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	29/04/2012
Review / Expiry date	28/10/2023
Approved date	27/10/2022
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
EDI review/Equality impact assessment	None
Key terms	Information technology
Purpose	To communicate the conditions of access to ICT facilities 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**
4.0	Republished following annual review – no changes made	Approved	C Milne, Head of Information Assurance and Governance	27 October 2022

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 by the University.

These Regulations are intended to support:

- 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; and
- 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 use within and outside the University, and includes use during travel and access of ICT facilities for remote teaching, learning and assessment.

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 recognised and approved business process.

3.2. Information and Communication Technologies (ICT) facilities

Shall mean:

- The University's (or any entity thereof) ICT facilities and services (i.e. under direct ownership or licence agreement where the University is a party) - including but not limited to:

    - Infrastructure
        - The University network (fixed and wireless)
        - Virtual Private Network
    - Platforms
        - Cloud computing services for which the University has a licence/contract to provide use e.g. Office 365, Microsoft Teams
        - Management Information Systems e.g. SITS (student record system)
        - Virtual learning environments e.g. Moodle, MMS
    - Hardware (fixed and mobile devices)
        - PCs
        - Laptops
        - Smartphones
    - Software and Apps (mobile applications)
        - Microsoft Office

- ICT facilities provided by the University to Authorised Users through third party providers – including but not necessarily limited to:

    - All of the items listed above;
    - External infrastructure including JANET, Eduroam and other or successor networks and systems such as the Internet accessed by means of the University's IT systems; and
    - Copyright materials procured under contract or licence, e.g. electronic journals, books and data-sets, e-learning materials.

3.3. Authorised use

Shall be use consistent with:

- The University's public tasks (teaching, learning, research etc.), values and objectives.
- 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/the use of personal data

The terms Processing and Personal Data shall take the same meaning as that set out in the General Data Protection Regulation ("the GDPR").

4. Legislative and regulatory framework

Use of University ICT facilities is subject to (1) applicable legislation from a number of jurisdictions (2) external regulation governing the use of UK academic computing and communication facilities and (3) 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. Notable legislation and regulatory items are listed here to illustrate the range of conditions under which University ICT facilities should be used and managed.

The following list of relevant legislative and regulatory items comprises the principal areas of applicable legislation. 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

- The Abusive Behaviour and Sexual Harm (Scotland) Act 2016
- Computer Misuse Act (1990)
- Copyright, Designs and Patents Act (1998)
- The Data Protection Act (2018)
- Human Rights Act (2000)
- 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 shall not be read in isolation. Other University policies, regulations and procedures 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, should also be consulted where appropriate. Examples include:

- Data protection policy;
- Information classification policy;
- Access to information during periods of staff absence;
- Recording of lectures and other learning and teaching activities (‘lecture capture’);
- Disciplinary procedures (student and staff);
- Harassment and bullying at work and study policy;
- Guidelines on Recording of Meetings involving University Staff and Students;
- Equality and diversity policy, and polices for the protection of protected characteristics; and
- Recording of lectures and other learning and teaching activities (‘lecture capture’)

5. Access to ICT facilities

All Authorised Users of the ICT facilities must comply with these Regulations and as applicable 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.

[1] Available online: https://community.jisc.ac.uk/library/acceptable-use-policy, accessed 31 March 2020

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.

Authorised users may connect to ICT facilities provided by or through the University from their own devices, where those follow University policy and guidelines for connecting to the University network. Where individuals connect from home the router used must have a different password than that set y default by the supplier, as some router usernames and passwords are commonly available on the internet, which may create a vulnerability if exploited.

5.1. Authentication credentials

Access to ICT facilities is normally controlled, i.e. authenticated, via username and password. The University may require that Multi Factor Authentication ("MFA") is also used. 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 confidentiality of all authentication credentials issued to, or established by them (i.e. a password change) – in particular their nondisclosure or release in any form to any individual – other than approved services i.e. password managers provided by internet browsers;
- 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. 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 or where that is not possible logging off from a device and/or service; and
- May be held liable by the University for misuse of ICT facilities (or other associated actions) where (1) the Authorised User has failed to take all reasonable precautions to maintain the confidentiality of authentication credentials issued to them and/or (2) where the authentication credentials have not been applied to secure ICT facilities from unauthorised use by a third party.

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);
- Use of ICT facilities should always be legal and reflect the values of the University;
- Authorised Users must accept the need, as and when it may arise, 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;
- 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 should also accept that use of ICT facilities may be monitored under specific conditions defined by law (see Section 9).

6.2. Acceptable use

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; and
- 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 includes but is not 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; and
- 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, as set out below. 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:

- Compromises or reduces or adversely effects the capacity of the Authorised User to carry out their work related duties;
- 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 use unless formally approved by the University; and
- Would breach these Regulations.

Personal use of ICT facilities outwith that deemed reasonable by the University may constitute a breach of these Regulations (see Section 15) and result in sanctions being imposed.

6.5. Specific requirements and prohibitions

It is beyond the scope of these Regulations to provide an exhaustive list of all possible prohibitions concerning the acceptable use of ICT facilities provided by or through the University. A number of selected areas are highlighted here.

6.5.1. Information security and information handling

Use of ICT facilities by Authorised Users must always be consistent with maintaining and preserving the confidentiality, integrity and availability of University data, personal data, information and information systems. Use of ICT facilities must be consistent with the guidance issued by IT Services from time-to-time, such as guidance on strong password creation and use and those for safe information handling set out in the University Information Classification Policy and the supporting implementation guidelines.

6.5.2. Data protection and using approved ICT services

No Authorised User shall use the ICT facilities (as defined herein) to hold or process personal data except in accordance with the provisions of The GDPR when read with the Data Protection Act 2018; where the use of personal data is purely for personal or household activities then the provisions of the legislation will not apply.

Authorised Users should refer to the University Data Protection policy, University Policy and guidelines on information classification and handling and to specific privacy 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 proactively take steps to ensure that ICT 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 (privacy) rights and freedoms of individuals. In that regard, the University before engaging with an ICT service provider is required by law to carry out due diligence to ensure that personal data for which it is responsible, can be made available to a third party (supplier/service) without undue risk. Legislation also mandates the contractual terms which must be enforceable and in place between the parties, to establish responsibilities and protect personal data.

Therefore, no Authorised User should transfer personal data to ICT facilities and/or services, nor procure such services, which have not been first approved by the University. Examples of such prohibitions would include the forwarding of emails used to conduct University business 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. The exclusion does not include personal/home devices used by Authorised Users or internet service providers used to connect to the ICT Facilities provided by or through the University.

The University Information Assurance and Governance function (dataprot@st-andrews.ac.uk) will provide support, and will undertake due diligence where approval for a new ICT service provider is required.

6.5.3. Passwords and other forms of secure authentication

University Password guidance establishes requirements for the creation and use of strong passwords. Authorised Users must follow the standards and instructions set out therein.

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.

Where required Authorised Users must use other forms of secure authentication that the University may reasonably require.

6.5.4. 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.

6.5.5. Protection of the rights and freedoms of individuals

Use of ICT facilities should always be respectful to and uphold the rights and freedoms of individuals. Use of ICT facilities to support the creation, storage or dissemination (transmission) of material which has the effect of harassing, intimidating, threatening, offending or causing real harm is strictly prohibited. Similarly, the tone of communications should be measured – aggressive behaviour is not acceptable. Authorised Users use of ICT facilities should also act within the standards and instruction set out within the University Policy concerning all aspects of equality and diversity (see Section 4.3).

6.5.6. Miscellaneous

The following actions are also strictly prohibited:

a. Causing damage either recklessly or deliberately wither intentionally or otherwise to any part of the ICT facilities and/or to content belonging to other Authorised Users whether as a result of Authorised Use or otherwise;
b. Degrading 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 other than approved services for the management of such credentials - passwords are confidential and are non-transferable;
f. Unauthorised 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.);
g. Unauthorised decommissioning and/or removal of hardware or software from the University's ICT; and
h. Retention of ICT facilities following the termination of employment or engagement with the University, unless formally authorised by the University.

6.6. Guidance

Where there is any doubt as to what constitutes acceptable or non-acceptable use or where it is believed that non-acceptable use conflicts or appears to conflict with a valid business requirement, persons should seek advice in the first instance from the University Head of Information Assurance and Governance (dataprot@st-andrews.ac.uk).

7. Waiver of liability

The University does not accept any liability whatsoever in respect of any loss, damage, injury, fines, offences, costs or expenses, penalties or other liability arising alleged to have been caused to Authorised Users as a result of use of the ICT Facilities. This includes any loss of information and/or services which Authorised Users may privately store on ICT facilities e.g. family photographs, contact details. 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);
- A credible threat to the 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; or
- Withdrawal is deemed necessary to protect the University's legitimate interests.

The University will provide as much advance notice to students and other learners associated with the institution of the withdrawal of ICT facilities.

ICT facilities may be withdrawn when:

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

9. Monitoring, interception and disclosure

The University will monitor and as appropriate log the use of ICT facilities in accordance with applicable legislation, these Regulations, the University Information Security Policy. The purpose of this monitoring is to:

- Facilitate 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 University Policy; 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 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 relevant policies and 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, 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 these Regulations. 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 for any purpose not permitted by these Regulations must first obtain the written agreement of the University Head of Information Assurance and Governance, who may also liaise with the University Chief Information Officer over any resulting cost implications in the light of the current policies of the University or where appropriate to secure written agreement of the relevant Head of School or Service Director.

11. Methodology

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

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 or personal data

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 or the IT Services CSIRT Team (csirt@st-andrews.ac.uk) 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 or loss of ICT facilities should be reported to the University's Security Service team.

Where it is suspected that personal data have become lost, stolen and/or compromised then the IT Service Desk and/or the University Data Protection Officer must be advised (dataprot@st-andrews.ac.uk). Where a personal data breach has occurred the University is under a legal obligation to log such incidents and where appropriate to report those to the UK Information Commissioner. Reporting the suspected or actual loss of personal data timeously is of significant importance; this can aid the University to promptly recover and/or contain a loss, thereby preventing or minimising harm to others.

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 arrangements under which access to ICT facilities are provided, 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.

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 Head of Information Assurance and Governance.

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, IT Services	May-2012
1.1	Minor changes (typographical	Approved	C Milne, Associate Chief Information	17-Oct-2014

	corrections and removal of reference to FATMAN network)		Officer Information Assurance & Governance	
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, Associate Chief Information Officer Information, IT Services	13-Aug-2015
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; • Prevention and recovery methods from suspected or actual information security incident; and Requirement to prevent people from being drawn into terrorism restated.	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	27-Nov-2017
1.3	Approved (Vice Principal, Governance)	Approved	C Milne, Head of Information Assurance and	03-January-2018

			governance, Office of the Principal	
1.4	Wording on the use of administrative passwords added (minor update).	Approved	C Milne, Head of Information Assurance and governance, Office of the Principal	12-December-2018
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, Office of the Principal	14-February-2019
2.0	Periodic review	Approved	C Milne, Head of Information Assurance and governance, Office of the Principal	April 2020
2.1	Section 6.5.5 updated: sending of emails that are aggressive in tone is a breach of these Regulations (Approved by University Information Compliance Group).	Approved	C Milne, Head of Information Assurance and Governance	06 November 2020
3.0	Annual review – minor updates made: MFA, reference to IT guidelines and router default passwords	Approved	C Milne, Head of Information Assurance and Governance	30 August 2021