ICT Acceptable Use Policy

Effective from 13 January 2014

Version Number: 4.0

Author: Senior Information Security Officer
Governance Services Unit
Document Control Information

Status and reason for development

Status: Revised version of ICT Acceptable Use Policy V3.2

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Summary of changes</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xx Dec 2013</td>
<td>Christa Price</td>
<td>General review and amendments including requirements for software requests and IT equipment move requests to be submitted to ITS. Inclusion of ITSERT ToR.</td>
<td>V4.0Draft</td>
</tr>
<tr>
<td>30 August 2012</td>
<td>Matthew Trump</td>
<td>Change to section 5.2.18 permitting use of p2p without requiring written permission of CIO.</td>
<td>V3.2</td>
</tr>
<tr>
<td>30 August 2011</td>
<td>Christa Price</td>
<td>General review from version 1 (2007), and included alumni use of Email for Life</td>
<td>V3.0</td>
</tr>
</tbody>
</table>

Policy Management and Responsibilities

Owner: This Policy is issued by the Executive Director of ITS, (Chief Information Officer (CIO)) and the University Secretary. The CIO has the authority to issue and communicate policy on University ICT facilities, services and usage. The University Secretary responsibilities include Information Governance functions within GSU.

Others with responsibilities (please specify): All subjects of the Policy will be responsible for engaging with and adhering to this policy.

Assessment

<table>
<thead>
<tr>
<th>Equality Analysis</th>
<th>Legal</th>
<th>Information Governance</th>
<th>Academic Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

Consultation

<table>
<thead>
<tr>
<th>Staff Trades Unions via HR</th>
<th>Students via USSU</th>
<th>Any relevant external bodies (please specify)</th>
</tr>
</thead>
<tbody>
<tr>
<td>□</td>
<td>□</td>
<td>..................................................</td>
</tr>
</tbody>
</table>

Authorised by: University Secretary & ITS Executive Director (CIO)

Date authorised: 17/12/2013

Effective from: 13/01/2014

Review due: 2 years by January 2016

Document location: University Policy & Procedure Pages

http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

Document dissemination and communications plan

US Online, Talk time Leadership Update, Student Channel.
1.0 Purpose
The purpose of this document is to specify the University of Salford (the University) policy on the acceptable (and prohibited) use of its information and communications technology (ICT) facilities and sanctions for non-compliance. The policy addresses the need to protect the University and its Users’ data, balanced with the need to protect the rights of the students, staff, alumni and associates.

2.0 Scope
2.1 The University of Salford’s Information Communications Technology (ICT) facilities are provided by the IT Services Division (ITS) and are made available primarily for the purposes of the University’s business. The ICT Acceptable Use Policy (AUP) is a set of rules that applies to all authorised Users of the University’s ICT facilities encompassing; students, alumni, staff and associates of the University. This policy does not form part of the contract of employment or student contract and can therefore be amended without Users’ consent.

2.2 ICT facilities encompass (but are not restricted to) the following services provided by the University of Salford and third parties on its behalf:

a. network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers;

b. network services, including (but not exclusively) Internet access, web services, email, wireless, messaging, shared filestore, printing, telephony and fax services, CCTV, door and car park access control;

c. university owned or leased computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, tablets, PDAs, mobile devices, smartphones, servers, printers, scanners, disc drives, monitors, keyboards and pointing devices;

d. software and databases, including applications and information systems, virtual learning and videoconferencing environments, ICT laboratories, software tools, information services, electronic journals & e-books.

2.3 The ICT facilities available will vary per user group, some users will only be entitled to use some limited facilities.

2.4 The University may make changes to the Policy at any time. Users will be notified of the changes.

3.0 Policy Statements
Any individual using the ICT facilities is deemed to have accepted this Policy and is bound by it.

ICT facilities are provided to Users primarily for University business purposes to support teaching, learning, research and professional & administrative activities. In addition, occasional and limited personal use of the facilities by staff and students is allowed. The University’s business purposes (primary purpose) of ICT facilities take priority over any personal use.

Email for Life accounts are made available after alumni have left the University to foster stronger links between the University and alumni, and to promote and facilitate communication between alumni and the University.

3.1 Acceptable Use
All users of the ICT facilities must comply with the following principles:

3.1.1 The University expects Users to use the ICT facilities and access to the Internet in a responsible manner in accordance with this policy and all applicable laws in the United Kingdom. If Users are in any doubt about what constitutes acceptable use, they should
seek the advice and guidance from their Line Manager, Programme Leader, University Sponsor or the ITS Service Desk;

3.1.2 Users must also comply with the regulations and policies that are applied by bodies external to the University in respect of the ICT facilities, including but not restricted to JANET (Joint Academic Network) and (in respect of student and alumni email accounts) Microsoft Corporation;

3.1.3 Only valid and authorised Users are permitted to use the ICT facilities. Each user is issued with a valid username and password that must be kept confidential and must not be shared with anyone else;

3.1.4 All Users are responsible for all activity that takes place under their usernames and must not allow anyone else to access the ICT facilities using their usernames and passwords. Access to the ICT facilities using someone else’s user name and password is prohibited;

3.1.5 All Users should be courteous and considerate of others when using the ICT facilities;

3.1.6 (In the case of staff and students) utilise the University provided email accounts as the primary mechanism for email communication with the University. For programmes of study, the Blackboard / Virtual Learning Environment is the alternative University provided communication mechanism;

3.1.7 (In the case of staff and students) ensure academic work requiring access to prohibited internet material (as described in Prohibited Activity) is only carried out following formal authorisation of the Extraordinary Internet access form (App 6);

3.1.8 (In the case of all Users) ensure personal use is occasional, reasonable and ensure personal use is compatible with and does not contravene the primary purpose of the facilities; interfere with, conflict with or take priority over the performance of University duties; waste resources; deny or impair the service to other users or have a negative impact on the University or other users; and when using social media;

a. be mindful of and safeguard the University’s reputation
b. comply with University Policy, particularly protecting sensitive or confidential information or material protected by copyright law
c. be mindful of the permanent record and electronic footprint a user makes available on the internet through using social media

3.1.9 (In the case of staff) an individual’s work communications and/or filestore may need to be accessed during his/her absence. Any such access will only be granted in accordance with the ITS Third Party IT Access Form (Appendix 5) and will supersede personal use;

3.1.10 Have appropriate authorisation and technical protection before sending or transmitting University confidential information external to the University data communications network (See Related Documentation)

3.1.11 Utilise good information security and management practices for the storage, access, retention and deletion of University information; (See Related Documentation)

3.1.12 Comply with all relevant copyright legislation, licences and agreements for software and electronic information resources when accessing and connecting to University ICT facilities;

3.1.13 Obtain authorisation for purchasing / obtaining software licences and for installing software on University owned computers from IT Services (via the ITS Service Desk);

3.1.14 (In the case of staff) where there is a requirement to move desktop computing equipment from one location to another, they must submit a moves request to the ITS Service Desk for authorisation and action. This will enable IT Services to maintain an accurate and up to date corporate asset register and ensure that the equipment is working correctly after the move is completed;

3.1.15 Users should make all reasonable efforts to send data that is ‘virus free’ and not open email attachments or click on links sent by unsolicited or untrusted sources;
3.1.16 Users should ensure any personally owned computer (with appropriate authorisation from IT Services) used to access University ICT facilities (and the University connection to the national Joint Academic Network (JANET)) have regularly updated operating systems & anti-virus programs thereby protecting the University network as much as possible from accidental or premeditated virus and hacking attempts and attacks;

3.1.17 All University systems owners must ensure that their information systems and supporting infrastructure comply with ITS Policy and current legislation;

3.1.18 Users acknowledge that the University does not endorse any third party goods or services and is not responsible for any goods or services that are accessible via third party websites. This includes (but is not limited to) all services that Microsoft makes available to users of its email accounts;

3.1.19 Users will be solely responsible for all claims, liabilities, damages, costs and expenses suffered or incurred by the University which result from their use of the ICT facilities in contravention of this Policy;

3.1.20 Users should report any technical problems, requests or concerns regarding a suspected policy breach directly to the ITS Service Desk

3.2 Prohibited ICT Activity
Users may not use University ICT facilities to:

3.2.1 cause the good name & reputation of the University or any part of it to be damaged or undermined by carrying out, facilitating or furthering inappropriate, criminal or any other activity that conflicts with all applicable laws in the United Kingdom and / or University policy or regulations;

3.2.2 contravene regulations and policies applied by bodies external to the University in respect of the ICT facilities, including but not restricted to JANET (Joint Academic Network) and (in respect of student and alumni email accounts) Microsoft Corporation;

3.2.3 carry out any personal business, gambling or non University related commercial purpose;

3.2.4 obtain unauthorised commercial gain;

3.2.5 commit the University via means of email to a contract (except for staff who are expressly authorised to do so using university purchasing procedures);

3.2.6 carry out activities of a nature that compete with the University in business;

3.2.7 sell or redistribute any part of the ICT facilities

3.2.8 carry out activities that conflict with an employee’s obligations to the University as their employer;

3.2.9 continue to use any item of networked hardware or software after a designated ITS authority has requested that use ceases because of its causing disruption to the correct functioning of the University ICT facilities, or for any other instance of unacceptable use;

3.2.10 carry out activities that unreasonably waste staff effort or network resources or activities that unreasonably serve to deny ICT facilities to authorised users;

3.2.11 deliberately or unintentionally receive, access, create, change, store, download, upload, share, use or transmit:

i. any illegal, obscene or indecent images, data or other material, or any data capable of being resolved into such material (other than in the course of properly supervised, lawful and authorised research);

ii. any infected material or malicious code (including, but not restricted to, computer viruses, spyware, trojan horses and worms) whether designed specifically or not, to be destructive to the correct functioning of computer systems, software, networks,
data storage and others’ data, or attempt to circumvent any precautions taken or prescribed to prevent such damage;

iii. any material which discriminates or encourages discrimination on any grounds;

iv. any material which the University may deem to be advocating illegal activity, threatening, harassing, defamatory, bullying or disparaging of others, abusive, libellous, slanderous, indecent, obscene, offensive or otherwise causing annoyance, inconvenience or needless anxiety;

v. any material that infringes the copyright or confidentiality of another person or institution, or infringes the Copyright laws of the UK and/or other countries (including but not exclusive to music, films, radio and TV);

3.2.12 place links to websites which have links to, or display, pornographic and inappropriate material, or which facilitate illegal or improper use, or place links to bulletin boards which are likely to publish defamatory materials or discriminatory statements; or where copyright protected works such as computer software, films, games or music are unlawfully distributed;

3.2.13 falsify emails to make them appear to have been originated from someone else, or send anonymous messages without clear indication of the sender;

3.2.14 carry out activities that criticise or harm individuals or that violate the privacy of other individuals;

3.2.15 gain or attempt to gain unauthorised access to facilities or services via the University ICT facilities, using automated processes or otherwise

3.2.16 allow, incite, encourage or enable others to gain or attempt to gain unauthorised access to, or carry out unauthorised modification to the University’s or others’ ICT facilities;

3.2.17 deliberately or unintentionally attempt to circumvent the University’s security systems, or deliberately or unintentionally use file-sharing systems (sometimes known as P2P or peer-to-peer) to download or upload copyright material without the copyright owners permission (including but not limited to music, films, games, and software);

3.2.18 overload, change, damage, curtail, corrupt, disrupt, deny, modify, re-route, dismantle or destroy (or cause to be overloaded, changed, damaged, curtailed, corrupted, disrupted, denied, modified, re-routed, dismantled, or destroyed) any ICT facility, network component, equipment, software or data, or its functions or settings, which is the property of the University, its Users, visitors, suppliers or anyone else, without the express permission of the University’s Chief Information Officer;

3.2.19 connect any non approved or personally owned ICT equipment to the University physical (wired) network points (with the exception of PC’s and laptops in University Halls of Residence) without written authorisation of IT Services (via ITS Service Desk) and adequate protection in accordance with point 3.1.17;

3.2.20 intentionally or unintentionally transmit unsolicited or unauthorised commercial or advertising material within the University or to other individuals or organisations in contravention of the University privacy statement or use any portion of the ICT facilities as a destination linked from such material. Such material includes unsolicited e-mail (spam), chain letters, hoax virus warnings, pyramid letters or other junk mail of any kind;

3.2.21 make, use, install, possess, distribute, sell, hire or otherwise deal with any unauthorised copies of software for any purpose without the licence and permission of its owner;

3.2.22 install any software without authorisation of ITS Services (via ITS Service Desk)

3.2.23 transmit, distribute, discuss or otherwise disclose (on Message Boards, email or any other mechanism) any University owned or held confidential information (See Related Documentation).
3.3 Alumni Email for Life

The provision of an Email for Life account for each alumnus is at the discretion of the University’s Chief Information Officer and, where provided, is subject to the following:

- a. Email for Life is currently provided without charge to the University so is offered as a free service for alumni. If the University is charged in the future and has to pass on the cost to alumni, the University will notify alumni before fees are introduced and give them the option of paying the fees or closing their accounts.
- b. As the service is free it is provided without any warranties, conditions or promises of any kind and restrictions may apply.
- c. Email for Life accounts may be terminated immediately at any time without prior notice to alumni if the University believes or suspects that alumni have contravened this Policy in any way or that its ICT facilities have been or will be put at risk.
- d. Email for Life accounts may also be terminated if they have not been accessed for 90 or more days (or any shorter period which the University may notify to alumni).
- e. Email for Life accounts that are terminated will be immediately disabled and their contents will be irretrievably deleted on the date of termination. The University will not be held liable for any alleged loss of alumni data resulting from such deletion.

Alumni should ensure the Salford email address is not their sole email contact and should make back-up copies of data within their Email for Life accounts.

3.4 Responsibility of the University

The University provides the ICT facilities for the benefit of itself and its staff, students and alumni and no guarantee is given that use of the ICT facilities will be fault-free, uninterrupted and secure.

Users of the ICT facilities understand and agree that the University will not be liable to them for any loss connected with their use of the ICT facilities however that loss may arise including (but not limited to) loss that is caused by the University’s negligence. However, nothing in this paragraph excludes or limits the University’s liability for death or personal injury that is caused by its negligence or for fraud or fraudulent misrepresentation by the University.

4.0 Enforcement of the ICT Acceptable Use Policy

4.1 Monitoring

All email, internet use, telephone calls and other ICT usage is logged, and may be subject to automated monitoring. Monitoring may be carried out in compliance with applicable obligations under the Data Protection Act 1998 and where this is permitted under the Regulation of Investigatory Powers Act 2000 (and associated regulations) for the purposes of:

- a. preventing or detecting criminal activities
- b. investigating or detecting unauthorised use of the University’s ICT facilities
- c. ascertaining compliance with regulatory or self-regulatory practices or procedures and standards
- d. ensuring effective system operation.

Records of all ICT activity will be retained in accordance with the ICT retention schedule. Any monitoring will be proportionate to the assessed risk to University ICT infrastructure and information systems. Where investigations into named individual’s accounts are deemed necessary, the ITSERT Investigation Authorisation form (Appendix 2) must be completed and appropriately authorised. In the event of security vulnerability reports or copyright infringement notices, routine investigation of network activity logs will be carried out without recourse to the ITSERT Investigation Authorisation form.

Tools used to protect the University ICT infrastructure may include (but are not limited to) use of historical log/logging files, print audit software, filtering software to limit browsing of inappropriate sites and downloads, automatic checking of emails and attachments for viruses; blocking of some telephone
numbers and deletion of certain files and emails deemed appropriate by the University’s Chief Information Officer.

Monitoring may also take place, to facilitate, academic and pastoral care by ensuring that students not using electronic systems vital for study are identified and encouraged to do so and thereby not fall behind or drop out.

The University reserves the right to inspect any items of University owned or leased computer equipment connected to the network. Any ICT equipment connected to the University's network can be removed if it is deemed to be breaching policy or otherwise interfering with the operation of the network.

4.2 Incident reporting

Information security events and actual or suspected breaches of this policy should be reported immediately to the ITS Service Desk.

4.3 Misuse and Sanctions

Violations of this policy may be investigated by the IT Security Emergency Response Team (ITSERT), or relevant School or Division in line with the appropriate University disciplinary policy (See Appendices for ITSERT Terms of Reference). Where disciplinary action is initiated by a School or Division, that School or Division will be responsible for communications with the subject and should make it clear to the subject under which policy action is being taken. Sanctions for violations of the ICT AUP may include:

a. Suspension or withdrawal of University ICT facilities
b. Disconnection, seizure & inspection of any ICT equipment that is in violation of this policy
c. Reconnection fee
d. Initiation of disciplinary action in accordance with the applicable discipline policy. In the case of staff, this could lead to a disciplinary sanction including a summary dismissal. In the case of students, this could lead to a disciplinary sanction including expulsion from the University.

Where there is evidence of a criminal offence, the issue will be reported to the Police (or relevant statutory body) for their action. The University will co-operate with and disclose copies of any data stored, appropriate logs and any hardware used (relevant to the investigation) to the Police (or relevant statutory body) and other appropriate external agencies in the investigation of alleged offences, in line with current legislation.

5.0 Related Documentation

- Information Security Policy
- Data Protection Policy
- Network Security & Connection Policy
- Staff and Student Disciplinary Procedures
- Confidential Information Policy (in draft)

The University of Salford’s external network connection is governed by the Joint Academic Network (JANET) policies: [http://www.ja.net/development/legal-and-regulatory/policy/index.html](http://www.ja.net/development/legal-and-regulatory/policy/index.html)


Microsoft Service Agreement available at [http://explore.live.com/microsoft-serviceagreement](http://explore.live.com/microsoft-serviceagreement)
6.0 Appendices

- Appendix 1: ICT AUP Agreement (hard copy signature required by Human Resources when staff sign a new contract – held in personnel file).
- Appendix 2: ITSERT Terms of Reference
- Appendix 3: Student AUP Code of Practice (link under Information Technology) [http://www.salford.ac.uk/university/governance/policies-and-procedures](http://www.salford.ac.uk/university/governance/policies-and-procedures)
- Appendix 4: ITSERT Investigation Authorisation form (link on ITS Service Desk Top forms list) [http://www.its.salford.ac.uk/servicedesk/](http://www.its.salford.ac.uk/servicedesk/)
- Appendix 5: Third party IT access form (link on ITS Service Desk Top forms list) [http://www.its.salford.ac.uk/servicedesk/](http://www.its.salford.ac.uk/servicedesk/)
- Appendix 6: Extraordinary Internet Access form (link on ITS Service Desk Top forms list) [http://www.its.salford.ac.uk/servicedesk/](http://www.its.salford.ac.uk/servicedesk/)
Appendix 1: ICT AUP Agreement

Please sign the below agreement and return the signed page to University of Salford Human Resources Division. Please retain a copy of the policy for your future reference.

I confirm that I have read, understood and agree to abide by the attached ICT Acceptable Use Policy V 4.0 specifying my responsibilities when using University of Salford ICT facilities. I will keep the copy of the ICT Acceptable Use Policy for my personal reference.

Name (in capitals):

Signature:          Date:

Appendix 2: ITSERT Terms of Reference V 3.0

1. Membership
The IT Security Emergency Response Team (ITSERT) consists of staff within IT Services and the Governance Services Unit, including but not limited to; Associate Director Operations, Network Manager, Senior Information Security Officer and other staff as relevant.

2. Responsibilities
The ITSERT is delegated by the University Secretary and the Chief Information Officer to have responsibility and authority to do the following:

a) be the University focal point for reporting and managing the technical investigation of AUP and IT security incidents and breaches by
   a. requesting and investigating ICT activity logs
   b. blocking, disabling or enabling IT accounts, network connections and access
   c. disconnecting or confiscating computer equipment from the network. This may be carried out at the request of a School, Division, College with appropriate evidence
   d. drawing in necessary resources to support the investigation of IT security incidents (financial, people) according to the significance rating of an incident

b) act as gatekeeper to ensure that requested investigations are appropriate and justified and that it is not a disproportionate invasion of privacy

c) categorise (to assist allocation of resources) IT security incidents/AUP breaches with a Significance Rating, ranging from 1-3;
   1. severe illegal incidents that must be reported to law enforcement agencies i.e. child pornography or terrorism activity only
   2. serious incidents that impact on a number of other IT users or systems, that impact on University reputation or include staff misuse e.g. virus attack or highly offensive web activity
   3. routine regular breaches of the ICT Acceptable Use Policy e.g. copyright infringement, student inappropriate web activity

d) escalate Severe (Significance Rating 1) incidents to ITS Executive Director (nominated Associate Director in his absence), Vice Chancellor and University Secretary as appropriate and Greater Manchester Police (in no particular order of reporting) . ITSERT will manage Serious and Routine (Significance Rating 2 and 3) incidents and will escalate to ITS Executive Director if considered necessary (See Section 4). ITSERT will notify the relevant HR Business Partner of Serious incidents involving staff.

e) issue an annual ITSERT report

3. IT security incident types and reporting
IT Security incidents may include (but are not limited to): University IT Equipment theft; copyright infringements; DoS/hacking/portscans/probes/virus infection; Email abuse; Web activity/misuse/defacement; Log-in misuse/password sharing; Information/confidentiality compromise; Server registration/rogue devices/hardware issues issues; physical and environmental security affecting information assets
IT security events and actual or suspected breaches of the ICT Acceptable Use Policy should be reported immediately to the ITS Service Desk. Full information will be passed directly to the ITSERT and will not be recorded elsewhere.
All reports will be treated in the strictest confidence, sharing information only with individuals who need to be involved in the investigation. This may include the Chief Information Officer, University Secretary, investigating technical staff, relevant Human Resources or Governance Services staff as well as the relevant Head of School or Division. All information and investigation material will be stored securely in limited access electronic storage and/or locked cabinets.

4. ITSERT response to incidents

On receiving a report, if assessed as SEVERE (whether staff or student), the Chief Information Officer, University Secretary (and relevant senior management) will be informed. Any evidence obtained at this point will be passed to the relevant law enforcement agency.

Procedures for staff and students will differ according to the significance rating of the incident and individual factors. The below response procedures are intended to be generic and used as a guideline for handling and responding to the incident.

4.1 Student incidents

For routine incidents such as infringement notices, virus infections etc report is investigated, user identified, account disabled (via ITS Service Desk request). Onus is on student to make contact, ITSERT member to explain reason for block, remind about the ICT AUP, re-enable accounts and apply £100 AUP reconnection fee to student record.

For incidents rated as Serious, an ITSERT investigation authorisation form should generally be completed. The relevant Head of School and GSU staff will also be informed.

If an account disablement is requested by the School, a justification should be provided to ensure the request is proportionate. In these cases the School Ops Manager;

- will remain in charge of the incident
- is listed as the point of contact (not ITSERT)
- is responsible for requesting the account re-enablement via ITSERT
- is responsible for communicating with the student and explaining under what policy the School is taking action.

4.2 Staff incidents

For routine incidents, the report is investigated, account disabled and, where relevant, a technician may be allocated to clean/fix the IT equipment.

For serious incidents, the relevant Head of School/Division and HR staff will be informed (unless investigation has already been initiated by them) and advice obtained. The investigation should be passed to HR or Head of School/Division at this point. If the investigation is to continue, an ITSERT investigation authorisation form (ITS Service Desk top forms) must be completed justifying and authorising access into individual accounts.

5. Sanctions for violations of the Acceptable Use Policy

These may include:

- e. Suspension or withdrawal of University ICT facilities
- f. Disconnection & seizure of any ICT equipment that is in violation of this policy
- g. Reconnection fee for students (£100 as at August 2013)
- h. Initiation of relevant disciplinary procedure for staff or student. In the case of staff, this could lead to a disciplinary sanction including a summary dismissal. In the case of students, this could lead to a disciplinary sanction including expulsion from the University.