Abertay University

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

Author	ICT Operations Manager
Approved by	Court
Approval date	2 November 2009
Review date	30 June 2015
Version	v1.1
Document type	Regulation
Document location	Abertay Knowledge/Information Governance and Security/Information Security
Linked documents	Information Security policy, Data Protection policy, Password policy, Electronic Mail and Messaging policy, Data Protection Act 1998, Freedom of Information (Scotland) Act 2002, Bullying and Harassment policy, Equality and Diversity policy

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.

These Regulations in part with other internal and external instruments provide a framework which describes conditions of access to and acceptable use of ICT facilities and services provided by the University or through third-parties with whom the University has engaged.

2. Purpose and scope

The purpose of this University Regulation is to provide a set of parameters which 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.

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. Consequently, these Regulations apply to all out of office (e.g. home) working.

3. Definitions

3.1. Authorised users

Are:

- Students and other learners associated with the institution 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 e.g. associate students.

3.2. Information and Communication Technologies (ICT) facilities

Information and Communication Technologies (ICT) facilities shall mean:

- The University's (or any entity thereof) Information Technology (IT) systems (i.e. under direct ownership) - including but not necessarily limited to:
  - Personal and mobile (i.e. laptop) computers;
  - All types of mobile communication devices including those capable of connecting to the Internet and other networks;
  - Telephones;
  - Network i.e. fixed and wireless;
  - Intranet i.e. the University Portal or successor service(s);
  - Electronic mail and other person-to-person or group communication services;
  - Virtual learning environments e.g. WebCT, Blackboard;
  - Software;
  - Hardware;
  - 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, FaTMAN, EduROAM (and other or successor networks and systems such as the Internet) by means of the University's IT systems;
  - 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;
- These Regulations;
- The terms of any licence agreement unless otherwise prohibited by the terms and conditions of another licence agreement.

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. 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 (1998)
- 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 (2008)
FATMAN Acceptable Use Policy (2009)

4.3. Relationship with existing University Policy 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 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), 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 (2009);
- Intellectual Property Policy (2007);
- Web Filtering Policy (2009);
- Dignity at work: dealing with personal harassment;
- Race equality policy for staff and students;
- Discipline procedure;
- Information Security Policy (2009);
- Electronic mail and Messaging Policy (2009);
- Password Policy (2009);

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.

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.

5. Access to ICT facilities

All Authorised Users of the ICT facilities must comply in full 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.

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. Credentials 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 the sole use of the Authorised User;
- Is responsible for taking all reasonable actions to maintain and preserve the integrity of all authentication credentials issued – 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 the legitimate Authorised user;
- May be held liable by the University for misuse of ICT facilities (or other associated actions) where the Authorised User has failed 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 and must also accept that such use may be monitored under specific conditions defined by law (see Section 9). 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.

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 (defined in Section 6.4 of these Regulations).

6.3. Non-acceptable use

An absolute definition of 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:

- Expose the University to legal and/or regulatory liability or reputational damage;
- Expose an Authorised User to legal and/or regulatory liability;
- Are abusive or threatening to others e.g. serves to harass, bully, discriminate or incite discrimination;

- Are designed or likely to result in the degradation, loss, damage or destruction of ICT facilities and allied services;
- Threaten the preservation and/or maintenance of the confidentiality, integrity and availability of 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;
- Is connected with private commercial business.

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

The University **Information Security Policy** 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 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)

The University **Data Protection Policy** sets how the University will fully comply with that Act in upholding the data protection principles. No Authorised User shall use the ICT facilities to hold or process personal information (as defined by Section 1 of the Data Protection Act 1998) except in accordance with the provisions of that Act.

Authorised Users should refer to the University Data Protection Policy and to specific fair collection notices issued by the University for further information on the manner in which their personal information will be collected and processed.

6.5.3. Passwords

The University **Password Policy** 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 in this Policy.

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 annoy, 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 e.g.:

- **Bullying and Harassment policy**;
- **Equality and Diversity policy**.

6.5.7. Miscellaneous

The following actions are strictly prohibited:

a) Causing damage (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 other Authorised User(s) of ICT facilities;
d) Gaining unauthorised access to ICT facilities by whatever means including the use of another Authorised User's authentication credentials;
e) Unauthorised monitoring of the use of ICT facilities and any communications;
f) 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) Decommissioning and/or removal of hardware or software from the University's ICT facilities outwith approved University procedures;
h) Use of ICT facilities for business/commercial activities which do not have the prior approval of the University.

6.6. Guidance

Where there is any doubt as to what constitutes acceptable or non-acceptable use persons should seek advice in the first instance from the Service Desk (Information Services). 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. 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).

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 breached 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 14).

9. Monitoring, interception and disclosure

The University will monitor the use of ICT facilities in accordance with 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;
- To establish the existence of facts and to ascertain compliance with these Regulations and all other relevant legislation and instruments herein;
- 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 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. This includes but not necessarily be restricted to the **Data Protection Act 1998** and the **Freedom of Information (Scotland) Act 2002**.

Monitoring, interception and disclosure will be subject to approved University procedures, for which the University Chief Information Officer has responsibility.

9.1. Filtering and interception of Internet traffic

The University uses 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.

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.

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;
- 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 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 and where appropriate the advice of the relevant Head of School or Service.

11. Methodology

These Regulations were partly informed by external benchmarking. This included a review of exemplar policies and regulations from Scottish and English universities. These Regulations build on a previous set which were approved by the University Court in February 2009. 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 Court 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 Court for approval.

13. Reporting breaches

In the first instance any suspicion of a breach of these Regulations should be reported to the University's Service Desk (Information Services). 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 14 of these Regulations).

14. 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 Student Disciplinary Code or Staff 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, or 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 Act 1998 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 Controller will report the matter to the UK Information Commissioner.

15. Availability

These Regulations will be published on the University Portal. They can be made available in different formats, please direct any requests to the University Service Desk (Information Services).

16. Contacts/further information

Enquiries regarding these Regulations can in the first instance be directed to the Head of Information Services.

Version control table

Version number	Purpose/change	Author	Date
v1.0	Policy approved by FPG&C (Oct 09) and then Court	C. Milne, Information Manager	2 Nov 2009
v1.1	Minor editorial changes made	F. Caldwell, Policy Officer	22 Oct 2014