University of Stirling
Information Technology Use Policy
Section 1
Introduction

This document is incorporated in *Regulations: Information Services* (and hence the University Regulations) and should be read in conjunction with that document.

1.1 Introduction to Policy

The overall aim of this Policy is to ensure that:-

- Required levels of ***confidentiality*** are always maintained
- Information is as ***secure*** as its level of confidentiality warrants
- ***Integrity*** of information is always protected
- Information is always ***available*** to those authorised to use the University's IT systems ("Users")
- Users understand what constitutes unacceptable Use of the University's IT
- Users understand the consequences of unacceptable Use

1.2 Introduction to Document

The Policy consists of four Sections as follows:-

Section 1 - Introduction
This Section provides an overview of the Policy, relevant laws and regulations.

Section 2 - Management Issues
This Section covers management responsibilities including the handling of incidents, Policy revisions and ensuring that all Users are fully aware of the Policy and its implications.

Section 3 - Acceptable Use Policy For Individual Use of Information Technology ("Individual AUP")
This Section sets out what constitutes acceptable Use of the University's IT by individual Users. All individual Users will be required to read and accept the terms of the Individual AUP.

Section 4 - Service Provider Policy for Information Technology Service Providers ("Service Provider Policy")
This Section sets out the framework governing the provision of IT services. It therefore goes beyond the Individual AUP in Section 3 in that it relates to service provision rather than just the Use of IT. The main such provider of IT is Information Services, but it will also cover IT services provided by Schools and by University Services generally, and indeed anyone providing services for others, e.g. operating web and other servers, installing communications equipment, and running systems.

1.3 Relevant Laws and Regulations

The University's IT and communications facilities and services must comply with the prevailing laws of the United Kingdom and Scotland; therefore all Users must comply with the relevant UK and Scottish legislation.

This Policy takes note of best practice within the sector, as well as relevant legislation and regulations, including the following:

Civic Government (Scotland) Act 1982
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Data Protection Act 1998

Digital Economy Act 2010
Electromagnetic Compatibility Regulations 1992
Equality Act 2010
Freedom of Information (Scotland) Act 2002
Health and Safety (Display Screen Equipment) Regulations 1992
Home Office Data Handling Requirements for Suppliers 2008
Human Rights Act 1998
Information Commissioner's Office *Employment Practices Code* 2005
JANET *Acceptable Use Policy* 2011
Obscene Publication Act 1959 & 1964
Protection of Children Act 1978
Regulation of Investigatory Powers Act 2000
Regulation of Investigatory Powers (Communications Data) Order 2010
Telecommunications Act 1984
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
University of Stirling *Single Equality Scheme 2009-2012*
University of Stirling *Rules and Regulations: Data Protection*
University of Stirling *Regulations*: *Information Services*

Any reference to a statute or regulation shall be deemed to be a reference to such statute or regulation as amended, substituted or varied from time to time.

1.4 Definitions
In this Policy, the following words and phrases shall have the meaning ascribed to them below:

Data Controller is the person who (either alone or jointly with others) determines the purposes and means of processing of personal data, as defined in the Data Protection Act;

Device means any network aware digital equipment used to access University password protected services on the University's network, via a fixed wired or wireless network point owned by the University or via the Internet from any location; digital equipment includes, but is not limited to, PCs, Apple Macs, laptops, data network aware mobile phones, iPhones, iPads etc; University password protected services include, but are not limited to, email, the Portal, Succeed, CampusNet etc;

Head means the Head of an academic School (as defined in Ordinance 48) or Service Director;

Individual AUP means the Acceptable Use Policy for Individual Use of Information Technology, set out in Section 3 of the Policy;

Information means any form of information or data capable of being stored or communicated in electronic form, including, without limitation, written, graphical, numerical, voice, music, video and multimedia data, Facebook (and similar social media) postings, YouTube material, Twitter postings, software and html and other programming code;

Information Centre means the information centre relating to information services at the University;

Information Technology (IT) means without limitation the computer hardware, software, networks, printers, peripherals and telecommunications equipment and digital services provided by the University for Users;

IT Security Officer means the person appointed by the Director of Information Services (currently the Manager of Systems and Network Services) or, if absent, the Director of

Information Services. The IT Security Officer can be contacted via emailing the Information Centre;

Malware means any software designed to infiltrate or damage a computer system without the owner's consent. It includes computer viruses, worms, Trojan horses, spyware, dishonest adware and other malicious and unwanted software**;**

Policy means this Information Technology Use Policy, including all Sections included within it;

Protected Personal Data means any Information about 1,000 identifiable individuals or more; or any Information that links at least one or more identifiable living person with the list of private information data sets appearing in the appendix to this Section (and this data set includes sensitive private data as defined in the Data Protection Act);

Provider means a person or organisation supplying or operating any IT or digital service to, or on behalf of, the University;

Section means a section included within the Policy;

University means the University of Stirling;

Use in relation to the University's IT, means any use of such IT in any manner including without limitation use to access, download, upload, process or communicate Information howsoever, and "**Using**" or "**Used**" shall be construed accordingly;

User means any person Using the University's IT; and

User Managers means the managers of Users, normally Heads, who have a key role in approving requests for their staff and/or students to be granted access to IT and additional services.

Appendix: Definition of Protected Personal Data

Source: Home Office Requirements for Suppliers: Definition of Protected Personal Data (September 2008)

Protected Personal Data includes all data falling into either category A or B below:

A. Any information that links one or more identifiable living person with private information about them

There should be protection for a data set that includes:

- One or more of the pieces of information through which an individual may be identified (name, address, telephone number, driving licence number, date of birth, photograph)

  combined with

- Information about that individual whose release could cause harm or distress, including:
  - Place of work
  - Bank/financial/credit card details
  - National Insurance number
  - Passport number/information on immigration status
  - Travel details (for example at immigration control, or Oyster records)
  - Tax, benefit or pension records
  - School attendance/records
  - Material related to social services (including child protection) or housing case work
  - Conviction/prison/court records/evidence
  - Groups/affiliations/political or other sensitive personal data as defined by the Data Protection Act (Section 2)
  - DNA or finger prints

Note this is not an exhaustive list. If in doubt contact the University's Data Protection Officer.

B Any source of information about 1,000 identifiable individuals or more, other than information sources from the public domain

University of Stirling
Information Technology Use Policy
Section 2
Management Issues

This Section sets out the management of the operation of this Policy.

2.1 Ensuring User Acceptance of This Policy

In order for this Policy to be fully effective it is essential that Users are fully aware of and accept the Individual AUP. Students are notified of the Policy and are required to accept it, when they are given access to the network. Staff are notified of the Policy and are required to accept it when they are first given access to the network. Other Users will be deemed to have accepted the conditions on first use of their account.

Access may be granted to selected IT services for individuals who have a significant connection with the University but who are not members of the University. Such access is at the discretion of the Director of Information Services (or nominated delegate) and will be in accordance with the published guidelines in "Eligibility for University IT Facilities and Services". Such users must agree in writing to abide by all Information Services' regulations and the Individual AUP, and privileges will be withdrawn in the event of any breach. Responsibility for any breaches of law or licence conditions and payment for any damages will be entirely their responsibility. There are regular reviews of permitted usage.

Copies of this Policy and any changes are published electronically on the University's website and may be obtained in alternative formats via the Information Centre.

2.2 Handling Disciplinary Action

Breaches of any of the Sections of this Policy are potentially disciplinary issues which for Users will be handled by the disciplinary procedures for existing staff and students or the loss of authorisation for IT use for others. Where contractual provisions entered into with any Provider are broken, account will be taken of relevant terms and conditions.

2.3 Handling Security Breaches

In Section 3 of this Policy, Users are asked to report any suspicion of a breach of the Individual AUP directly to the Information Centre by email. There will however be instances when, perhaps because of sensitivities, Users report it to a line manager or other senior individual. In these cases the person receiving the allegation should report it to Information Services either via the Information Centre or if necessary direct to the IT Security Officer or the Director of Information Services.

Where necessary the IT Security Officer will authorise summary suspension of access to both the accounts under threat and those of the alleged perpetrators. Where these involve access to departmental IT facilities, the IT Security Officer will make such decisions jointly with the relevant Head whenever practicable. The IT Security Officer will normally only act independently of the Head when there is a threat to services outside the department concerned, or where the Head is himself/herself involved in the alleged breach or where time is of the essence and the Head is unavailable. Initial account suspensions will normally be lifted within 2 working days unless a further suspension is approved by the University Secretary (or if absent the Director of Human Resources Services and Organisational Development for a member of staff or the Academic Registrar for a student), or unless it has been decided to take actions under the staff or student disciplinary procedures, in which case the provisions of the relevant procedures will apply.

In some cases the inquiry will involve the investigation of the traffic or content of User accounts in line with Section 3.9 of this Policy. Technical staff will normally only carry out such work on the direct instructions of the University Secretary (or if absent the Director of Human Resources Services and Organisational Development for a member of staff or the Academic Registrar for a student).

There is guidance available for staff on handling incidents involving social networking services, “Information Services guidance on social networking”.

2.4 Authorising Access to Information for Academic Purposes

Section 3.3 of this Policy contains the following statement:-

> “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 student Users must gain written approval from their Head, and other Users must gain written approval from the IT Security Officer, for these specific activities. Information that is illegal to possess is never allowed and any approval received will not cover or apply to such Information”.

When the Head or IT Security Officer is granting such approval care must be taken to ensure that it is specific and is not authorising the handling of illegal Information. A copy of this approval must be lodged with the IT Security Officer prior to any Use of the IT in reliance upon it, so that the IT Security Officer will know not to pursue what may be thought to be a breach of the Individual AUP.

When authorising such requests the Head should normally consult the IT Security Officer and be aware that he or she may be removing a ‘safety margin’ that normally protects Users from stepping over the boundary from ‘undesirable’ to ‘illegal’ Information. For this reason the Head or IT Security Officer should normally remind the requestor to be particularly vigilant when working in these areas.

2.5 Management of the IT Use Policy

The Director of Information Services will take the lead in an annual review of this Policy, with any revisions being approved by the University Court.

This version of the Information Technology Use Policy was agreed by University Court on 20 June 2011 and became effective on 1 August 2011.

University of Stirling
Information Technology Use Policy
Section 3
Acceptable Use Policy
For Individual Use of Information Technology
("Individual AUP")

The University provides facilities for the creation of and access to a wide range of Information via its IT facilities. This Individual AUP sets out how the User may and may not use IT facilities (whether provided by the University or by the individual) to support their individual work and applies equally to all Users.

You must read, understand and accept this Individual AUP before you use IT at the University.
If there is anything you do not understand it is **your responsibility** to ask the Information Centre to explain. Any breaches of this Individual AUP may result in disciplinary action which may result in dismissal from employment or programme of study, or revocation of your authorisation to Use the IT. Where an illegal activity is suspected to have taken place the University is likely to request the police to investigate.

If you Use IT for more than individual use, e.g. operating a web server, running a system used by more than one person or configuring network equipment, you must additionally comply with the more detailed 'Service Provider Policy' at Section 4.

Copies of this document are available on the University's web site and from the Information Centre.

****

3.1 SCOPE OF POLICY

a) This Individual AUP covers ALL the use of IT and ALL the ways Information is accessed using IT.

b) This Individual AUP applies to ALL Users.

c) This Individual AUP applies to ALL Use of IT wherever such usage takes place and regardless of ownership of the equipment involved.

3.2 ALLOWABLE USE

a) The University provides IT to support the educational, research, administrative and business functions of the University, including access for personal development to improve individual knowledge, skills and career enhancement. The only other Use allowed is as defined below under 'private use'.

b) Private Use of IT (i.e. use for leisure or other personal pursuits) is allowed by Users subject to the following conditions:

   i) the private Use does not inconvenience or distract educational, research, administrative or business Users;
   ii) for staff, such private Use does not interfere with their individual work as an employee or impede the work of other Users;
   iii) all private Use complies with any relevant legal obligations and constraints, including copyright protection of downloadable files (which includes, but is not limited to, embedding copyright material into digital works);
   iv) such private Use does not adversely affect the performance, reliability or availability of the University's systems for other Users (examples of types of

Use that may place such loading include the transfer of music and video files, the playing of games over the network or similar network-intensive activities);

v) any personal financial transactions conducted using IT facilities are conducted at the individual's own risk;
vi) files associated with private Use must not interfere with educational, research, administrative or business activities;
vii) the private Use must not involve activities which may bring the University into disrepute or which involve a misstatement implying that such Use is official Use in accordance with University business or otherwise not in a private capacity;
viii) the right to private Use may be withdrawn at any time by the University in respect of any User or Users, including without limitation where such right is abused or interferes with the efficient operation of the University;
ix) all private Use is exercised at the User's own risk and the University shall not be liable for any loss suffered by any User is respect of such private Use, including without limitation any loss caused directly or indirectly by any virus or any loss of data or Information of the User or any failure of the IT or loss of availability or functionality of the IT whatsoever; and
x) the private Use is not a prohibited Use in terms of Section 3.3 below.

c) Private Use specifically excludes:
(i) private commercial activity which breaches licensing conditions or copyright (as described in Section 3.6 below);
(ii) betting and gambling;
(iii) transfer of music, video and multi-media files where this infringes copyright;
(iv) playing of games for leisure over a network.

3.3 PROHIBITED USE

a) Information used by a User must not be offensive, abusive, discriminatory, illegal to possess, damage the University's interests, or otherwise contravene University regulations. Users should note that possession or dissemination of such Information may be a criminal offence. Users should ensure that their Use of IT complies with all relevant UK and Scottish laws, including, without limitation, laws relating to: discrimination on grounds of age, disability, gender reassignment, marriage and civil partnership status, pregnancy and maternity, sex, sexual orientation, race, religion and belief; libel and defamation; copyright protection. The University does not tolerate the use of its IT Systems to discriminate unlawfully, harass or bully.

Examples of offensive Information include all forms of pornography and violent images. These examples would certainly include:-
i) indecent images of children under 16 which it is illegal to possess; and
ii) obscene materials which it may be an offence to publish but not to possess.

Other examples might be:
i) materials comparable to those available on the top shelf in a newsagent which is neither an offence to publish nor possess but which some may find distasteful; or
ii) materials which could be construed as distasteful to reasonable people.

b) Users should note that Use applies equally to all storage, processing or transmission of Information, examples of which would include viewing of web pages, data files and the content of emails, Facebook postings, Twitter postings, blogs, wikis, podcasts, Instant Messaging sessions and content produced by similar electronic communication tools and services.

c) Alleged breaches of 3.3 a) or 3.3 b) above may result in material and communications being removed from information systems managed by the

University; this may be temporarily while an investigation is underway or permanently in the light of the results of an investigation and/or disciplinary action.

d) 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 student Users must gain written approval from their Head, and other Users must gain written approval from the IT Security Officer, for these specific activities. Information that it is illegal to possess is never allowed and any approval received will not cover or apply to such Information.

e) The University recognises that Users may accidentally connect to unacceptable web sites or receive unsolicited unacceptable emails. In these cases audit logs may be used to demonstrate that such visits are rare and short, and hence likely to be unintentional and so not constituting a breach of this Policy.

f) No User is permitted to create or transmit unsolicited bulk or marketing material to Users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which Users have chosen to subscribe or is part of the normal official operating activities of the University.

3.4 ENSURING SECURITY

a) Passwords must be handled responsibly as they are the 'keys' to IT facilities and hence are allocated to individual Users and must be kept private to that User. Misuse of a password is a serious breach of security, and will lead to disciplinary action or withdrawal of access to the University's IT.

Each User is responsible for all Use made via a password allocated to such User (including, without limitation, all access to web pages or other Information, all sending of email communications, etc).

b) Users must not disclose their password to anyone by any means whatsoever. Information Services staff will never ask a User to disclose their password.

c) A password which a User becomes aware had been discovered by others must be promptly changed.

If at any time a User thinks someone may have discovered their password, perhaps by watching them type it, they must immediately either change it themselves or contact the issuer. If in doubt as to who to contact call the Information Centre in the first instance.

d) When required to change passwords Users must ensure that such changes are made promptly.

e) New passwords must be at least 6 characters long and must not include strings easily remembered by others. Users are advised to use a combination of letters and digits in passwords; it is not good practice to repeat the use of a password, or to use personal names of the User or the User's partner, or children etc as a password. Passwords must never be written down.

f) A Device (such as PC) must never be left logged into a User's personal account (ie a section of the IT system with restricted access protected by a password) unless the Device itself is locked or the location of the Device is physically secure. Users are responsible for ensuring that no one else can use a Device which is logged in under their User ID as such other person could send emails in the User's name, read confidential files, change private data, or spend a User's printer credits.

If a Device, whether personally owned or supplied by the University, is synchronised with data stored on a University system (such as email), then as a minimum that Device should have a pass code enabled to prevent unauthorised access.

Users must not log on to any other person's account. Arrangements may be made for new temporary users by contacting the Information Centre.

g) Users are responsible for ensuring that, when using IT to use Information of a confidential nature, all reasonable precautions are taken to protect the confidentiality of such Information. In particular, without limitation, Users must ensure that when carrying out confidential work on a Device, such as a PC, the screen cannot be read by others.

h) Appropriate encryption should be used for Information of a confidential nature stored on a portable Device (such as laptops) and portable storage media (such as USB storage devices, CDs, DVDs etc.).

i) Portable Devices and portable storage media must be kept physically secure.

j) In the event that a Device synchronised with data stored on a University system is lost or stolen, the User must immediately change all University passwords.

k) Information relating to University work or study should normally be kept on a "network drive" provided and administered by Information Services, and it can be assumed that back-up security copies are being taken. Information containing Protected Personal Data must only be stored on a "network drive".

Notwithstanding (k) above, if a User chooses to store the Information on a local hard disk, (often designated "C", "D" or "E" drives on a Windows PC), then the User must also periodically make a back-up copy of such Information to a suitable form of another storage device, which should then be kept securely.

3.5 ABUSE OF SECURITY

a) Users may only attempt to Use IT facilities 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 facility. Such Use is always subject to the terms of this Individual AUP.

If a User is not sure whether they have rights to access a facility they must contact the administrator of that system before attempting access.

b) All forms of 'network probing or sniffing', hacking, and any unauthorised modification of any IT are prohibited unless specifically approved in writing by the IT Security Officer.

c) Users must not undertake any actions to disable or circumvent systems which protect the security of a University owned Device. This includes anti-virus, firewall and prevention of unauthorised software installation measures.

d) Users may not connect equipment to the network not approved by the IT Security Officer.

Any breach of this Section 3.5 of the Individual AUP may be a criminal offence under the Computer Misuse Act 1990 to the extent that it constitutes illegal use of hardware, software or information.

3.6 BREACH OF COPYRIGHT AND LICENCE CONDITIONS

a) Users should never copy (including copying by downloading), reproduce or distribute any Information (including any music, videos and computer programs) unless specifically authorised by the owner or licensor of the copyright in such Information, or to the extent otherwise permitted under the Copyright, Designs and Patents Act 1988. If Users have any queries about copyright compliance, they should contact the University's Data Protection Officer.

b) Information is usually licensed for educational (i.e. teaching on a University programme and research) use only. It must not be used for other purposes unless either more broadly based licence conditions are publicised via the University's website or the specific authority of the person holding the licence on behalf of the University has been obtained and even then only if the licence allows such use. Such 'other purposes' will in general include consultancy, student projects that benefit other organisations, and presenting short courses.

3.7 BREACH OF DATA PROTECTION ACT

a) Personal data must only be stored, managed and processed in accordance with the Data Protection Act. This Act requires that all personal data be handled and processed fairly and lawfully for only the purposes registered; that such data and its processing be minimised in achieving those purposes; that it be kept only as long as necessary to achieve those purposes; that it be kept up to date; and that it be kept securely. This covers any data which relates to a living individual who can be identified from that data or from that data and other Information which is, or is likely to come into, the possession of the Data Controller.

b) Users must comply with the terms of the University's "Regulation on Data Protection", which forms part of the University Calendar. All personal data must be kept securely in accordance with section 3.4.

c) No unencrypted portable Devices, or portable storage media, containing Protected Personal Data, should be taken outside secured office premises nor any Protected Personal Data transferred to third party owned Devices or storage media without the prior written consent of the University's Data Protection Officer. Protected Personal data should not be transmitted by email.

d) If in doubt about the implications of the Data Protection Act Users must consult the University's Data Protection Officer.

e) The University's Data Protection Officer must always be consulted where personal data is to be transferred to a third party. This includes storing any personal data on an information service which is not managed by the University. Regular transfers to University partners do not require a separate consultation with the University's Data Protection Officer for every transfer.

f) Disposal of University owned Devices and storage media must be in accordance with the University's "Disposal Procedure" which can be found on the University's web site.

g) In the event of suspected, or actual, loss, or unauthorised disclosure, of personal data, the University's Data Protection Officer must be informed immediately.

3.8 COMPUTER MALWARE

a) Users are responsible for taking all reasonable precautions to ensure that computer Malware (ie any software designed to infiltrate or damage a computer system without the owner's consent; eg computer viruses, worms, Trojan horses, spyware, dishonest adware and other malicious and unwanted software) is not introduced, or disseminated. Users must follow notices and instructions on how to reduce the impact of Malware.

b) Users of a Device such as a PC that is to be connected to the University's network or networks (except for IT equipment wholly managed by Information Services) via a fixed wired or wireless connection point owned by the University must ensure that Malware checking software is permanently installed, regularly updated and always active on that Device and that software patches addressing security issues are kept up to date. Further information is available from the Information Centre.

Users may assume that Malware checking software is installed on IT equipment wholly managed by Information Services on University premises. Users should email the Information Centre immediately in the event that they become aware of the presence of Malware.

c) Users should be aware that email attachments may carry Malware. If a User suspects that this may be the case, the User should not open the attachment but should contact the Information Centre for advice.

d) If a User believes a University owned Device has been infected by Malware, the User must immediately stop using it, switch off and email the Information Centre.

e) If a User obtains information about Malware, the User must notify the Information Centre. The User should NOT circulate the information to other Users as there are many false Malware alerts.

f) If Information Services becomes aware of Malware on a Device, access for the Device to the University's network may be removed.

3.9 RIGHTS TO RECORD, MONITOR AND INTERCEPT

a) The University reserves the right to (i) access all Information on its IT equipment; (ii) monitor and/or record all Use of IT by Users (subject to the University complying with the Data Protection Act (1998), Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Human Rights Act 1998); (iii) withdraw services at any time and without notice; and (iv) pass on any unapproved costs to Users.

b) The University undertakes that any access to, monitoring and/or recording of emails, data files or web access containing personal data will be carried out in line with the UK Information Commissioner's *Employment Practices Code.*

c) This Individual AUP sets out the conditions under which Users should be aware that access to, monitoring and/or recording of their use of, the University's IT may take place:

i) the business purpose of any access, monitoring and recording will be established and any information collected will only be used for the purpose for which the access, monitoring and recording was introduced;

ii) automatic blocks on content may be set;

iii) where possible access, monitoring and recording will be of traffic data rather than content. Traffic data includes email and web addresses, message headings and size but not what is written within the message and web pages;

iv) quantitative and qualitative monitoring and recording may be used in the management of specified services, such as a help desk;

v) third party automatic monitoring may be used for the purpose of diverting Users to web pages with changed locations;

vi) support tools to allow support staff to provide real-time remote diagnosis and resolution of problems may be installed on some systems. No individual Device will be accessed without the member of the University using that system first giving their express permission.

d) **Access for Business Purposes**

i) Where staff are absent, and prior arrangements have not been made, upon the authorisation of the Head (or nominee), a member of staff nominated by the Head may open emails and data files to ensure correct business responses. This will not breach password security procedures as described in section 3.4. The information will not be used for other purposes unless it reveals suspected criminal offences or serious misconduct, in particular any item marked confidential or similar will not normally be viewed. This type of access will be revoked when the member of staff returns;

ii) Where access, monitoring and interception are carried out on the basis of detecting viruses, blocking unsolicited emails and access to unacceptable Information the processes will be automated wherever possible;

iii) Except as described above, monitoring information will only be collected/accessed for the purpose of preventing or detecting a crime or the apprehension of offenders, or in the case of suspected serious misconduct. The affected Users will be informed of this action before it takes place unless this would be likely to prejudice this purpose.

e) **Access for Academic Purposes**

i) Students should be aware that work submitted for assessment is subject to paragraph 24 of the “Intellectual Property Policy” in the University’s Calendar.

ii) Students should not submit to plagiarism detection software used at the University on behalf of other students.

iii) Students should be aware that when classroom control software is in use, staff may view their activity in IT laboratories.

iv) Staff should be aware when using classroom control software that :

a) it is possible, but forbidden, to access students’ home folders without the explicit consent of each individual
b) care must be taken not to use the ‘logoff’, ‘reboot’ or ‘send messages to all’ functions inappropriately.

****

If a User becomes aware of, or has any suspicions of, any breach of this Individual AUP then he or she must email the Information Centre immediately. If the issue is confidential the User does not need to give details to the Information Centre but can just ask the staff there to arrange for a senior member of Information Services staff to contact them directly.

Student and staff member Users should remember that any breaches of this Individual AUP could result in disciplinary action which may result in dismissal from employment or programme of study. Users should remember that any breach of this Individual AUP can result in the withdrawal of authorisation to Use the University's IT. Where alleged illegal activity may have taken place the University may bring in the police to investigate.

University of Stirling
Information Use Technology Policy
Section 4
Acceptable Use Policy for the
Information Technology Service Providers
("Service Provider Policy")

4.1 Scope of this Policy

This policy applies to the operation of any communication and information technology equipment within or owned by the University that provides services to others. This includes servers (MIS, data, application, web, others), information on servers, and communications equipment. Within this Section all such devices are referred to as 'systems'. Most of these systems are operated by Information Services but this Policy also applies to anyone operating such equipment directly connected to the University's network, for example a web server for a research project or a University business system.

The 'Acceptable Use Policy for Individual Use of Information Technology' (Section 3) also applies to any User involved in an IT service Provider role.

4.2 Roles

Within this Policy a number of roles are referred to as defined below:

System Owner – A member of staff who is the final authority for any item of equipment or set of Information which is in use for legitimate University business purposes but not wholly within the responsibility of Information Services. This may cover equipment, software, processes, data or a combination of these. For example the Director of Finance would be the owner for the University's Finance system. The System Owner is expected to consult with Information Services before the specification and purchase or before commissioning any substantive upgrades.

System Custodian - Delegated by the System Owner to be responsible for system management functions. Systems must be managed by suitably trained and qualified personnel to oversee their day to day running and to preserve security and integrity in collaboration with System Owners. All personnel with systems management responsibilities shall be given relevant training in information security procedures.

IT Development Personnel - These carry out work that involves changing or extending IT systems. As part of this Policy they have a duty to ensure that work is carried out in a way that complies with this Policy. If appropriate, they will implement automated security measures.

IT Operational Personnel - These carry out work to ensure the correct operation of IT systems in accordance with this Policy and operational instructions.

IT Security Officer - The senior member of staff in Information Services who has the responsibility for ensuring that this Policy is enforced. The role holder will:

- understand the IT infrastructure of the University as relevant to security;
- authorise temporary suspension of accounts pending instructions from the System Owner, the appropriate User Manager, the Director of Human Resources and Organisational Development or Academic Registrar;
- approve and register the attachment of equipment to the network as in 4.3. below;
- approve the attachment of 'non compliant systems' as in 4.4 below.

4.3 Registration and operation of IT Systems

All systems that fall within the scope of this Policy must be registered with the IT Security Officer and operated as agreed, in terms of compliance, network security etc. Each system should have one, and only one, System Owner and one, and only one, System Custodian. Every System Owner and Custodian should have a designated deputy who can fulfil the appropriate role in the event of absence.

Information Services reserves the right to disconnect any IT System from the University's network without warning at any time; before this eventuality, Information Services will make all reasonable attempts to contact the System Owner or System Custodian.

4.4 Managing the Operations Environment

Particular thought must be given to the logical and physical operational environment as access to this environment normally allows conventional IT security to be circumvented. IDs/Passwords used in this environment that provide privileged access to systems for system management and operational reasons must be managed as below.

User IDs (for higher levels of access to systems) - These IDs will normally be allocated to specific Users but will not normally be the same as used by that User for his/her normal work, i.e. they should only normally be used for the approved operational tasks. In some cases these 'super user IDs' are dictated by the system, and hence are used by more than one User. This will be avoided wherever possible.

Account Creation/Modification - Accounts will only be created with the written authority of the System Owner or the nominated depute. No person with the capability to create an account may do so without authorisation.

Access Rights - Account configuration will be carefully considered to allow access only to appropriate Information on the system as agreed by the System Owner. If necessary a User may be issued with multiple user IDs so that the more powerful ID is used only when necessary.

Logging Usage - All activity through these accounts must be logged if the system permits. The logs should be stored by the System Custodian in accordance with the policy described in "Management, Storage and Retention of Systems Logs for IT Systems" and made available to the IT Security Officer on demand.

Account Deletion – Procedures will be implemented to remove these accounts immediately they are not required for either operational or staffing reasons.

Passwords (for User IDs with higher levels of access) - All the principles defined in section 4.9 for the management of user passwords apply but due to the importance of the privileged access rights of these staff the following additional points apply:

- these types of passwords must be routinely changed as agreed;
- shared passwords should normally be changed immediately any User with access to the passwords leaves the University, changes role, or is subject to disciplinary procedures;
- whenever passwords are changed, copies must be lodged with the relevant System Custodian.

Development Personnel - Internal and external development personnel will not normally have update access to the operational environment for 'live systems'. In exceptional cases when this access is required it will take place with the written authorisation of, or in the presence of, the System Custodian.

Physical Environment - Access to systems and system consoles can allow normal security measures to be circumvented. All environments where such equipment is located must be physically secure. Unauthorised personnel should never be left unattended with access to systems.

Change management – The implementation of new or upgraded software must be carefully planned and managed, to ensure that the increased information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

Formal change control procedures, with audit trails, must be defined by the System Owner and used for all changes to systems. All changes must be properly tested, and authorised by the System Owner, before moving to the live environment.

4.5 Backup and Media Control

In order to guarantee the security of Information, systems should be configured to reduce the chance of loss of data stored on fixed media. All systems must be backed up to portable backup media and copies stored in remote location. Use of fault tolerant equipment and security measures will be agreed with the IT Security Officer, as in 4.3.

Verifying Backup Media - A procedure should normally be implemented to read samples of the backup media on an alternative system to ensure the contents of the media are readable and contain the intended Information. In the event that a risk assessment has been undertaken which concludes not reading samples of backup data is an acceptable risk, this must be agreed by the System Owner in discussion with the IT Security Officer.

In the event that the System Custodian delegates the day to day operation of backing up, they must ensure and verify that adequate procedures are in place to meet the obligations of this Section.

4.6 Malware

This includes all types of malicious programmes. Measures must be implemented to protect against the introduction, spread or storage of such programmes.

4.7 Managing User Accounts on Business Systems and similar

(Note: Use of network accounts is governed separately by Information Services)
The following principles must be followed in the management of User accounts on IT equipment:-

User IDs - Where a service is provided to more than a single School or Service Area, the standard University user ID must be used as issued by Information Services.

Account Creation/Modification - Accounts must only be created within the guidelines agreed between the IT Security Officer and the System Owner.

Access Rights - All accounts must be configured where practicable to allow access only to appropriate Information on the system as defined by the System Owner.

Account Deletion - Procedures must be implemented to remove accounts when no longer required for either operational or staffing reasons.

4.8 Managing Shared Accounts

These are not normally permitted as it is not possible to know who is using them in the event of any security breaches. They may be allowed for special purposes on the written approval of the System Owner when their functionality is suitably restricted.

4.9 Managing User Passwords

Accounts should normally have passwords. The only exceptions will be as approved by the IT Security Officer. Systems must be implemented to ensure passwords are managed in line with the following principles.

Structure of Passwords - Passwords should be at least 6 characters long and include alpha, numeric and at least one character of another type where systems permit. Their structure must be random. Recognisable passwords may be allowed if the user is forced to change the password the first time it is used.

Initial Password Creation - All accounts should normally be allocated a password at creation. The System Custodian should keep secure copies of these passwords only if required. If this practice is adopted, the User should be notified this is the case. Passwords must be issued to Users in a secure way: normally face to face or by sealed confidential post.

Password Changing by the User - Facilities should be available for each User to change password in a way that keeps the password confidential to the individual, where systems permit. Passwords must be changed periodically, for example: at least every 3 months for systems containing sensitive Information, such as personal, financial, staff and every 6 months for students. These changes should normally be forced by the system where the system permits this. Passwords must not be reused within 12 months where systems can be configured to enforce this.

Password Changing by IT Operational Personnel or System Custodians - Normally when a User has forgotten his/her password, it will be necessary for passwords to be changed. In these cases the same authority will be required as for account/password creation.

Not displayed - Passwords should never be displayed on screens.

Stored Securely/Encrypted - Password files on systems must normally be stored in secure files or encrypted in a way which prevents unauthorised recovery.

Incorrectly Entered Passwords – Where systems permit, all unsuccessful logins should be logged and monitored and, if necessary, the accounts should be suspended pending investigation.

Disclosure of Passwords – Users must never be asked to disclose their passwords.

4.10 Data Protection Act and Confidentiality

All data relating to individuals must be stored in secure filing systems and managed and processed in accordance with the Data Protection Act. Information regarding the requirements of the Data Protection Act may be obtained from the University's Data Protection Officer. Protected Personal Data must be managed in accordance with sections 3.4 and 3.7 of this Policy. Tools to enable remote support (that is, where a User is assisted by support staff taking control of the Device he or she is using by the means of software operating on another Device) must not be used on a Device used by a User without their express permission beforehand. This should be obtained preferably by phone and the remote access only enabled once work has been saved where possible. The confidentiality of files must be respected at all times while using remote support tools.

Access rights should be assigned to minimise the number of Users who can transfer personal data onto other systems or portable storage media and the amount of such data which can be transferred. Wherever possible there should be audit logs to record such transfer of personal data.

4.11 Investigating Security Incidents

If a System Owner or User Manager suspects a breach of security, he or she should contact the IT Security Officer. Investigation and suspension of accounts will be dealt with according with the procedure set out in 2.3.

Breaches of this Service Provider Policy could result in disciplinary action which may result in dismissal from employment or programme of study. Where alleged illegal activity is suspected to have taken place the University is likely to bring in the police to investigate.