

ICT Acceptable Use Policy

1.0 Policy Administration

Table for completion by Author			
Document Title	ICT Acceptable Use Policy		
Document Category	Policy		
Policy ref.	Unique ref no. Issued by GSU	Version Number	3.0
Status	Revised (updating ICT AUP V2.0)		
Reason for development	Updated Department references Terms and conditions for Alumni Email for Life		
Scope	This Policy applies to: All Staff, Students, Associates and Alumni with authorised access to the University ICT facilities.		
Executive Summary	<p>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.</p> <p>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.</p>		
Author /developer	Senior Information Security Officer	Owner	Director IT Services.
Assessment	<ul style="list-style-type: none"> • Information Governance - Yes • Equality Impact Assessment - Yes • Legal - Yes 		
Consultation (where relevant)	<ul style="list-style-type: none"> • Trade Unions – N/A as no major change • External Statutory or Regulatory bodies – N/A 		
Authorised by (Board)	Executive Committee	Date: 30th August 2011	
Effective from	31 st August 2011		
Review due	2 years – August 2013		
Document location	IT Services and Library Policies webpages and Student 'Get ready for registration' pages for transfer to new University policy pages (Winter 2011)		
Document Dissemination / Communication Plan	<ul style="list-style-type: none"> • US online briefing to all staff • Link on above specified webpages 		
Document Control	All printed versions of this document are classified as uncontrolled. A controlled version is available from the University Policy page on the University of Salford website.		

2.0 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.

3.0 Scope

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, notwithstanding article 12 of the Charter "Academic Staff employed by the University shall have freedom within the law to question and test received wisdom, and to put forward new ideas and controversial or unpopular opinions, without placing themselves in jeopardy of losing their jobs or privileges". 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.

ICT facilities encompass (but are not restricted to):

- 3.1 network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers;
- 3.2 network services, including (but not exclusively) Internet access in Halls of Residence, web services, broadband, email, wireless, messaging, network filestore, printing, telephony and fax services, CCTV, door and car park access control;
- 3.3 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;
- 3.4 software and databases, including applications and information systems, virtual learning and videoconferencing environments, language laboratories, software tools, information services, electronic journals & e-books;
- 3.5 third party provided IT services including (but not limited to) email accounts;
- 3.6 personal computing equipment, which must be authorised, where it is used for University business.

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

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

The University may make changes to the Policy at any time by giving notice of such changes to users.

4.0 Governance & Management

This policy is issued by the Executive Director of ITS who, as Chief Information Officer of the University has the responsibility for (and the authority to delegate responsibility for):

- 4.1 developing and communicating policies and procedures for the University's ICT facilities, services and usage;
- 4.2 managing and protecting the ICT facilities;
- 4.3 removing or inspecting computer equipment from the University network if it is deemed to be interfering with the network operation or breaching policy;
- 4.4 withdrawing the use of, or suspending, User network accounts if it is deemed necessary to safeguard the University information, infrastructure, network and reputation;
- 4.5 preventing, detecting and investigating alleged and actual cases of ICT misuse;
- 4.6 enforcing sanctions directly or referring individuals for disciplinary action as necessary to safeguard the University and its members.

5.0 Policy Statements

5.1 Acceptable Use

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.

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

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

The University expects Users to use the ICT facilities 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;

- 5.1.1 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;
- 5.1.2 Be responsible for all activity that takes place under their usernames and 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;
- 5.1.3 Be courteous and considerate of others when using the ICT facilities;
- 5.1.4 (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;
- 5.1.5 (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 4);
- 5.1.6 (In the case of staff and students) ensure personal use is occasional, reasonable and (in the case of all Users) 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;
- 5.1.7 The University's business purposes (primary purpose) of ICT facilities take priority over any personal use;
- 5.1.8 (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 (Appendix 3) account procedure and will supersede personal use;
- 5.1.9 Ensure a user has appropriate authorisation and appropriate technical protection before sending or transmitting University owned sensitive, confidential or commercially sensitive information external to the University network or email system;
- 5.1.10 Comply with all relevant copyright legislation, licences and agreements for software and electronic information resources when accessing and connecting to University ICT facilities;
- 5.1.11 Obtain authorised and appropriate software licences and installation via IT Services;

- 5.1.12 Make all reasonable efforts to send data that is 'virus free' and not open email attachments from unsolicited or untrusted sources;
- 5.1.13 Utilise good information security and management practices for the storage, access, retention and deletion of University information;
- 5.1.14 Ensure any computer (on or off campus) 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;
- 5.1.15 All University systems owners must ensure that their information systems and supporting infrastructure comply with agreed ITS policy and current legislation;
- 5.1.16 ITS scans for spam and viruses however, due to the rapidly changing nature of technology, the University cannot guarantee that the network and email communications are spam and virus free. The University will not be held responsible for any damage to users' systems or information that may occur through such virus or hacking attacks;
- 5.1.17 Report any technical problems, requests or concerns regarding a suspected policy breach directly to the ITS Service Desk;
- 5.1.18 In addition to this Policy, Users must 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;
- 5.1.19 Access to the internet via the ICT facilities is strictly subject to compliance with all applicable laws in the United Kingdom;
- 5.1.20 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;
- 5.1.21 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.

5.2 Prohibited ICT Activity

Users **may not** use University ICT facilities to:

- 5.2.1 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;
- 5.2.2 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;
 - 5.2.3 carry out any personal business or commercial purpose or gambling;
 - 5.2.4 gain unauthorised personal, commercial or any other form of financial gain;
 - 5.2.5 commit the University via means of email contract except for staff who are expressly authorised to do so using university purchasing procedures;
 - 5.2.6 carry out activities of a nature that compete with the University in business;
 - 5.2.7 sell or redistribute any part of the ICT facilities
 - 5.2.8 carry out activities that conflict with an employee's obligations to the University as their employer;
 - 5.2.9 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;
 - 5.2.10 carry out activities that unreasonably waste staff effort or network resources or activities that unreasonably serve to deny ICT facilities to authorised users;
 - 5.2.11 deliberately or unintentionally receive, access, create, change, store, download, upload, 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;

- 5.2.12 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)
- 5.2.13 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;
- 5.2.14 falsify emails to make them appear to have been originated from someone else, or send anonymous messages without clear indication of the sender;
- 5.2.15 carry out activities that criticise or harm individuals or that violate the privacy of other individuals;
- 5.2.16 use automated processes or otherwise, to gain or attempt to gain unauthorised access to facilities or services via the University ICT facilities;
- 5.2.17 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;
- 5.2.18 deliberately or unintentionally attempt to circumvent the University's security systems, or use file-sharing systems (sometimes known as P2P or peer-to-peer) without first gaining the written permission of the University's Chief Information Officer;
- 5.2.19 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;
- 5.2.20 connect any non approved ICT equipment (including but not limited to wireless access points) to the University network or set up any network services, without the express permission of the University's Chief Information Officer (this excludes connectivity of PCs and laptops by students, staff or specified associates in University Halls of Residence as this is permitted);
- 5.2.21 connect any personally owned computers to the University physical network points without written authorisation of ITS Service Desk and adequate protection in accordance with point 5.1.15;

- 5.2.22 register any domain name which includes the name of the University or any name which may mislead the public into believing that the domain name refers to the University;
- 5.2.23 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;
- 5.2.24 make, use, install, possess, distribute, sell, hire or otherwise deal with any unauthorised copies of computer software for any purpose without the licence and permission of its owner;
- 5.2.25 install any software not licensed to the University or unauthorised copies of software on the University computer systems or computers connected to the ICT network under any circumstances;
- 5.2.26 without authority transmit or distribute to any third party or discuss (on Message Boards, email or similar media) any sensitive, confidential or commercially sensitive information of the University or any of its staff, students, alumni or associates.

6.0 Enforcement of the ICT Acceptable Use Policy

6.1 Monitoring

Monitoring and recording of emails, internet use, telephone calls or other ICT usage is not routinely carried out, but may be carried out (in compliance with applicable obligations under the Data Protection Act 1998) 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 telecommunications system
- 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 and for individual investigations require completion and appropriate authorisation of the ITSERT Investigation Authorisation form (Appendix 2). 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, with the prior permission of the students, 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.

6.2 Incident Reporting

Information security events and actual or suspected breaches of the Acceptable Use Policy should be reported immediately to the ITS Service Desk.

6.3 Misuse and Sanctions

Violations of the Acceptable Use Policy may be investigated under the University's appropriate disciplinary procedure. Sanctions for violations of the policy may include:

- a. Suspension or withdrawal of University ICT facilities
- b. Disconnection & seizure of any ICT equipment that is in violation of this policy
- c. Reconnection fee
- d. 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.

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.

7.0 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.

8.0 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.

9.0 Related Documentation

- Information Security Policy
- Data Protection Policy
- Staff and Student Disciplinary Procedures
- Network Security & Connection Policy

The University of Salford's external network connection is governed by the Carrier's policies Joint Academic Network (JA.NET) <http://www.ja.net/services/publications/policy-documents.html>:

- JANET Connection Policy
- JANET Security Policy
- JANET Acceptable Use Policy.

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-service-agreement?ref=none>

Controls addressed in this policy from ISO/IEC 27001:2005 Information Security Management Systems – Requirements

7.1.3	Acceptable Use of Assets
8.2.3	Disciplinary process

9.2.6	Secure Disposal or re-use of equipment
10.4.1	Controls against malicious code
10.4.2	Controls against mobile code
13.1.1	Reporting information security events
13.2.1	Responsibilities and procedures
13.2.3	Collection of evidence

10.0 Appendices

Appendix 1: Student AUP Code of Practice (link on IT Services homepage (useful documents) <http://www.library.salford.ac.uk/policies/aupcop.pdf>)

Appendix 2: ITCERT Investigation Authorisation form (link on IT Services Service Desk Top forms list) <http://www.its.salford.ac.uk/servicedesk/>

Appendix 3: Third party IT access form (link on IT Services Service Desk Top forms list) <http://www.its.salford.ac.uk/servicedesk/>

Appendix 4: Extraordinary Internet Access form (to be linked on ITS Service Desk Top forms list) <http://www.its.salford.ac.uk/servicedesk/>

Appendix 5: ICT Facilities Agreement (hard copy signature required by Human Resources when new staff join and sign contract – held in personnel file).

AUP Code of Practice for Students

Prohibited ICT Activity

The ICT Acceptable Use Policy (AUP) <http://www.library.salford.ac.uk/policies/ictaup.pdf> applies to all students and staff. It details acceptable and prohibited ICT activity. All ICT usage is automatically logged and may be monitored (in accordance with the Regulation of Investigatory Powers Act 2000). Main activities you **must not do** include:

- Deliberately or unintentionally port scan or use port scanning software;
- Use peer to peer (p2p) filesharing software such as Torrent, Bear Share or Shareaza to download or upload copyrighted, obscene or illegal material (including, but not limited to) music, films, games and software;
- Access and/or transmit illegal or obscene material, or material that discriminates on any grounds;
- Connect or attempt to connect to University ICT systems without permission;
- Run server operating systems or services without permission;
- Make, install or distribute unauthorised copies of computer software on computer equipment connecting to the ICT network;
- Connect any form of network device (i.e. routers, wireless access points, switches or hubs) to the ICT network;
- Transmit unsolicited material, junk mail or spam; and;
- Deliberately or unintentionally cause the interruption of any University service or another user's data or system, e.g. by virus infection.

Sanctions for breach of AUP may include;

- Withdrawal of University ICT and Library facilities;
- Disconnection & seizure of equipment that is in violation of the policies;
- Reconnection fee of **£100** for ICT AUP breaches on Student Finance record;
- Initiation of student discipline procedure.

AUP Breach - What to do next

If your IT account has been blocked, you will need to meet with a member of the ITSERT team to discuss the matter (arranged via ITS Service Desk). Following an AUP breach, you must stop that activity, remove the offending software from your computer and attend the Finance Department at Faraday House to pay the AUP reconnection fee on your student finance record. IT and Library access will be re-activated unless the case is a more serious breach of the AUP and leads to disciplinary action.

Passwords to protect you and your access

You are responsible for all activity that takes place under your username.

- Protect your internet, filestore and Blackboard access by using a memorable password for your account.
 - Use a combination of at least 8 letters, numbers and symbols that you must not tell anyone and don't need to write down. Try using a memorable saying or phrase e.g. My best friend's birthday is April 4 - buy gift! = MbfbiA4-bg!
- You'll also need to protect you Student Email account and password, and your Athens password. Contact the Service Desk if you need any help. Tel:0161 2952444 or email its-servicedesk@salford.ac.uk
- If you are worried someone has guessed your University account password, press Ctrl, Alt and Delete keys, whilst logged on in a campus PC Suite to change your password. You can also use these keys to log off and shut down the computer.
- The University of Salford will never ask you to reveal any passwords via email, or send phishing or 'threatening' messages insisting you change passwords – these are attempts by fraudulent people to steal your identity and financial details. Do not respond to such emails, just delete them.

Protect yourself – personal security

Follow the CampusWatch advice leaflet on physical and personal safety. Report Security concerns to Estates Security Control (24/7) on 0161 2954773.

Protect your personal computer

You can help protect the University network and information by protecting your personally owned home computer. Viruses and spyware can infect and slow your computer and be misused for criminal purposes so you should set regular updates for anti-virus, operating system and anti-spyware software as well as weekly scans.

1. If you are in Halls of Residence, the Clean Access Agent will help you to set the necessary updates. Ensure you also set a weekly scan of your computer for viruses.
2. If you are not in Halls, but use a computer on the internet you should set the updates on your computer yourself. If you need some help, book on one of the Library IT training courses 'How to protect your personal home computer'.

Saving your work

Your personal space on the University ICT network is known as your F: drive. It is unique to your username. If you save to other devices be aware of version control and keep backup copies.

Copying & Copyright

Please be aware that copyright laws apply to all library, e-library material as well as material on the internet. See posters next to every Library photocopier and check the Information Governance website at <http://www.infogov.salford.ac.uk/copyright/>

ITSERT Investigation Authorisation form

The purpose of this guide and form is to specify criteria and procedures for a member of the IT Services ITSERT to obtain access to a University of Salford (UoS) Users' ICT account or University owned IT equipment, when carrying out an ITSERT investigation. This will assist in maintaining the chain of custody and documentation of an investigation so that actions can be defended if challenged in court or a disciplinary hearing. This form **must** be completed when investigating IT security incidents with an ITSERT Significance Rating of:

- **Severe** – illegal incidents that must be reported to law enforcement agencies
- **Serious** – incidents that impact on a number of other IT users or systems, that impact on University reputation or include staff misuse.

In line with the ICT Acceptable Use Policy, certain conditions must be fulfilled before access to ICT activity logs, accounts or equipment is authorised. These conditions include:

- clearly scoped request (see below)
- justification of the request (in line with legislative and UoS policy framework) to enable a specific and targeted investigation
- identification of the equipment, services or individual to be investigated
- request directed via the IT Services ITSERT
- formal written authorisation by the Director of the requesting Division/Faculty, **and** by the IT Services Director as the University's Chief Information Officer.

Requests for access may include (but are not limited to):

- access to, copy and capture of ICT activity logs for investigation
- removal or disconnection of University owned ICT equipment
- access is required to otherwise comply with the ICT Acceptable Use Policy or the Regulation of Investigatory Powers Act 2000.

Incidents with a **Severe** significance rating may not always be investigated by the ITSERT and may instead be immediately reported to the relevant Police force. However, the ITSERT may use this form to collect initial evidence.

Completed forms will be securely stored with strictly limited access (subject to legislation including the Freedom of Information Act 2000 or Data Protection Act 1998) for 7 years from end of case.

Warning: IT Services technical staff authorised to search for evidence relating to a particular case should not deviate from that enquiry. However, should other concerns or material be identified during this investigation, it may lead to a re-categorisation of the incident and response by the University. Technical staff are required to treat **all** material confidentially and **not** to act upon it or disclose it to any other person except those directly associated with the investigation. Technical staff must preserve the confidentiality of any private or personal data that he/she may inadvertently view whilst undertaking the investigation. A failure to do so could constitute an offence under the terms of the Human Rights Act 1998 or related legislation and a disciplinary matter.

Staff completing and authorising the form overleaf are certifying that they have read and understood this guide. The form should be completed electronically (where possible), then printed for hard copy signature of applicant and authorise.

ITSERT Investigation Authorisation form V4.0

A) Details of person making the request		
Name (in capitals):	School/Division:	
Role:	Phone ext:	
Signature:	Date:	
B) Details of account/user/equipment to be investigated		
Name (in capitals):	UoS Username:	
School/Division:	Ext. No.	
Building and Office Number		
UoS IP/MAC address (if known):		
Equipment and core services used by the individual (please list if known):		
Any additional facts or identifying equipment (include ref to other information sources):		
C) Details of alleged activity		
Date and time of alleged activity:		
Nature of alleged activity:		
Reason for investigation:		
Specific description of the information/data being requested:		
D) Confirmation of HR involvement in staff and temporary staff investigations		
HR Business Partner involved in the investigation:		
E) Authorisation by Head of School/Executive Director of Support Division.		
I approve /do not approve the investigation to proceed as detailed above in sections B and C. I confirm that I am acting in accordance with the ICT AUP and Staff and Student Disciplinary Procedures.		
Name (in capitals):		
Role:	Signature:	
F) Authorisation by IT Services Director. (Associate Director in his/her absence)		
I authorise/do not authorise the investigation to proceed as detailed above in sections B and C. I confirm that I am acting in accordance with the ICT AUP and Staff and Student Disciplinary Procedures.		
Name (in capitals):		
Signature:	Date authorised:	
Please send form in a sealed envelope to Christa Price, Senior Information Security Officer, Acton Square.		

Guidelines for accessing third party accounts on ITS managed systems

Warning: Individuals granted operational access to another user's data may **only view material that is necessary to complete the operational requirement for which access was granted.** The individual is required to treat **all** material confidentially and **not** to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. Where access is provided to another users filestore or email, please note:

- two people should be present when viewing
- access will be time limited (usually 1 week)

A failure to preserve the confidentiality of any private or personal data that is inadvertently viewed, whilst undertaking operational matters, may constitute an offence under the terms of the Human Rights Act 2000 or other legislation.

1. The purpose of this guideline is to specify procedures for a member of University staff to gain access to another staff member's IT account, on systems provided or managed by IT Services. In line with the ICT Acceptable Use Policy, it is necessary to provide the full information specified overleaf. Ideally IT account access should be provided with the consent of the individual concerned. However when obtaining consent is not possible, the operational requirement can include (but is not limited to);
 - operational access to another staff member's e-mail or filestore during his/her **unexpected absence**; for example due to an accident, illness; or,
 - operational access to a former staff member's data after he/she has ceased University employment (this should be made prior to the individual leaving); or,
 - operational access to archived data and the original account holder is unavailable to grant permission; or,
2. The person requesting access and the authorisers are certifying that they have read and understood this guideline. The form should be completed electronically (for each individual occasion on which access is required) and forwarded to the relevant Executive Dean, Director or Head of School for authorisation.
The authoriser should email the completed form (from his/her email account) to the ITS Service Desk its-servicedesk@salford.ac.uk
3. The application form also requires authorisation from the University's Data Protection Officer, Information Security Officer or IT Security Specialist to confirm that the access is compliant with the relevant legislation and can proceed.



Third Party IT Account Access Request Form

This form should be completed electronically and submitted by email to the ITS Service Desk in accordance with the guidelines overleaf.

A) Details of person making the request

By completing this form I confirm that I have read and agree to comply with the guidelines for Accessing a Third Party IT Account.

Name:		Username:	
Faculty/School/Division:		Phone Ext:	

B) Details of account to be accessed

Name:		Username:	
Faculty/School/Division:		Phone Ext:	

C) Details of what access is being requested and justification for this request (tick✓)

F Drive: Access to specific files/folders (specify below)	
F Drive: Access to files but not password (see warning overleaf)	
Email: "Out of Office" message (specify below) asking users to send email to the account listed in A	
Email: Redirect from account listed in B to account listed in A (specify time limit below)	
Email: Access to contents of mailbox (see warning overleaf)	
Telephone: Reset voicemail PIN	
Other: (specified below)	

Details of request

Reason Access Required:

When sections A, B & C are fully completed, this form is to be passed on to the requestor's Executive Dean, Director or Head of School for authorisation.

D) To be completed by the requestor's Executive Dean, Director or Head of School

I authorise the person in Section A to access the account of the person in Section B for the reason and period specified in Section C. I confirm that the level of access required is necessary for operational purposes.

Name:		Position:	
Faculty/School/Division:		Date:	

Once completed, this form should be emailed to the ITS Service Desk (its-servicedesk@salford.ac.uk) from the email account of the Executive Dean, Director or Head of School as proof of authorisation.

Incomplete forms or insufficient level of authorisation will be returned to the Requester for full completion.

Extraordinary Internet Access form V1.0

The purpose of this form is to register 'supervised and lawful research' with the IT Services Division. Extract from JANET AUP <http://www.ja.net/company/policies/janet-aup.html>

- "11. JANET (Joint Academic Network) may not be used for the following;
12. Creation or transmission, or causing the transmission, (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;"

Terms and Conditions

1. Access to obscene or indecent images is barred in open access areas/PC suites.
2. The request may involve further discussion with your School and / or Greater Manchester Police.
3. Printing of obscene or indecent images is only allowed on the applicant's personal printer.
4. Send the completed form to: Senior Information Security Officer, Acton Square. Tel 0161 2955910.

Applicant's Name (in capitals):	
Role:	School:
Student/Staff Username:	Phone ext:
Date access required (start date to end date):	
Description of the research activity and type of material involved:	
Is illegal material likely to be accessed? YES/NO	
If "Yes" have the police been consulted? YES/NO	
As the applicant, I accept responsibility to use the extraordinary internet access responsibility and comply with the terms and Conditions above: Applicant's Signature: Date:	As Head of School/Research Institute, I accept responsibility for the conduct of the Applicant and the research activity detailed above: Signature: Date:

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 and understood the attached ICT Acceptable Use Policy 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: