile devices in public places to avoid the risk of information being viewed. Care should also be taken if discussing confidential information in public places and/or on public transport to avoid the risk of information being viewed or overheard by unauthorised people.

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

All mobile devices must have have power on passwords to protect not only the device itself, but also the data stored on the device. If the device is damaged or stolen, and you are found to be negligent, then you may be liable to pay any insurance claim.

All mobile devices must be encrypted except where noted below.

Personal/Home PCs and mobile devices should not be used to store SRUC data, including email, unless they comply with SRUC's information security requirements, i.e.:

- Data and hard drives on which it is stored are encrypted by default.
- Operating software can be shown to be up to date.
- Anti-virus is installed, up to date and operating correctly.
- Passwords meet SRUC's password security guidelines.
- Data is backed up elsewhere and protected from unwanted destruction, modification and corruption.

No non-SRUC-approved cloud services may be used to store SRUC data, including Email.

3.1 Encrypted Devices When Travelling

In some countries it is prohibited by law to own and use encryption technologies. Portable PCs or notebook computers containing encryption technologies must not be taken to these countries. The user has to comply with this regulation in his/her own interest and in the interest of the company (confiscation of equipment, data loss, etc). For advice contact Information & Digital Services on the direct line **4444 (Tel: 0131 535 4444)**.

4 Approved Mobile Devices

SRUC shall ensure that mobile devices adhere to a number of additional criteria, before allowing its use as an approved device to access corporate SRUC data and systems.

In particular, an “approved device” must:

- be updated with the most recent security updates as soon as they are available
- incorporate means to prevent unauthorised use of the device
- incorporate means to protect data on the device, including when a device is lost or stolen
- allow encryption of data in transmission to the device, by use of appropriate network protocols

SRUC shall use utilities to remotely manage mobile devices that have been approved for use within SRUC.

4.1 Prevention of unauthorised use

In order to prevent unauthorised use of a device, the device must allow SRUC to:

- enforce SRUC-compliant password parameters (length, complexity, etc)
- enforce password expiration rules
- apply password re-use rules
- configure the maximum number of failed password attempts
- enforce password rules remotely (by the Information & Digital Services Group’s system administrators)

SRUC remote management utilities may be used to enforce:

- password rules on the device
- inactivity time rules for lock-down of the device
- an automatic “local wipe” of the device.

4.2 Protection of data on the device

In order to protect data on the device is, the device must:

- allow hardware-based encryption for data stored on the device
- ensure that hardware-based encryption is always enabled and cannot be disabled by users
- allow deactivation and erasure if the device is deemed to be lost or stolen

SRUC remote management utilities may be used to:

- enforce “remote wipe” of the device, including data stored upon it, if the device is lost or stolen (or is suspected to be lost or stolen)

4.3 Protection of data in transmission

Key policy criteria for the protection of data in transmission to the device:

- device settings must accord with SRUC’s general security policies as they affect data transfer
- device must be proven to work with SRUC’s VPN and other network technologies

5 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.

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 not obscene or defamatory or inappropriate in other ways. Personal e-mail use should not interfere with the performance of the employee's/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 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 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.

SRUC e-mails should not be forwarded to personal email accounts (see section 3 above regarding the use non-approved cloud services for storage of SRUC data)

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.

5.1 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).

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 a senior Human Resources manager (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 staff intranet.

While SRUC reserves the right to access an employee's SRUC e-mail account, individual staff may not access another user's SRUC e-mail account without prior written permission from the owner of the e-mail 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 e-mail account must clarify this arrangement by completing the 'Request to Access User's Account Form' – as mentioned already.

Once the form has been completed it should be sent to the Information & Digital Services Group for filing and future reference.

5.2 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 unsolicited or untrusted sources.

5.3 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.

6 Data Protection

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

This prescribes a number of further rights and responsibilities regarding data protection.

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 any digital format, including email and file storage. 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 or other files 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 or transferring files containing personal information to countries outside the European Union, especially if those countries do not have equivalent levels of protection for personal data;

7 Removable media

This policy applies to both supplied portable and removable devices and personal items used for our business.

Portable devices and removable mediums include:

- CD, DVD, floppy disk, tape, zip disk, etc.
- External hard disk
- USB memory stick
- Solid-state or other storage card (e.g. CompactFlash, SD, other new digital storage, etc.)
- Any portable device that can download data from another device directly, such as a phone, tablet, wearable device, etc

No personal, sensitive or confidential information shall be stored on any non-SRUC supplied removable media devices except when specific permission is given by Information & Digital Services.

- The storage medium must be **encrypted** to at least the required organisation specification.
- When using removable media from device to device, the media must be **scanned for viruses** and malware prior to use
- Due to the high risk of loss or data corruption, removable media must **not contain the only copy of important data**. Backups of the data must be maintained or the data on removable media must be a backup of source data properly stored on resilient data systems.
- Unencrypted portable media is used only in a single location, not transported and are kept securely locked away at all times when not in use. (Note that such activity carries some inherent risk of loss or breach of confidentiality of the data so anyone working in this way must be made aware of the dangers.)
- It is important that you **report any lost devices** or compromises to personal data as soon as possible to the Head of Information & Digital Services (IDS) . The Data Protection Act specifies that any data breaches must be reported to the Information Commissioners Office (ICO) within a very short timeframe once discovered or reported, so the IDS staff and the Data Protection Offcer need to be informed as quickly as possible.
- Any portable device or removeable media that you find **where the owner is unknown or untrusted** must not be attached or plugged into to a SRUC or personal device due to the high risk of malware on the device or media. Report the found device to the Head of Information & Digital Services (IDS). Removable media to be **disposed of must be securely wiped** of data in order to prevent the reading of any remnant data left on the media or device

8 Personal 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 transactions. 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 the Group Manager of Information & Digital Services (or nominee), 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 & Digital Services (or nominee) for each download
- make occasional and reasonable use of personal e-mail (e.g. G-mail) and social networking websites (e.g. Facebook, Twitter) during breaks, outside of working hours, etc.
- not access undesirable information. Undesirable materials include, but are not restricted to pornographic, violent, sexist and racist material, and gambling sites

IDS reserves the right to block sites which appear on national information security databases as malicious or otherwise inappropriate for business use.

“Reasonable use” includes occasional use during designated breaks or outside normal working hours of the Internet for personal research, shopping, accessing personal e-mail 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; online 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.

9 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
- 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.

9.1 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 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.
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.

10 Password protection

It is essential that all users (employees/consultants/contractors/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

Staff 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. Staff must not give their password to their line manager or any other senior member of staff even if they are requested to do so.

Password Guidance may be found in Appendix B.

11 Clean Screen and Clean Desk Policy

At the end of each day, or when desks/offices are unoccupied, any SRUC classified information must be locked away in either filing cabinets, secure cupboards/drawers or offices, which have been provided to all staff, as appropriate.

Any 'confidential' or 'management-in-confidence' classified SRUC information or data must by securely disposed of using one of the shredders provided by SRUC. Under no circumstances should this type of waste paper be thrown away with normal rubbish in the bins under each desk.

11.1 Clean screen procedures

Whenever you leave your PC, laptop, or mobile device that has access to SRUC data, it is essential that the device is either:

a) shut down, or
b) logged out, or
c) the screen is locked (by using 'Win+L' or ⊞+L)

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 activity and transactions entered through their User ID whether or not they were present at the time.

If visitors or other non-authorised persons are 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.

12 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) 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.

13 Use of SRUC Telephones

There will be occasions when users need to make short, personal telephone calls in order to deal with occasional urgent personal problems. Other non-urgent personal calls should be made using non-SRUC telephones. 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. Equally, it is legitimate to receive personal calls and occasional, short, non-urgent calls can be received as long as they do not interfere with work requirements.

It is unlikely that personal calls about domestic problems and arrangements would arise at weekends, or during periods of leave, and SRUC telephones should not be used for personal calls in those circumstances.

Premium-rate telephone services not directly connected with SRUC-related work are not permitted. If such services are used the employee/student must 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 recording 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.

14 Monitoring of the use of telephones, 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) records of telephone call details from particular extensions for recharging purposes

b) normal network and digital systems monitoring

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 duly authorised nominee), may grant permission for the monitoring of an employee's/student's telephone calls and use of e-mail or the Internet. Managers who suspect misuse should in the first instance advise, in confidence, a Human Resources Manager.

14.1 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.

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.

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.

15 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.

15.1 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**

16 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.

16.1 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.

17 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*.

18 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).

19 APPENDIX C – Relevant Legislations

The following sections provide high level summaries of various points that might be relevant to users and system administrators as it pertains to the creation, processing, storage, and transmitting of information.

The Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:
1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

Data Protection Act 2018

Provides a safeguard for personal privacy in relation to computerised or other systematically filed information; it regulates the use of *personal data* meaning information about living human beings. It is an offence to process personal data except where they are:
1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to countries outside the EEA without adequate safeguards

General Data Protection Regulation

The GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act, and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover.

Freedom of Information (Scotland) Act 2002

The Freedom of Information (Scotland) Act 2002 is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act 1996

"Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm."

Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008

The Protection of Children Act 1978 *prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs.* Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.

The definition of 'photographs' include data stored on a computer disc or by other electronic means which is capable of conversion into an image.

It is an offence for a person to […] distribute or show such indecent photographs; or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment. Note: The term "make" includes downloading images from the Internet and storing or printing them out.

End of Document