University of St Andrews

Regulations governing the use of University information and communications technology (ICT) facilities

Document type	**Policy**
Scope (applies to)	Staff and students
Applicability date	30/04/2012
Review / Expiry date	29/05/2020
Approved date	03/07/2019
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
Equality impact assessment	None
Key terms	Information technology
Purpose	To communicate the conditions of access to ICT faclities provided by or through the University, and to establish what is/is not acceptable use of those facilities.

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.5	Requirement for strong passwords clarified (section 6.5.3) and the confidentiality of administrative passwords reinforced (section 5.1)	Approved	C Milne, Head of Information Assurance and governance	14 Feb 2019

1. Introduction

Whilst the benefits and opportunities available through Information and Communications Technology (ICT) such as the Internet, wireless/portable computing and mobile communication etc. are widely recognised and appreciated their use is not without risk to the University, its students, staff and the wider communities served by the institution. To exploit the opportunities offered through ICT and to minimise the threats access to these technologies requires effective management.

2. Purpose and scope

The purpose of this University Regulation is to provide a set of parameters which with other internal and external instruments sets out conditions of access and levels of use of ICT facilities and services provided by or through the institution (defined in Section 3, below) which are *acceptable* to and required of the University (or any of its entities).

These Regulations are intended to support and as appropriate ensure the:

- Proper use of ICT facilities and services;
- The protection of Authorised Users (defined in Section 3 of these Regulations), the University and others external to the University who may be impacted by the use of ICT facilities by Authorised Users of the institution;
- Appropriate access to and management of these resources.

2.1. Intended audience

These Regulations apply to all individuals who have been granted access *to ICT facilities* and services provided by or through the University i.e. Authorised Users (defined in Section 3 of these Regulations).

2.2. Where these Regulations apply

These Regulations apply to all locations and instances where ICT facilities and services provided by or through the University are accessed – irrespective of the ownership of the technology and the service(s) used to access those ICT facilities and services. Consequently, these Regulations apply to all out of office (e.g. home) access.

3. Definitions

3.1. Authorised users

Are:

- Students and other learners associated with the University of St Andrews who have completed their registration with the University onto a programme or course of study;
- Staff, i.e. individuals under a contract of employment with the University or an entity of the University;
- Members of the University Court;
- Elected student officers;
- Third parties i.e. contractors or sub-contractors engaged under contract to undertake work for the University;
- Any other person or entity formally authorised by the University to use the ICT facilities, through a recognised and approved business processes.

3.2. Information and Communication Technologies (ICT) facilities

Shall mean:

- The University's (or any entity thereof) Information Technology (IT) systems (i.e. under direct ownership or licence agreement where the University is a party) - including but not necessarily limited to:
  - Personal and mobile (i.e. laptop) computers and tablet/smart devices;
  - All types of mobile communication devices including those capable of connecting to the Internet and other networks;
  - Telephones;
  - Network, i.e. fixed and wireless;
  - The University intranet;
  - Electronic mail and other person-to-person or group communication services;
  - Virtual learning environments, e.g. Moodle, MMS;
  - Software;
  - Hardware;
  - (Recorded) information;
  - Data.

- Information Technology (IT) systems provided by the University to Authorised Users through third party providers – including but not necessarily limited to:
  - All of the items listed above;
  - External resources including JANET, Eduroam and other or successor networks and systems such as the Internet accessed by means of the University's IT systems;
  - External "Cloud" computing providers;
  - Copyright materials procured under contract or licence, e.g. electronic journals, books and data-sets, e-learning materials.

3.3. Authorised use

Is consistent with:

- The education, research and mission of the University;
- The conditions as set out within these Regulations;
- The terms of any licence agreement unless otherwise prohibited by the terms and conditions of another agreement with which the University has formally entered into and/or accepted.

3.4. Processing

In relation to materials, data or information will take the same meaning as that set out in General Data Protection Regulation ("the GDPR").

4. Legislative and regulatory framework

Use of University ICT facilities is subject to applicable legislation from a number of jurisdictions (UK, Scottish and European), external regulation governing the use of UK academic computing and communication facilities and by the terms and conditions provided for by license agreements. This includes legislation that creates a duty on universities to have due regard in preventing people from being drawn into terrorism. These Regulations also apply in supplement to existing University Policy and Regulation. Notable legislation and regulatory items are listed here to illustrate the range of conditions under which University *ICT facilities* should be used and managed.

A complete list of relevant legislative and regulatory items is not provided. Omission of a particular legislative item or regulation etc. from these Regulations does not negate the responsibility of either the University or an individual to meet other obligations set out in law or in regulation.

4.1. Legislation

- Computer Misuse Act (1990)
- Copyright, Designs and Patents Act (1998)
- The Data Protection Act (2018)
- Human Rights Act (2000)
- The General Data Protection Regulation
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information (Scotland) Act (2002)
- Communications Act (2003)
- Trade Marks Act (1994)

4.2. Regulation

- JANET Acceptable Use Policy[1]

Reference to any legislative or regulatory item (or similar instrument) shall be construed as a reference to that item as amended by any subsequent or successor legislation, regulation or instrument.

4.3. Relationship with existing University Policy, procedures and Regulation

These Regulations provide the overall framework for the management of ICT facilities to help ensure their use is and remains acceptable to the University. These Regulations do not work in isolation. Other University Policy, (published) procedures and Regulation are also of relevance in providing direction and more detailed discussion. In the main, these policy areas are concerned with preserving and maintaining the confidentiality, integrity and availability of information and information systems (i.e. *Information Security*) and the safe and secure handling of information, data and personal data (i.e. *University policy and guidelines on information classification)*, the legal and ethical use of information and intellectual property and the protection of the rights and freedoms of individuals. Specific items include:

- Data protection policy;
- Disciplinary procedures (excluding those covered by the Model Statute);
- Disciplinary procedures (Academic);
- Harassment and bullying at work and study policy; and
- Information classification policy.

As noted throughout these Regulations, compliance with the conditions set out here will on occasion also require observance of other University Policy and Regulations referred to herein.

5. Access to ICT facilities

All Authorised Users of the ICT facilities must comply with these Regulations and all other legislation, regulation and instruments referred to herein and any rules made by the University from time to time for the day-to-day operation of these facilities. Authorised Users must also comply with any instructions given by University staff in the performance of their duties when connected to the management of ICT facilities.

No person shall use or cause to be used or seek access to any of the ICT facilities provided by or through the University without having first obtained full registration or formal authorisation from the University as an Authorised User.

[1] Available online: https://community.jisc.ac.uk/library/acceptable-use-policy, accessed 05 January 2017

5.1. Authentication credentials

Physical access to ICT facilities is normally controlled, i.e. authenticated, via username and password. On occasion other forms of authentication may be used e.g. Multi Factor Authentication. Credentials, which also include those required for accessing 'administrative' systems are assigned to individual Authorised Users on the strict understanding that each Authorised User:

- Accepts that all authentication credentials assigned to them are and shall remain for their sole use;
- Is responsible for taking all reasonable actions to maintain and preserve the integrity of all authentication credentials issued to them – in particular their nondisclosure or release in any form to any individual;
- Shall take sensible precautions to ensure that ICT facilities to which access is authenticated via username and password etc. are denied to all other persons other than a legitimate Authorised user – this will include ensuring that when unattended a device or service that an Authorised User is logged on to, cannot be accessed by another individual, normally by locking the device;
- May be held liable by the University for misuse of ICT facilities (or other associated actions) where the Authorised User has failed to take all reasonable actions to maintain the integrity of authentication credentials issued to them.

6. Use of ICT facilities

6.1. General conditions of use

Use of ICT facilities must be acceptable to the University and consistent with the definition of Authorised Use as set out in these Regulations (see Section 3.3), and thus comply with these Regulations, and the legislative, regulatory and policy frameworks and other relevant instruments presented herein.

Use of ICT facilities should always be legal and as appropriate reflect academic integrity and the standards and requirements of the University. In order to achieve this, Authorised Users must accept the need to be restrained in the use of available resources. This may include on occasion surrendering the use of ICT facilities (following the direction of a member of University staff) and making those facilities available to other Authorised Users where there are pressing resource constraints and access is required to undertake activities as described in section 6.2 of these Regulations with the exception of activities falling within the scope of personal use (see section 6.4). Use should demonstrate respect for intellectual property, the ownership of data and the preservation and maintenance of the confidentiality, integrity and availability of information (including personal data) and information systems available at and through the University.

The University has a statutory duty to have due regard to the need to prevent people from being drawn into terrorism. When working with such materials, Authorised Users must ensure that such activities fall within the academic and/or research requirements of the University at all times.

Authorised Users must also accept that use of ICT facilities may be monitored under specific conditions defined by law (see Section 9).

6.2. Use of ICT facilities

Authorised Users may use the ICT facilities only for purposes directly related to (as appropriate):

- Undertaking a programme and/or course of study – including the administration and management of learning;
- Academic research – including the administration and management of research;
- The discharge of duties of employment with the University (or an entity of the University) or in the completion of a contract with the University (or an entity of the University);
- Executing duties associated with a position of office, e.g. the University Court;
- A reasonable level of personal use (as defined in Section 6.4 of these Regulations).

6.3. Non-acceptable use

An absolute definition of the use of ICT facilities which is *not acceptable* to the University is difficult to achieve, but certainly includes – but is not necessarily limited to actions that:

- Are concerned with unlawful activities;
- Expose the University to legal and/or regulatory liability or significant reputational damage;
- Expose an Authorised User to legal and/or regulatory liability or disciplinary action by the University for a breach of any of its Policy or Regulation, including offences surrounding the promotion of terrorism;
- Are abusive or threatening to others, e.g. serves to harass, bully, discriminate or incite discrimination or extremism;
- Are designed or likely to result in the degradation, loss, damage or destruction of ICT facilities (as defined by these Regulations) and allied services;
- Threaten the preservation and/or maintenance of the confidentiality, integrity and availability of data, information and services;
- Attempt to circumvent any of the University's own or linked computing and Information Security measures;
- Infringes third-party copyright or other intellectual rights;
- Exceeds the University's view of acceptable personal use (see Section 6.4 of these Regulations).

6.4. Personal use

A reasonable level of personal use of ICT facilities is permitted on a conditional basis. Personal use of ICT facilities must not interfere with University business or the performance of specific University duties. Abuse includes the personal use of ICT facilities that:

- Causes unwarranted expense, disruption or liability to be incurred by the University;
- Significantly impedes or adversely affects performance and/or availability of ICT facilities and allied services to other Authorised Users;
- Is connected with private commercial business unless formally approved by the University Court.

Personal use of ICT facilities outwith that deemed reasonable by the University may then constitute a breach of these Regulations (see Section 15).

6.5. Specific requirements and prohibitions (of use)

It is beyond the scope to these Regulations to provide an exhaustive list of all possible prohibitions concerning the acceptable use of *ICT facilities* provided by or through the University. For the avoidance of doubt and/or where it is necessary to provide more detail and/or instruction a number of selected areas are highlighted here.

6.5.1. Information security and information handling

The University Information Classification Policy and supporting implementation guides establishes a framework – encompassing appropriate guidance and a suitable set of controls (including allied University policy, lines of responsibility) designed to ensure that specific information security objectives and standards for information handling and use required by the University to maintain and preserve the *confidentiality, integrity and availability* of information and the systems deployed to create, disseminate and manage that information remains uncompromised and available to the University. Use of *ICT facilities* by Authorised Users must always be consistent with maintaining and preserving the *confidentiality, integrity and availability* of University information and information systems.

6.5.2. Personal information (Data protection)

No Authorised User shall use the ICT facilities (as defined herein) to hold or process personal data and or sensitive personal data (as defined by Sections 1 and 2 of DPA) except in accordance with the provisions of that Act. It should be noted that the said Act contains a number of exemptions. The Act allows for the processing of personal data for domestic purposes where those (personal) information are used by an individual only for that individual's personal, family, or household affairs (which include any recreational purposes).

Authorised Users should refer to the University Data Protection codes, University Policy and guidelines on information classification and handling and to specific fair collection notices issued by the University for further Information on the manner in which personal information should be collected and processed.

Data protection legislation requires that organisations take steps to ensure that the facilities and services used to process personal data are such that those data can be processed i.e. collected, stored and used without risk to the rights and freedoms of individuals. In that regard the University before engaging with an ICT service provider will carry out due diligence to ensure that personal data for which it is responsible for can be made available without any undue risk to individual's privacy and the institution. No Authorised user should transfer personal data to IC facilities and/or services which have not been first approved by the University. Examples of such prohibitions would include the forwarding of non-personal emails from a University email account/service to another third-party service or use of "Cloud" services other than those made available to the University under the Microsoft campus licence agreement.

6.5.3. Passwords and other forms of secure authentication

University Password guidance establishes requirements for the creation and use of strong passwords, the protection of passwords and frequency of change. Authorised Users are required to follow the standards and instructions set out therein, and where required to use other forms of secure authentication that the University may reasonably require. Those guidelines apply across **all** University passwords, which include 'Administrator' passwords (see below) and 'User' passwords.

In some instances, authorised users will have access to administrative services for the performance of specific tasks. Administrative services are only to be used, by exception, to perform a specific task that could not otherwise be undertaken; once completed use of the administrative service is to immediately cease for the

avoidance of doubt an administrative service must not be activated/remain active in case use is required.

6.5.4. Electronic mail and messaging policy

The University Electronic Mail and Messaging Policy recognises electronic mail as a formal business communications tool at the University and the business requirement to manage electronic mail messages as University records within clearly defined conditions. This Policy clarifies how University electronic mail and messaging systems should be used to support institutional requirements including those necessary to meet legislative obligations. Authorised Users are required to follow the standards and instructions set out in this Policy and should refer to this for additional information on the use and management of electronic mail.

6.5.5. Intellectual property

No *Authorised User* of the ICT facilities is permitted to store, copy, reproduce, modify, disseminate (i.e. transfer) or use any material not generated by the Authorised User which may have intellectual property rights vested in them belonging to a third party, without either prior written permission from the owner of such intellectual property rights or having purchased the relevant rights to use the material in question.

6.5.6. Protection of the rights and freedoms of individuals

Use of ICT facilities should always be respectful to and uphold of the rights and freedoms of individuals. Use of ICT facilities to support the creation, storage or dissemination (transmission) of material which serves to harass, intimidate, threaten, offend or cause real harm is strictly prohibited. Authorised Users use of ICT facilities should also be consistent with the standards and instruction set-out within the University Policy concerning all aspects of equality and diversity (see Section 4.3).

6.5.7. Miscellaneous

For the avoidance of doubt the following actions are strictly prohibited:

a. Causing damage either recklessly or deliberately (including destruction) to any part of the ICT facilities and/or to materials belonging to other Authorised Users whether as a result of Authorised Use or otherwise;
b. Intentionally seeking to degrade the performance of any of the ICT facilities;
c. Depriving either recklessly or deliberately other Authorised User(s) of ICT facilities – this includes denying access where others require to undertake activities as described in section 6.2 with the exception of activities falling within the scope of Personal Use as defined by these Regulations (see section 6.4);
d. Gaining unauthorised access to ICT facilities by whatever means including the use of another Authorised User's authentication credentials;
e. Disclosing the details of a University password to any third-party - passwords are confidential and are non-transferable.
f. Unauthorised monitoring of the use of ICT facilities and any communications;
g. Installation (including unauthorised connection) or use of hardware or software on the University's *ICT facilities* other than that formally approved by the University (i.e. through procurement and information security Policy, Procedures and Regulation etc.);
h. Decommissioning and/or removal of hardware or software from the University's ICT facilities outwith approved University procedures;

i. Use of ICT facilities for business/commercial activities which do not have the prior approval of the University or the University Court.

6.6. Guidance

Where there is any doubt as to what constitutes acceptable or non-acceptable use or where non-acceptable use conflicts or appears to conflict with a valid business requirement, persons should seek advice in the first instance from the IT Service Desk. For issues related to academic use and/or research discussions should take place with the appropriate Head of School.

7. Waiver of liability

The University does not accept any liability whatsoever in respect of any loss, damage, injury, offence, costs or expenses, penalties or other impositions alleged to have been caused to Authorised Users or unauthorised users as a result of use of the ICT Facilities. This will include any loss of all information and/or services of which the individuals may privately store on ICT facilities e.g. family photographs, contact details. Furthermore, the University does not accept any liability whatsoever in respect of any loss, damage, injury to third parties or expenses or costs alleged to have been caused to Authorised Users or unauthorised users by reason of defect in any apparatus or as a result of failure of software or hardware comprising part of the ICT Facilities.

8. Withdrawal of ICT facilities

ICT facilities will be withdrawn when:

- An individual no longer meets the definition of an Authorised User as defined by these Regulations (see Section 3 of these Regulations); and
- A credible threat to the availability of ICT facilities is believed or has been found to exist, e.g. an Authorised User's ICT account has become compromised by a malicious third party/cyber-attack.

The University will provide advance notice to students and other learners associated with the institution of the withdrawal of ICT facilities, other than where the student or learner has not completed their programme or course of study.

ICT facilities may be withdrawn when:

- An Authorised User is under investigation where it is suspected that they have breeched any condition(s) of these Regulations and/or of any other relevant legislation, University Policy, Regulation or relevant instrument herein;
- It has been found that a breach of these Regulations has occurred (see Section 15); or
- Withdrawal is deemed necessary to protect the University's legitimate interests.

9. Monitoring, interception and disclosure

The University will monitor the use of ICT facilities in accordance with legislation, these Regulations, the University Information Security Policy and relevant sub-policies. The purpose of this monitoring is to:

- Help ensure the continued effective system operation i.e. that ICT facilities are available for the benefit of all Authorised Users, without any undue interruption, including supporting proactive and reactive information security measures allied with detecting and/or guarding, against any external malicious interference, or to support the University's efforts when recovering from an interruption to services;

- To establish the existence of facts and to ascertain compliance with these Regulations and all other relevant legislation and instruments (i.e. University Policy and Regulation etc.) referred to herein; and
- To prevent or detect crime.

Information including network session connection times, Internet use (services accessed), network traffic (flow and volume), disk utilisation, electronic mail storage (volume) is collected and monitored. Information on telephone, printing and photocopying usage is also collected and monitored (i.e. itemised bills: basic call details). The University will comply with all relevant legislative requirements applicable to monitoring and logging activities.

Monitoring, interception and disclosure will be subject to approved University procedures, for which the University Vice-Principal Governance has responsibility.

9.1. Filtering and interception of Internet traffic

The University uses reserves the right to make use of automated Web (Internet) filtering facilities to block Websites (and related content) which the University believes are incompatible with the conditions of Authorised Use and by extension these Regulations. The University also reserves the right to make use of all relevant system/service logs to take all reasonable steps to identify, prevent and/or recover from any credible threat to the availability of ICT systems/services, information, data and personal data.

9.2. Disclosure of personal information

The University will disclose personal information in this regard when required to do so by law, and at all times will abide by its Data Protection Policy and allied procedures.

The University may also disclose personal data, which could include internet protocol addresses and cookie identifiers from system/service logs to third parties for the purposes of the detection and prevention of crime, and/or to undertake proactive and retrospective analysis of the operation of a system or a service, with a third party, e.g. a contractor, notably to maintain the availability of ICT facilities and services.

10. Responsibilities

Access to and use of the Facilities requires Authorised Users to accept responsibility to use the ICT facilities in accordance with the Regulations and the instruments referred to herein. Other specific responsibilities include:

- Authorised Users must report any actual or suspected breach of these Regulations (see Section 13 of these Regulations);
- Authorised Users are individually and exclusively responsible for the use of ICT facilities made available to them through the access Authentication Credentials (see Section 5.1 of these Regulations) issued;
- Authorised Users must report the suspected or actual loss and/or compromise of ICT facilities made available to them at the earliest opportunity (see Section 14 of these Regulations); and
- Any Authorised User wishing to use any of ICT facilities (as defined herein) for any purpose not permitted by these Regulations must first obtain the written agreement of the University Chief Information Officer who has the responsibility for determining such applications and any necessary resulting charges in the light of the current policies of the University or where appropriate to secure written agreement of the relevant Head of School.

11. Methodology

These Regulations were partly informed by external benchmarking. This included a review of exemplar policies and regulations from Scottish and English universities. On conducting an

equality impact assessment no equality or diversity issues were identified as likely to arise through implementation of these Regulations.

12. Review

These Regulations will be reviewed at regular intervals. The review period will be approved by the University and recorded on the accompanying coversheet for the Regulations. Any significant change to relevant legislation, University Policy or procedures primarily concerned with information *confidentiality, integrity and accessibility* may trigger an earlier review. These Regulations will be presented to the University for approval.

13. Reporting breaches

In the first instance any suspicion of a breach of these Regulations should be reported to the University IT Service Desk. If a suspected or actual breach has occurred the University Chief Information Officer may sanction the withdrawal of access to ICT Facilities (See Sections 8 and 15 of these Regulations).

14. Loss of and/or compromise of ICT facilities

The suspected or actual loss and/or compromise of ICT facilities made available to Authorised Users via IT Services should be reported to the IT Service Desk at the earliest practical opportunity. The loss of ICT facilities made available via Schools and Services should be reported to the appropriate Head of School or Service, or their nominee. The theft of ICT facilities should be reported to the University's Security Service team.

15. Sanctions

Failure of an Authorised User to comply with these Regulations may result in access to University ICT facilities being denied (either on a temporary or permanent basis), and/or disciplinary action being taken depending on the severity of the breach under the University's disciplinary procedures (as applicable). Where contractual terms have been broken the University will review its position with that party. This could lead to termination of a contract of employment, studies, research or the provision of goods/services. Where it is believed that a criminal action has occurred, the University will also report this to law enforcement agencies. The University also reserves the right to advise third parties of any infringements of their rights, and to pursue civil damages against any party.

Where a serious breach of the data protection legislation has occurred i.e. where a substantial loss of, or unauthorised access to personal information has occurred (volume or sensitivity) - where the potential harm to individuals has become an overriding consideration, then the University Data Protection Officer assess whether the University is required by law to provide notification to the UK Information Commissioner.

16. Interpretation of these Regulations

The University Vice-Principal, Governance (or as required their nominee) shall be the sole arbiter of these Regulations as to their meaning and application.

17. Availability

These Regulations will be published on the University Website. They can be made available in different formats, please direct any requests to the University Chief Information Officer.

18. Contacts/further information

Enquiries regarding these Regulations can in the first instance be directed to the University Head of Information Assurance and Governance.

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.0	Approved (Principal's Office)	Approved	C Milne, Associate Chief Information Officer Information Assurance and Governance, IT Services	May-2012
1.1	Minor changes (typographical corrections and removal of reference to FATMAN network)	Approved	C Milne, Associate Chief Information Officer Information Assurance and Governance, IT Services	13 Aug 2015
1.2	Minor revisions made to align Regulations with requirements placed upon the higher education sector through the Prevent strategy Presented to University ICT Strategy & Planning Group (paper ICT/15/07)	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	27 Nov 2017
1.3	Minor revisions made: • References to secure information handling i.e. Information Classification added; • IP addresses and cookie information being personal data and the circumstances where those data can be used and/or transferred to a third party added; • Future proofing for known elements of revised data protection law;	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	03 Jan 2018

	• Prevention and recovery methods from suspected or actual information security incident; and • Requirement to prevent people from being drawn into terrorism restated.			
1.4	Minor changes made.	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	12 Dec 2019