Acceptable Use Policy

Last Revised: 15 January 2024

Document Control

Title	Acceptable Use Policy
Abstract	To ensure users are bound to protect the organisation's information, business applications and systems, and the organisation's security obligations are met.
Version	1.4
Date Issued	7 December 2021
Status	Issued
Document owner	Information Services
Creator name	James Blair
Creator organisation name	The University of Stirling
Subject category	Information security
Access constraints	Public

Document Revision History

Version	Date	Author	Summary of changes
0.1	28 Aug 2019	James Blair	Initial draft
0.2	30 Aug 2019	David Telford	Substantial update with general AUP, ref to unacceptable content and use
0.3	12 Sep 2019	James Blair	Minor updates
0.4	12 Sep 2019	Gerry Mason	Minor updates
1.0	1 Nov 2019	David Telford	Governance updates
1.1	6 Dec 2019	Helen Beardsley	Minor updates
1.2	6 Dec 2019	Gerry Mason	Minor updates
1.3	2 Sep 2020	Victoria Szymanska	Review and minor updates
1.4	7 Dec 2021	Victoria Szymanska	Review and minor updates; updated link to data breach reporting form and removed it from appendices. Document issued
1.5	15 Jan 2024	Lesley Gibson	Minor Changes

Table of Contents

1 Background, Purpose and Scope

1.1 Background

The objective of information security is to achieve and maintain a condition where all information is always available to all those who need it, where it cannot be corrupted or disclosed to unauthorised persons and its origin is authenticated. This involves the preservation of:

- **Confidentiality** - ensuring that information is only accessible to authorised persons;
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods;
- **Availability** - ensuring that authorised users have access to information and associated assets when required;
- **Non-repudiation** – the reasonable assurance that, where appropriate, a user cannot deny being the originator of a message after sending it.

1.2 Purpose

The purpose of this document is to specify and communicate guidance and requirements for acceptable use of the University of Stirling systems. It is independent of any hardware and software environment and should be used as a generic baseline for the implementation of security for any system or application.

1.3 Scope

This document contains user responsibilities and guidance for the following subject areas:

- Protection Against Malware;
- Internet Use;
- E-Mail Use;
- User Access Control;
- Information Classification and Handling;
- Communication Security;
- Use of Encryption;
- Data Backup;
- Computer Equipment;
- Reporting of Security Incidents;
- BYOD /Mobile.

2 Statement of Policy

It is the policy of the University of Stirling to ensure that information assets are protected from all threats, whether internal or external, deliberate or accidental. Specifically, the following measures will be put in place:

- Detection and prevention controls to protect against malicious software (malware) and appropriate user awareness procedures will be implemented;
- Use of e-mail and access to the Internet and the World Wide Web (WWW) will be controlled and monitored;
- All access to University of Stirling systems and data will be in accordance with the minimum privilege principle, in that access is denied except where it is specifically required for functional purposes;
- All users will be authenticated and accountable for their actions on the University of Stirling systems;
- Only equipment approved by the University of Stirling is to be used. The installation or connection to the University of Stirling network of unauthorised devices is forbidden;
- Sensitive information will not be transmitted over insecure connections. Where confidentiality is a critical issue, cryptographic measures will be applied to protect the data where appropriate;
- All IT equipment, especially portable computers, will be adequately secured to prevent theft;
- All security incidents will be reported and resolved through appropriate management channels as soon as possible after the incident is discovered;
- All personnel have a responsibility to adhere to the policy and standards regardless of their status;
- All regulatory and legislative requirements will be met;
- All personnel with access to the University of Stirling IT systems will receive appropriate education and regular updates in organisational IT Security Policy, standards and procedures.

3 Security Requirements

3.1 Use of Systems and Information

The University of Stirling's information technology is provided to support educational and business functions of the University, including access for personal development to improve individual knowledge, skills and career enhancement. The only other usage allowed is as defined in section 6 under 'personal private use of information technology'.

Information must NOT be offensive, abusive, discriminatory, illegal to possess, damage the University's interests, or contravene University regulations. Examples of offensive information include all forms of pornography and violent images. Pornography as defined here includes:

1. Indecent images of children under 18 which it is illegal to possess.
2. Obscene materials which it may be an offence to publish but not to possess. Materials comparable to that available on the "top shelf" in a newsagent which is neither an offence to publish nor possess but which some may find distasteful;
3. This section applies equally to all storage, processing or transmission of information, including viewing of web pages, data files and the content of emails;
4. It is acknowledged that there can be valid academic reasons to access information that would normally not be allowed under this policy. In this situation staff and students must gain written approval from their Dean of Faculty or Service Director for these specific activities. Information that it is illegal to possess is never allowed;
5. The University recognises that users may accidentally connect to unacceptable web sites or receive unsolicited unacceptable emails. Audit logs will demonstrate that such visits are rare and short, and hence unintentional. In these cases, no action will be taken against the user. Users must only attempt to access information technology services which are either clearly publicly available, for example public web sites, or ones to which they have been personally granted specific rights by the administrator of that service.

If a user is not sure whether they have rights to access a service, they must contact either the Information Centre information.centre@stir.ac.uk ext. 7250, or the University Research Ethics Committee where the access is required for research, before attempting access.

No forms of 'network probing or sniffing' are permitted unless specifically approved in writing by the Director of Information Services, as advised by the University Information Security Manager, who can be contacted via the Information Centre. **A breach of this part of the policy is interpreted as a criminal offence as it is illegal use of hardware, software or information.**

The University has a statutory duty 'to have due regard to the need to prevent people from being drawn into terrorism'. The use of IT facilities to support terrorist activity is not permitted and may result in a criminal charge. Access to material promoting terrorism is not permitted, unless this access has been specifically allowed by the University Research Ethics Committee as part of an approved programme of research.

3.2 Personal Use of University Information Technology

The University of Stirling allows personal/private use of its information technology by staff and students subject to the following conditions:

1. It must not inconvenience or distract any educational or business function;
2. It must not in any way interfere with their individual work as a member of staff or a student of the University;
3. It must not in any way impede the work of other users;
4. It must not place a heavy load on the systems. (Examples of types of use that are allowed but must not impact others, your work or the work of the University include the legal transfer of music and video files, the playing of games over the network, or similar network intensive activities.);
5. Any personal financial transactions conducted using University IT facilities are done at the individual's own risk;
6. Private use specifically excludes private commercial activity, betting and gambling.

Personal/private use may be withdrawn on an individual or group basis if it is abused or interferes with the efficient operation of the University. Further, it may lead to disciplinary action where activities impact the individual's work or the work of others and the University.

3.3 Password

This section defines the regulations for the use of passwords that are critical as they are the 'keys' to all information technology security:

1. All workstations must be protected with a password. (This function is carried out by Information Services for workstations on the University network);
2. Authorised users are responsible for the security of their passwords and user accounts. Passwords must be kept secure and never shared with anyone else;
3. Passwords must be at least 12 characters long and include alpha, numeric and at least one other character. Their structure must make them hard to guess. Guidance on creating passwords is available on the University Intranet;
4. Passwords should never be displayed on screens;
5. If at any time a user believes their password has been compromised, they must immediately change it or request that it is changed;
6. Should a user request a password change on their behalf, proof of identity will be required as for account/password creation;
7. Passwords should never be "remembered" on the computer but entered by the user on all occasions.

3.4 General Acceptable Use

This section defines general regulations that govern the use of information technology within the University of Stirling:

1. Always log off or lock a workstation before leaving it. This is to ensure that no one else can access the user's information or can use the workstation without identifying themselves, e.g. to send an abusive email in the user's name;
2. When confidential work is being carried out ensure no one else can read the screen;
3. Protect equipment from physical theft. This is vitally important for portable equipment;
4. Ensure that all important data is backed up regularly and copies are kept in a separate secure location. Liaise with the Information Centre if you require assistance. (This function is carried out by Information Services for information stored on the University network);
5. Respect the legal protections for information and software provided under copyright and licenses. Never copy electronic information or computer programs unless specifically authorised in writing. Never run or install software without a valid license;
6. Licensed electronic reference information and computer software must not be used for 'non-core' University purposes without the specific written authority of the Dean of Faculty or Service Director holding the license on behalf of the University. For this purpose, such 'non-core' activities include consultancy, student projects that benefit other organisations (including their employers), and presenting short courses;
7. Do not move information from the University premises unless it is necessary. All personal and business critical information moved using data storage devices should be protected using approved encryption software;
8. All PCs should be patched with the latest security critical patches and up to date patches;
9. All data storage devices including laptops, USB sticks, CDs, DVDs that are brought in to the University must be checked for viruses on every occasion before use;
10. All workstations connected to the University of Stirling network, whether owned by the University of Stirling or not, shall be continually executing approved virus-scanning software with a current virus database;
11. Never introduce malicious programs into the University of Stirling network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) by any means.

N.B. Regulations 8–11 are carried out on all university workstations running the standard Information Services images.

Physical devices include laptops, tablets mobile phones, USB sticks, CDs, DVDs etc. and all other mobile devices.

Inform the Information Centre immediately if you think that any workstation may have a virus or is behaving abnormally. Contact: information.centre@stir.ac.uk ext. 7250.

3.5 Protection Against Malware

Malware (computer viruses, spyware and other forms of malicious code) exploit vulnerabilities in software programs and can cause loss and damage to information, software and IT equipment.

The University of Stirling uses a variety of products e.g. anti-virus, and software security patches, which are constantly updated to minimise the threat from viruses and other malicious code. The University of Stirling PCs and laptops are also protected by these controls. You must not change or remove these controls on your PC or laptop, otherwise the IT network and systems will become more vulnerable to the threat from viruses and other malicious code.

You must ensure that:

- You do not introduce a virus or malicious code into the corporate network by downloading unauthorised or suspect software from the internet or from computer media e.g. DVDs, CDs and USB storage devices onto your PC, laptop or any University of Stirling system;
- All software and data which originates from outside the University of Stirling must be checked for viruses and malicious software prior to it being opened or used – if you need help, contact the Information Centre information.centre@stir.ac.uk ext. 7250;
- If you are suspicious of a virus or malicious code, you must stop using your PC or laptop immediately and contact the Information Centre information.centre@stir.ac.uk ext. 7250;
- If you receive a suspicious e-mail, you should not open it or the attachment, as this may well activate a virus or other form of malicious code. Again, immediately contact Information Centre information.centre@stir.ac.uk ext. 7250.

More information can be found in the Anti-Malware Policy.

3.6 Internet Use

The internet presents users with opportunities for easy, rapid and efficient access to a wealth of useful information, but also creates certain risks, including security risks and legal liability risks.

This policy applies when using any equipment in any location on any University of Stirling network.

You should note that the University of Stirling network and systems may be subject to monitoring and inappropriate use may result in further action, including disciplinary action up to and including dismissal.

3.6.1 Acceptable Use

Accessing the internet for the legitimate business purposes is regarded as acceptable use.

In addition, you may occasionally access the internet for personal use, such as personal email, travel etc. You must use your proper judgement as to what constitutes occasional access, however it must be based on minimal access to the websites and services necessary for daily life that in no way interfere with fulfilling your role within the University of Stirling (either in terms of the services accessed or the time spent using them).

3.6.2 Unacceptable Use

The following are deemed as unacceptable use, regardless of whether it is for business or personal reasons:

- Any activity that may adversely impact or damage the reputation of the University of Stirling;
- Unauthorised downloads of material which infringes any copyright, trademark, patent, trade secret or other proprietary rights of a third-party. This includes unauthorised copying of copyright material, digitisation and distribution of copyright photographs, software;
- Unauthorised downloading of any unlicensed or 'hacked' illegal software;
- Using peer-to-peer software or services;
- Knowingly accessing or sending:
    - Material likely to facilitate an illegal act;
    - Information about, or software designed for, breaching security controls or creating computer viruses;
    - Material that is obscene, sexually explicit, defamatory, incites or depicts violence, or describes techniques for criminal or terrorist acts;
    - Material that is illegal under local or international law.
- Excessive personal use of the internet, social media etc.;
- Compromising security controls of the University of Stirling or any other organisation;
- Disabling or intentionally overloading any computer system or network;
- Knowingly circumventing any system that protects privacy or security;
- Accessing information or traffic not intended for you;
- Any activities that intentionally adversely affect the ability of others to use University of Stirling services;
- Deliberately propagating any viruses, malware or other software intended to cause disruption;
- Making any statement on your own behalf or on behalf of the University of Stirling that may cause offence, libel or damage the reputation of others.

If in doubt about whether or not an activity is considered unacceptable then do not do it. If you require advice then please contact the Information Centre information.centre@stir.ac.uk ext. 7250.

3.7 E-Mail Use

3.7.1 General

E-mail presents opportunities for easy, rapid and efficient global communications but it introduces security threats such as malicious code attacks, e.g. viruses, unsolicited or undesirable e-mail, fraudulent attempts to acquire sensitive information such as passwords, unauthorised content, and breaches of legislation, e.g. computer misuse and copyright legislation. E-mail is provided as a means of improving communications, knowledge and effectiveness at work.

This policy applies when using:

- The University of Stirling e-mail on any network;
- Any University of Stirling equipment or technology that has an e-mail capability, including desktops, laptops, smartphones.

All usage of University of Stirling e-mail facilities must be regarded as the property of the University of Stirling and must not be regarded as private. You should note that the University of Stirling network and systems may be subject to monitoring and inappropriate use may result in further action, including disciplinary action up to and including dismissal.

3.7.2 Usage and Guidelines

You must:

- Obey the law and comply with relevant legislation. You are responsible for observing copyright, intellectual property rights and licensing agreements that may apply to information, documents and software;
- Take care to ensure that intended e-mail recipients are carefully selected before sending e-mails;
- If an e-mail is received in error, then you must inform the originator that the error has occurred as soon as possible;
- Avoid sending unnecessary messages, especially with large attachments. Consider referring to shared directories on fileservers or cloud-based document sharing that are approved by the University rather than sending attachments (files or documents) in e-mails. This will enable efficient use of e-mail in terms of reducing requirements for e-mail file storage, and efficient use of network bandwidth to transmit e-mails;
- Practice good e-mail account management such as deleting e-mails that do not need to be retained;
- Take care if e-mails are received from unknown and unexpected sources. Do not open suspicious e-mails and their attachments or web links, as these may contain malicious software. It is good practice to save attachments to the local desktop (or other relevant computer folders) before opening them, so that they can be automatically checked for malicious software content. If in doubt, either permanently delete suspect e-mails (delete them from the ‘deleted items’ folder too) or contact your Line Manager;

- Seek legal advice before entering into any e-mail communication that could later be interpreted as contractual. Care should be taken to ensure that the content of e-mails remains objective (not subjective) as far as possible, and that personal comments that could lead to dispute and legal issues are not included;
- Carefully check e-mails before sending them, and only distribute e-mails to users who need to know.

You must not:

- Use e-mail for personal financial gain or political purposes. Personal advertising is strictly forbidden;
- Configure your e-mail for automatic forwarding unless there is a justified business requirement, authorised by the relevant Line Manager;
- Use e-mail to store or transmit:
    - Pornographic, obscene, offensive, racist, defamatory, harassing or intimidating material;
    - Unsolicited messages (known as spam), hoax and nuisance e-mails. If such e-mails are received, never open, reply to or forward them to other users. Replying to them is likely to lead to the receipt of further such e-mails. Contact your Line Manager if in doubt;
    - Information which is sensitive or confidential. If there is a business case for using e-mail to transmit and store sensitive information, then advice on suitable protective measures (e.g. use of strong cryptography) should be sought from Information Security Management;
- Access or transmit malicious software, e.g. viruses and spyware. (Spyware is software that is installed and used in an unauthorised way to capture information, including keystrokes, bank details, credit card details and passwords);
- Attempt to disable or circumvent malicious software controls installed by the University of Stirling;
- Circulate information received about computer viruses. In many cases, these e-mails are hoaxes. If in any doubt about a received e-mail, contact your Line Manager for advice, otherwise delete the e-mail immediately;
- The identity of an e-mail's sender can be faked (known as spoofing), and the content of an e-mail can be changed in an unauthorised way between the e-mail being sent and received. Use of faked e-mails that request confidential information such as bank account details is known as 'phishing'. If an apparently legitimate e-mail is received that requests sensitive information, verbal confirmation of the request shall be sought (and internally approved by the relevant Line Manager) before fulfilling the request;
- Attempt to 'spoof' e-mails, transmit anonymous e-mails, or change the origin or content of e-mails that have been sent or received;
- Use e-mail to store and transmit any illegal or unauthorised software, including games, music and screensavers;
- Use e-mail for entering into electronic contractual agreements. If there is a business case for use of e-mail in this way (and the use of electronic signatures), then advice should be sought from the relevant Line Manager.

3.8 Use of Social Media

All use of commercially available web-based e-mail and social networking communication applications must be compliant with local applicable laws and legislation. In addition:

- Commercially available e-mail applications, including but not limited to Gmail, Yahoo!, Outlook and AOL, must only be used for personal communication. The University of Stirling information classified as Internal, Restricted or Confidential must never be communicated over this medium;
- Commercially available social networking applications, including but not limited to Twitter, Facebook and Snapchat, must only be used for personal communication in line with Human Resource's Social Media policy, unless required as part of a job duty. The University of Stirling information classified as Restricted or Confidential must never be communicated over this medium;
- Instant messaging interactions involving University of Stirling information must only be transmitted using applications which are formally approved and managed by the University of Stirling IS team;
- Instant messaging communications which transmit University of Stirling information must be secured, including but not limited to encrypting communications and managing file transfers in compliance with the University of Stirling Encryption procedure;
- Commercially available (non- University of Stirling managed) and web-based instant messaging applications, including but not limited to Messenger, WhatsApp, Weechat, Skype, Instagram and SnapChat, must only be used for personal communications and/or for communicating the University of Stirling information classified as Public.

3.9 User Access Control

3.9.1 General

- Each device connected to the University of Stirling network is a potential gateway into the system and consequently every user has a personal responsibility to ensure that they control access to their PC/laptop by diligently complying with the access control procedures.
- You must only access and use the University of Stirling network, systems and applications if you are authorised to do so. If you are granted access, it is so that you are able to perform your duties efficiently.
- User Access to the systems is controlled using UserIDs and passwords. Unless specially otherwise authorised, all UserIDs and passwords are unique to each individual and consequently you will be accountable for all actions on systems that are linked to your logon ID.
- You are personally responsible for controlling access to your PC and therefore it is important that you strictly adhere to the measures stated below.

3.9.2 User Responsibilities

- **Do not** leave your PC unattended when logged on. Normally the system or application will force a lockout after a pre-determined period, and you will be required to re-enter your password and UserID to regain access. The lockout can also be facilitated manually by pressing Ctrl-Alt-Delete and locking the PC manually. Where this is impractical to implement, for example, in areas where work teams share access to a single workstation, dispensation will be applied. In such situations the appropriate line manager will own the risk and be responsible for the security of the workstation.
- **Do not** allow anyone else to use your UserID and password.
- **Do not** use someone else's User ID and password to access the network unless specifically authorised to do so. In some cases, "unauthorised access" can be regarded as a criminal offence.
- **Do not** leave sensitive information displayed on an unattended PC screen. If you are moving away from your immediate work area you must initiate the lockout yourself.
- **Do not** disable, interrupt or change the configuration settings of any security control (e.g. antivirus) installed on any managed University of Stirling resource, or a personally owned device that has had University of Stirling security controls installed for the purposes of accessing University of Stirling information.

3.9.3 Passwords

In many cases the system will enforce password length and quality. If this is not the case **you must**:

- Change temporary passwords on first use;
- Use a mixture of numbers, uppercase, lowercase and punctuation so that it includes characters from three of the following four categories:
    - uppercase characters (A - Z);
    - lowercase characters (A - Z);
    - Base 10 digits (0 - 9);
    - Non-alphabetic characters (for example !, $, #, %).
- Use at least 12 characters in length;
- Make it (or the key sequence) easy to remember so you don't need to write it down, but make it as long as possible;
- Make it easy to type quickly so it is difficult for an observer to see.

You must not:

- Immediately re-use the same password when you change it.
- Use a recognisable word from a dictionary and in particular:
    - The name of your spouse, parent, colleague, friend, towns, months or days;

  - The number of car/motorbike registration or telephone;
  - Common dictionary words;
  - Series of identical numbers/letters;
  - Obvious keyboard sequences;
  - Use your account name or parts of your name that exceed two consecutive characters.
- Base the password on any of the following criteria:
  - Months of the year or days of the week;
  - Date of birth;
  - Family name, initials, car registration numbers or any other relevant personal information;
  - Company names or identifiers;
  - Telephone numbers or any other all-numeric value;
  - More than two consecutive identical characters.
- Write it down or disclose via email;
- Use default passwords;
- Share your password with others.

If you suspect that your password has been compromised, that password must be changed immediately. Immediately after changing the password that is suspected of being compromised, you must report the suspected compromise to the Information Centre information.centre@stir.ac.uk ext. 7250.

More information can be found in the Access Control Policy.

3.10 Ownership of Information

You should be aware that:

- All University of Stirling information is ultimately the property of the University of Stirling;
- The University of Stirling may monitor, inspect, search and/or record any activities occurring on the University of Stirling resources without limitation. This includes electronic communications, without notice of any kind;
- Users of the University of Stirling resources have no expectation of privacy.

3.11 Data Classification and Handling

3.11.1 General

All information that is handled by the University of Stirling has a classification to determine the level of security it requires and the way in which it must be handled.

The University of Stirling Data Classification and Handling Policy (www.stir.ac.uk/GDPR) specify labelling and handling procedures. These procedures apply to all information irrespective of its form, including electronic information, e.g. databases and files, computer media-based information, e.g. stored on flash drives, CDs and DVDs, and paper-based documents, e.g. contracts, facsimiles and printed reports.

For every document you produce, you are personally responsible for defining its classification on behalf of your department. When you are classifying information, you must consider its sensitivity and how much protection it needs.

When using University of Stirling information, you must handle it in a secure manner based upon its classification.

More information can be obtained from Data Classification and Handling Policy (www.stir.ac.uk/GDPR).

3.11.2 Data Control

- The University of Stirling information classified as Confidential may only be transmitted electronically if approved by the information owner and when it is secured appropriately according to all applicable policies and standards based on its level of classification.
- Users may not copy University of Stirling information classified as Confidential to personal storage devices (e.g. any device not owned or managed by the University of Stirling), including but not limited to USB, external drives, smartphones and tablets.
- Users may not synchronise or share University of Stirling Confidential information using internet enabled commercial services with file sharing capabilities (e.g. DropBox,). Only services which are managed and operated by the University of Stirling may be used for this purpose.

3.11.3 Clear Desk Policy

You must ensure that information classified as Restricted or Confidential (either computer media or documentation) are not left unattended and insecure, but are appropriately stored in locked areas or facilities, e.g. locked cabinets, and that access to relevant keys is controlled.

At the end of a working day, you must:

- Logoff your PC or laptop;
- Clear your desk and lock all Restricted or Confidential computer media and documents away in a drawer or cabinet with suitably restricted access.

3.12 Protection of Personal Information

The Data Protection Act 2018(DPA 2018) protects individuals from misuse of their personal data. The Act covers data held in both electronic and paper form. Our information systems are designed to protect personal data. Compliance with the University of Stirling Information Security policies, standards and procedures will ensure that the security of staff, student and customer data is not compromised as a result of intentional or unintentional systems misuse.

3.12.1 Call Notes and Other Records

Notes entered in Customer Relationship Management systems (CRMs), transaction systems or recorded in documents and emails are subject to the Data Protection Act, and any individual whose information is recorded is entitled to see these records or other details we hold about them. Therefore:

- Call notes, documents and emails could be disclosed in litigation. Untrue statements made about a colleague, student, customer, supplier or a third party, even those intended as a joke, can be viewed as harassment, libel or slander and could result in you, the University or both being sued;
- You must not use any terms that are defamatory; what may be intended as a joke or light-hearted comment could cause offence to others;
- The information contained within CRMs, staff or student records systems is highly confidential. You must not disclose any information obtained from these systems to any third party;
- You must not use any information obtained from these systems for any purpose other than your legitimate work for the University;
- You must not copy any of the information in these systems for any purpose other than your legitimate work for the University and if you do possess any such copy you must not remove it from the University premises.

3.12.2 Payment Cards - PCI Data Security Standards (PCI DSS)

PCI Data Security Standards (PCI DSS) require the University of Stirling to take proper care of customer information when:

- Selling products and services;
- Processing refunds;
- Resolving payment problems;
- Implementing fraud prevention measures.

The University of Stirling Information Security policies, standards and procedures are designed to meet the requirements of PCI DSS and therefore your adherence to those standards is essential to ensure the University of Stirling complies. Failure to do so would not only result in the withdrawal of payment card facilities but also damage the University of Stirling brand.

3.13 Communication Security

Due care must be taken when using telephones, voicemail, answering machines, facsimiles and recording equipment (e.g. photographic, video and audio equipment) to ensure the protection of sensitive information.

It is important that before you conduct a telephone conversation in an open plan office area or outside of the University of Stirling premises, you must consider the nature of the topic you are about to discuss. If the conversation is of a sensitive nature, you must ensure that there is

no possibility of eavesdropping. Remember to always be aware of who is around you when holding a confidential conversation. In addition, messages containing sensitive information must not be left on voicemail and answering machines.

When sending or receiving sensitive information by facsimile, you must ensure that the information is not compromised. Always check the recipient facsimile number to ensure that it is correct before sending information. Ensure that the information is collected immediately from the facsimile. Ensure that all sensitive information sent by facsimile is destroyed when no longer needed, by shredding using confidential waste containers.

3.14 Use of Encryption

If there is a business case for using e-mail to transmit and store sensitive information, then advice on suitable protective measures (e.g. use of strong cryptography) should be sought from Information Security Board Information Centre information.centre@stir.ac.uk ext. 7250.

The use of encryption methods not provided or approved by the University of Stirling is forbidden.

More information can be found in the Encryption procedure.

3.15 Data Backup

Back-up and recovery procedures and technology are implemented for centrally held data in order to protect the University of Stirling from losses or corruption of information and software, e.g. due to unauthorised changes to information and software, technical failures, viruses and fire.

All staff are responsible for ensuring that any data that they create, or change is backed up on a regular basis. This is achieved by ensuring that data is stored on central systems which IS backs up on a regular basis (i.e. not on a local laptop / desktop).

Therefore, you should ensure that:

- You minimise storage of data on your individual device;
- You save data or regularly back up data to the centrally controlled systems;

3.16 Computer Equipment

3.16.1 User Responsibilities

- You must always take care of IT equipment allocated for your use and treat it as if it is your own.
- All of the IT equipment and software that you have been assigned remains the property of the University of Stirling. All users have an obligation to ensure that this equipment and software is safeguarded and only used as intended by the University of Stirling.

- Unless specifically authorised and approved, direct connection of non-University of Stirling equipment to the wired network or WLAN is forbidden. Requirements for connectivity of Third-Party devices are contained in the Third-Party Access Policy.
- In addition, you must not use personally owned information processing facilities (e.g. iPads, Smartphones etc.) to process the University of Stirling information without formal authorisation or use of authorised and secured products.
- Other than your laptop, you must not remove any IT equipment from the University of Stirling premises without the authorisation of Information Services and relevant information system owners or line managers.
- You must not expose your IT equipment to any environmental hazard, such as extremes of temperature.
- You must not install any software on your IT equipment. If you require any software for your work, you must consult your line manager and Information Services.
- You must not modify your IT equipment in any way; this includes any amendments to the hardware and software configuration.
- You must protect your IT equipment against loss, theft and unauthorised access:
    - Always ensure that computer equipment is always physically secure, including when it is in offices and travelling;
    - Keep it securely in the office whenever you do not need it elsewhere;
    - Avoid having it visible in a vehicle or leaving it unattended in a vehicle;
    - Where issued or available always use a Kensington lock to make it physically secure;
    - Do not leave it unattended, for example, when travelling or in a restaurant;
    - Consider if other security measures are appropriate for where it is located.
- Do not keep your computer PIN, username or password with the equipment.
- Avoid keeping important files only on the computer in order to prevent them from being completely lost if a computer fails or is stolen.
- Immediately report any lost or stolen equipment to the Information Centre information.centre@stir.ac.uk ext. 7250.

3.16.2 Secure Disposal and Re-use of Equipment

All University of Stirling information and software must be securely wiped from IT equipment before disposal or re-use of the equipment. All equipment intended for disposal and re-use must be returned to Information Services, who will, where appropriate, securely wipe information and software from the equipment.

3.17 Reporting of Security Incidents and Personal Data Breaches

3.17.1 General

For the University of Stirling to be able to manage and deal with security incidents successfully, they must be captured and logged. There is a difference between an information security incident and a personal data breach. Whilst all personal data breaches are information security incidents, not all information security incidents are necessarily personal data breaches. In this Policy the term security incident includes personal data breaches. In the case of a personal data breach there may be a requirement to report the incident to the Information Commissioner's Office within 72 hours.

If you suspect or have knowledge of a security incident, a breach of information security policy and standards, a software malfunction, a security weakness in any information system, or a personal data breach you must report the concern immediately via the Information Centre information.centre@stir.ac.uk ext. 7250.

Examples of a security incident or breach include:

- Loss of equipment or sensitive data;
- Physical damage to IT equipment;
- Compromise of sensitive documents and information;
- Unauthorised use of another user's profile (masquerading of user identity);
- Divulging a password to another person without authority;
- Improper use of e-mail or the internet, e.g. harassing e-mails, downloading or distribution of pornographic images;
- Unauthorised copying of information;
- Damage to property that could impact information security;
- Access to premises without authority;
- Theft of IT equipment.

Any security incident that leads to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data is also referred to as a personal data breach.

It is vital that you report all security incidents immediately. Personal data breaches which do not involve IT (e.g. loss or theft of paperwork, information posted to the wrong address, etc.) should also be reported to the Information Centre who will pass it on to the Data Protection Unit as appropriate. Withholding information and failing to report an incident could result in you being held personally liable.

Other than taking simple recovery steps, such as recalling an email sent to the wrong recipient, you should not attempt to deal with the security incident (other than reporting the incident). You should not take any action that could interfere with integrity of log files and preservation of evidence otherwise you could potentially become involved in disciplinary or legal action.

If in doubt, contact your Line Manager for advice.

3.17.2 Reporting Actual/Suspected Security Breaches

All security incidents, personal data breaches or suspected incidents must be immediately reported via the Information Centre information.centre@stir.ac.uk ext. 7250. The Information Centre will be responsible for informing Information Security Management, the Data Protection Unit or other areas as relevant.

If it is appropriate to do so, also report the security incident to your own Line Manager.

When reporting an incident, the reporter should provide details of:

- The exact nature of the security incident or personal data breach;
- An indication of the seriousness of the incident/breach (e.g. the sensitivity of the personal data involved, the number of individuals whose data may be involved, who may have access to the data);
- If possible, what action needs to be taken immediately to mitigate the breach.

In all cases, Information Security Management is ultimately responsible for ensuring that the Security Incident/ Personal Data Breach Report Form in Unidesk is completed with the help of the person reporting the incident, and where relevant, Information Security Management may seek input from other staff, e.g. Human Resources or an appropriate line manager.

The details of information security incidents can be very sensitive, e.g. details of offenders and the offence committed. The following aspects should be noted:

- All persons involved in the reporting and documenting of information security incidents must ensure that sensitive information is disclosed to only those people who need to know the details;
- All sensitive information must be handled with discretion;
- Related conversations must not be overheard, and related documentation must not be disclosed to those who do not need to know.

3.17.3 Involvement with Security Incidents

Members of staff must not attempt to deal with the security incident (other than reporting the incident), otherwise they may become involved in disciplinary or legal action. The integrity of log files and preservation of evidence is vital.

If inappropriate data content is discovered, e.g. obscene images, the following must be observed, otherwise disciplinary or legal action may be taken:

- Close the file, and do not copy it or show it to others;
- Password lock relevant computing equipment immediately - by simultaneously pressing the <Ctrl> <Alt> <Delete> keys and selecting ‘Lock Computer’;

- Place any physical copies in a suitable envelope to ensure no one else can see them;
- Immediately contact Information Security Management, Human Resources and your Line Manager in person or by telephone.

3.17.4 Evaluation and Response

Once a security incident or personal data breach is contained, depending on the type of incident, a review may be conducted into the cause of the incident and the effectiveness of the response. Any staff involved in the incident may be asked to feed into the review process or implement changes of practice because of the breach. If ongoing problems are identified, then an action plan should be drawn up to rectify the issue. In the case of the most serious breaches a report will be submitted to the Audit Committee.

4 Responsibilities

Role	Responsibilities
Information Services Directorate	Define and authorise policy
Information Security Board	Create procedures, standards and controls
Information Security Manager	Has direct responsibility for maintaining this policy and providing advice on implementation.
Information Centre (Security Incident Response Team)	Handle incoming incidents
Information Services staff	Be familiar with and always adhere to the Incident Management Process.
End users	Be familiar with and always adhere to the Systems Usage Policy, regardless of their status.