University of Salford MANCHESTER

ICT Acceptable Use Policy (AUP)

Version Number: 4.1

Effective from 17 December 2015

Author: Senior Information Security Officer &
Head of Information Governance
Legal, Planning & Governance
Directorate

Document Control Information

Status and reason for development

Revision of ICT AUP V4.0 to include rules on cloud computing for confidential University information, password complexity and Prevent duty.

Revision History

Date	*Author*	*Summary of changes*	*Version*	*Authorised*
Sep '15	C Price & M.Stephenson	Update re PREVENT statutory duty and organisational changes, password complexity, ref to ICT activity logs and Cloud services rules for confidential information	V4.1	Director LPG: 9/12/15 CIO: 13/11/15 Info&Tech Mgt Grp:30/09/15 Ops Board: 23/07/14
Jan '14	C Price	General review, software and IT equipment move requests. Inclusion of ITSERT ToR.	V4.0	Uni Sec. & CIO: 17/12/13
Aug '12	M Trump	Change to section 5.2.18 permitting use of p2p not requiring written permission of CIO.	V3.2	Executive: Sep 12
Aug '11	C Price	General review and alumni use of Email for Life	V3.0	Executive: 30/08/11

Policy Management and Responsibilities

Owner:	This Policy is issued by the Director of Estates, Facilities & IT in his capacity as Chief Information Officer (CIO) and Director of Legal Planning and Governance in his capacity as 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 on behalf of the University.
Others with responsibilities (please specify):	All subjects of the Policy will be responsible for engaging with and adhering to this policy.

Assessment	*Cross relevant assessments*	*Cross if not applicable*
Equality Analysis	X	
Legal	☐	☐
Information Governance	X	☐
Academic Governance	☐	X

Consultation	*Cross relevant consultations*
Staff Trades Unions via HR	☐
Students via USSU	☐
Any relevant external bodies (please specify)	☐

Authorised by: Information & Technology Management Group (ITMG). Minor changes may be authorised by the Director of Legal, Planning & Governance and the Director Estates, Facilities & IT on behalf of the (ITMG).

Date authorised: 30/09/2015

Effective from: 17/12/2015

Review due: 3 years by December 2018

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, Student Channel news item, inclusion in HR processes for new staff.

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. This policy is a key component of the overarching University Information Framework. The Information Framework exists to ensure that all those who are authorised to, should be able to easily access all the information they need to fulfil their role.

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 students, staff, associates and alumni 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 Each user is issued with a valid username and password which must be used to authenticate and gain access to the ICT facilities. The password 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. Passwords must meet the Password complexity requirement of

a. 9 characters
b. Alphanumeric (at least 1 number)
c. Mix of upper and lower case letters
d. Changed every 6 months;

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 (Related Documentation);

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 Third Party Access to IT Account Form (Related Documentation) 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 The University only endorses and supports the use of cloud computing services for the management and storage of University information where this has been undertaken under a University negotiated contract approved by Legal, Planning and Governance and IT Services. In the absence of such a contract, University owned information should be stored within University managed storage;

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

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

3.1.15 (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;

3.1.16 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;

3.1.17 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;

3.1.18 All University systems owners must ensure that their information systems and supporting infrastructure comply with ITS Policy (See Related Documentation) and current legislation;

3.1.19 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;

3.1.20 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;

3.1.21 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 access any University system by circumventing the network authentication process;

3.2.5 obtain unauthorised commercial gain or obligations;

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

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

3.2.8 sell or redistribute any part of the ICT facilities

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

3.2.10 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;

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

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

a. any terrorist related or extremist material, or any data capable of being resolved into such material (other than in the course of properly supervised, lawful and authorised research – see Related Documentation). This is a requirement of the University's Prevent Duty under s26(1) of the Counter-Terrorism and Security Act 2015 as specified by guidance issued under s29(1) of the Act.

b. 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);

c. 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;

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

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

f. 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);

3.2.13 place links to websites which have links to, or display, pornographic or 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;

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

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

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

3.2.17 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;

3.2.18 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);

3.2.19 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;

3.2.20 connect any non-approved or personally owned ICT equipment to the University physical (wired) network points without written authorisation of IT Services (via ITS Service Desk) **and** adequate protection in accordance with point 3.1.17;

3.2.21 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;

3.2.22 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;

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

3.2.24 save or share any University owned confidential information on any cloud computing service unless it is under a University negotiated contract approved by IT Services and by Legal, Planning and Governance Directorate.

3.2.25 otherwise transmit, distribute, discuss or disclose (on Message Boards, email or any other mechanism) any University owned or held **confidential information** (See Related Documentation).

3.3 Exceptions to this Policy

3.3.1 Where, for operational reasons, an exception to this Policy is required, it must be requested in accordance with the published process (Related Documentation) and approved by the relevant member of the University Management Team and the Associate Director: IT Services. The acceptable and prohibited activity sections are based on statutory and contractual requirements which will take priority over any operational exceptions.

3.4 Alumni Email for Life

The provision of an Email for Life account for each alumnus is at the discretion of the University's Director of Estates, Facilities & IT 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.
f. The University accepts no liability for any loss of data from an Email for Life account.

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.

3.5 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. ICT activity logs will also include access to University ICT facilities when using personally owned computers or mobile devices. 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 IT Account Investigation Request form (Related Documentation) 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 IT Account Investigation Request 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) (see Appendix 2 for Terms of Reference) or relevant School or Division in line with the appropriate University disciplinary policy. (See Related Documentation section). 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

5.1 University Policy

The following directly related policies and documents are located within the University Policy & Procedure Pages (or under ‘P’ on the Staff Channel A-Z index)

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

- Information Security Policy
- Data Protection Policy
- Network Security & Connection Policy
- Forensic Readiness Policy (in draft)
- ITSERT Terms of Reference
- Access by Ex-Employees to IT Accounts
- Internet Activity Requests by Line Managers
- Retention of IT System logfiles, deleted emails and leavers accounts
- Student AUP Code of Practice
- Student Disciplinary Procedures

The following HR documents are located on the HR Policy pages

http://www.salford.ac.uk/hr/policies-and-forms

- Staff Disciplinary Policy

5.2 Internal Forms

ITS Service Desk Top forms http://www.its.salford.ac.uk/servicedesk/

- IT account investigation request form
- Third party access to IT accounts form
- Extraordinary internet access form

5.3 External documents

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

Microsoft Live@Edu Code of Conduct available at http://explore.live.com/code-of-conduct

Microsoft Service Agreement available at http://explore.live.com/microsoft-serviceagreement

UUK Guidance: Oversight of security-sensitive research materials in UK Universities at

http://www.universitiesuk.ac.uk/highereducation/Pages/OversightOfSecuritySensitiveResearchMaterial.aspx#.VgEZjIeFPcs

6.0 Appendices

- Appendix 1: ICT AUP Agreement
  (hard copy signature required by Human Resources when new employees sign their contract of employment – to be held in personnel file).

Appendix 1: ICT AUP Agreement

Please sign the below agreement and return the signed page to University of Salford Human Resources Directorate. 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 4.1 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: