ICT Acceptable Use Policy

Version Number 4.3

Effective from 18 July 2018

Author: Senior Information Security Officer

Legal & Governance Directorate

Document Control Information : Revision History (most recent first)

Author	Summary of changes	Version	Authorised & Date
CP	General updates, inclusion of remote working advice to enable deletion of current Mobile Devices Policy	V4.3	Director L&G: 21/06/2018 CIO: 02/07/2018
CP, MS, MH	General updates and amended prohibited internet access form to support Prevent Duty	V4.2	Director L&G: 09/02/2017 CIO:29/03/2017
CPrice& M.Stephenson	Update re PREVENT statutory duty, organisational changes, password complexity, Cloud services rules for confidential information	V4.1	Director LPG: 9/12/15 CIO: 13/11/15 Info &Tech Mgt Grp:30/09/15
C. Price	General review, software and IT equipment move requests. Inclusion of ITSERT ToR.	V4.0	Uni Sec. & CIO: 17/12/13
M. Trump	Change to section 5.2.18 permitting use of p2p not requiring written permission of CIO.	V3.2	Executive: Sep 12
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 Chief Information Officer (CIO) and the Director of Legal & Governance Directorate. The CIO has the authority to issue and communicate policy on University ICT facilities, services and usage. The Director of L&G 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.

Author to complete formal assessment with the following advisory teams:

Equality Analysis (E&D, HR) *Equality Assessment form*	1. *This is mandatory. EA submitted 16 July 2018.*
Legal implications (L&G)	2. *N/A*
Information Governance (L&G)	3. *Incorporated as part of revision process*
Student facing procedures (QEO)	4. *N/A*
UKVI Compliance (Student Admin)	5. *N/A*

Consultation:

Staff Trades Unions via HR Students via USSU Relevant external bodies (specify)	1. N/A

Review:

Review due:	1 year by July 2019
Document location:	University of Salford Policy pages http://www.salford.ac.uk/policies

The owner and author are responsible for publicising this policy document.

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, employees, alumni and associates. This policy is a key component of the overarching University Information Framework which states 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 To whom the policy applies

2.1.1 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, employees and associates (including contractors and service providers) of the University. **Any individual accessing University information using the ICT facilities (whether on personally owned or University issued devices) is deemed to have accepted this Policy and is bound by it.** This policy does not form part of the contract of employment or student contract and can therefore be amended without Users' consent. The University may make changes to the Policy at any time. Users will be notified of the changes.

2.1.2 ICT facilities are provided to Users primarily for University business purposes to support teaching, learning, research & enterprise and professional & administrative activities. Occasional and reasonable personal use of the facilities is acceptable, however, the University business purposes of ICT facilities take priority over any personal use. (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 (see Related Documentation).

2.1.3 The ICT facilities and access to University information will vary per user group; some users will only be entitled to use some limited facilities. The University reserves the right to refuse access to particular computing equipment, devices or software where it considers that there is a security risk to its information or ICT facilities.

2.1.4 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;

2.1.5 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.

2.1.6 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.

2.1.7 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.

2.2 Incident reporting

Security incidents and actual or suspected breaches of this policy should be reported immediately to the Digital IT Service Desk Digital-ITServiceDesk@salford.ac.uk 0161 2952444.

2.3 Definitions

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

a. network infrastructure and services, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers, internet access and web services, email, wireless, messaging, shared filestore, printing, telephony and fax services, CCTV, door and car park access control;

b. university owned computing hardware (hereafter referred to as devices), both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, tablets, smartphones, servers, printers, scanners and monitors;

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

2.4 Alumni Email for Life

The provision of an Email for Life account for each alumnus is at the discretion of the University CIO and, where provided, is subject to the following:

a. 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.

b. 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).

c. The contents of Email for Life accounts that are terminated will be irretrievably deleted. The University will not be held liable for any alleged loss of alumni data resulting from such deletion.

3.0 Policy Statements

3.1 Acceptable Use and User Responsibilities

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

3.1.1 Use the ICT facilities in a responsible and courteous manner in accordance with:

3.1.1.1 this policy 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;

3.1.1.2 all relevant copyright legislation, licences and agreements for software and electronic information resources;

3.1.1.3 all applicable laws in the United Kingdom;

3.1.2 (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;

3.1.3 (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;

3.1.4 All users are expected to understand the data classification (see Related Documentation) of the document(s) they are handling and must not place that information at risk; whether accidentally or deliberately. Such risks may include sending document(s) to a commercial competitor, a member of the public, a colleague or applying insufficient safeguards to the information in electronic or paper form.

3.1.5 (In the case of System owners) ensure their information systems or supporting infrastructure adhere to industry best practice including technical security measures and system governance;

3.1.6 Report any technical problems, requests or concerns regarding a suspected policy breach directly to the Digital IT Service Desk;

Protecting University information and ICT facilities

3.1.7 Be responsible for all ICT activity under username and not share passwords. Password complexity is specified on the Digital IT webpages

3.1.8 Be mindful of the effect on University (and personal) reputation in relation to any use of social media whether personal or work related. Social media leaves a permanent record and electronic footprint. Using social media in such a way as could bring the University into disrepute will be actionable as a disciplinary matter;

3.1.9 Ensure personally owned devices have up to date and patched operating system and active anti-virus protection;

3.1.10 Not click on unsolicited attachments or emails or respond to phishing emails requesting passwords;

3.1.11 Notify Digital IT of University IT equipment changes (office move or role changes) to ensure update of IT Equipment register;

3.1.12 Return all University IT equipment to Digital IT at end of employment, contract or use period. This ensures IT re-image or secure erasure and disposal. University IT equipment must not be sold, given away or otherwise disposed of by the user;

3.1.13 Obtain System Owner written approval before transmitting University confidential information externally. Ensure data is adequately protected (including use of encryption);

3.1.14 (In the case of all employees and associates processing information on behalf of the University), take precautions when working from remote / off campus locations; including (but not limited to):

a) Be aware that using personally owned mobile devices to carry out University work can create risks including; data protection; vulnerability to virus infection or malware; unintentional or unlawful compromise of data;

b) Where possible, use University issued computers/devices to access and process University information from remote locations, as they are subject to consistent technical standards, support and security measures;

c) Use University managed storage (shared drives) and information systems, which is protected by network username and password.

d) Ensure University information is stored securely if extracted from University managed storage/systems: Obtain System Owner authorisation **and** use an encrypted USB / mobile device. Ensure it is the minimum information necessary; is temporary and is deleted as soon as the information is no longer required;

e) Do not store University information in ‘personal’ or ‘free’ cloud storage that do not meet the University security requirements and are not subject to the protections within a University negotiated contract. Such instances of prohibited storage include personal drives such as google, dropbox, skydrive;

f) Delete University information from a personally owned IT equipment before leaving University employment or when selling, transferring or disposing of, the device. (may be asked to provide written confirmation);

g) Use reasonable care and security measures to prevent loss or theft of IT equipment and information: not leave unattended in a public area or when travelling, keep in a secure access controlled area when not in use and follow a clear desk policy; use a device lock i.e. PIN, password or other mechanism to prevent casual access;

h) Report loss/theft/breach of University information or IT equipment to the Digital IT Service Desk immediately. The Service desk will advise on appropriate actions including: password change, user notification to network provider; remote wiping of device, IT asset register update, security incident investigation and asset replacement process;

i) Report theft of University IT equipment to the Police and to Estates Security team (Maxwell 0161 2954773)

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 sell or redistribute any part of the ICT facilities;

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

3.2.5 carry out activities of a nature that compete with the University in business, obtain unauthorised commercial gain or obligations;

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

3.2.7 carry out activities that unreasonably waste network resources, deny ICT facilities to authorised users or continue to carry out activity after a designated Digital IT authority has requested that use ceases;

3.2.8 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. 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;

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);

3.2.9 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;

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

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

3.2.12 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);

3.2.13 access any University system by circumventing the network authentication process, gain or attempt to gain unauthorised access to facilities or services via the University ICT facilities, using automated processes or otherwise

3.2.14 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;

3.2.15 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 written permission of the University's Chief Information Officer;

3.2.16 connect any non-approved or personally owned ICT equipment to the University physical (wired) network points without written authorisation of Digital IT Services (via Service Desk) **and** adequate protection in accordance with point 3.1.9;

3.2.17 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;

3.2.18 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;

3.2.19 install any software without authorisation of Digital IT (via Service Desk)

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

3.2.21 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

Where, for operational reasons, an exception to this Policy is required, the request should be made in writing to the IT Security Emergency Response Team (ITSERT@salford.ac.uk) and approved by a relevant member of the University Management Team. This includes using the Prohibited Internet Access form (see Related Documentation section) to request authorised access to prohibited internet material.

4.0 Enforcement of the ICT Acceptable Use Policy

Breaches of the ICT Acceptable Use 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 Related Documentation section). The initiating 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. 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.

Where there is evidence of a criminal offence, the issue will be reported to the Police. The University will co-operate with and disclose copies of any data and ICT activity logs, and equipment used to the Police (or other appropriate external agencies).

5.0 Related Documentation

5.1 University Policy

The following documents are located within the Policy & Procedure Pages http://www.salford.ac.uk/policies :

- Information Security Policy (Information Governance section)
- Data Classification Guide (Information Governance section from August 2018)
- ITSERT Terms of Reference (Information Technology section)
- IT arrangement for leavers and their managers
- Retention of IT System logfiles, deleted emails and leavers accounts
- Student Disciplinary Procedures (Academic Governance)
- Staff Disciplinary Policy

5.2 Digital IT Documentation

- Prohibited Internet access form (IT Security tile of the DIT webpages) https://www.salford.ac.uk/__data/assets/word_doc/0020/1175051/ProhibitedInternetAccessFormV2.1.docx
- Third party access to IT accounts form (IT Accounts tile of the D IT webpages) https://www.salford.ac.uk/__data/assets/word_doc/0003/915573/ThirdPartyAccess-to-IT-accounts-V4-3.docx
- IT account investigation request form (located within the IT Security tile of the DIT webpages) https://www.salford.ac.uk/__data/assets/word_doc/0010/901468/180605ITInvestigationrequestFormV4.6.docx

5.3 External documents

The University of Salford's external network connection is governed by the Joint Academic Network (JANET) policies: https://community.jisc.ac.uk/library/janet-policies/security-policy

Microsoft Service Agreement available at https://www.microsoft.com/en-gb/servicesagreement/

UUK Guidance: Oversight of security-sensitive research materials in UK Universities http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/oversight-of-security-sensitive-research-material-in-uk-universities.aspx