UoS Information Security

ICT Acceptable Use Policy

Doc ID: UoS-IS-Doc202-ICT Acceptable Use Policy

Version Number V7.0

June 22nd 2022

Author: Head of Information Security
Digital IT

Table of Contents

Introduction

The ICT Acceptable Use Policy (ICT AUP) defines a common set of rules and behaviours relating to the University of Salford's IT infrastructure and other information assets.

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, associates, and alumni.

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 changes to this policy via news articles published on The Hub.

Scope

The ICT Acceptable Use Policy applies to all authorised users of the University's ICT facilities including 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 its terms.

System owners shall ensure their information systems or supporting infrastructure adhere to the policies, standards and processes set out in the Information Security Framework and industry best practice where such guidelines are missing.

Definition

In this document, the term "ICT facilities" includes, but is not restricted to, the following systems and equipment provided or hosted by the University of Salford, and third parties on its behalf, to access and process University information:

1. Network infrastructure and services, including, but not limited to, the physical IT infrastructure, wireless access services, networks, servers, firewalls, connection points, switches and routers, internet access, email, messaging, shared file stores, printing, telephony services, CCTV, and digital physical access controls.
2. University owned computing hardware devices (hereafter referred to as devices), both fixed and portable, including, but not limited to, workstations, laptops, tablets, smartphones, servers, printers, scanners, and monitors.
3. Software, databases, any structured or unstructured University data, applications, information systems & services, virtual learning and videoconferencing environments, ICT laboratories, electronic journals, and e-books.

Liability of Use

The University does not endorse any third-party goods or services unless specifically indicated and is not responsible for any goods or services that are accessible via third party websites.

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

Users will be solely responsible for all claims, liabilities, damages, costs, and expenses suffered or incurred by the University resulting from said users' use of the ICT facilities in contravention of this policy or any other form of bad faith.

Users of the ICT facilities understand and agree that the University will not be liable 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.

Access to ICT Facilities

Discretional Access

Access to the ICT facilities and University information will vary based on user group, job role, and other considerations.

The University ultimately reserves the right to refuse access to ICT facilities and information resources where it considers that such access poses an unacceptable level of security risk.

Personal Use

ICT facilities are provided to users for University business purposes to support teaching, learning, research, professional, and administrative activities.

Occasional and reasonable personal use of the facilities is acceptable. However, University business purposes of ICT facilities take priority over any personal use. Users shall ensure personal use does not:

1. contravene the primary purpose of the facilities,
2. interfere with, conflict with, or take priority over the performance of University duties,
3. waste resources,
4. deny or impair the service to other users, or
5. have a negative impact on the University, its reputation, or other users.

Administrative Access

Certain professional functions within the University require elevated level of access to ICT facilities.

Where users have been provided with administrative accounts separate to their normal user account, such administrative accounts must:

1. Only be used for carrying out administrative functions
2. Not be used for web browsing
3. Be secured with multi factor authentication

Protecting University Information and ICT Facilities

The University needs to implement technical and procedural controls to protect its ICT facilities as well as the data and well-being of its staff and students. These protective measures must not be disabled, bypassed, circumvented, or reconfigured. You must not prevent the timely installation or re-configuration of security controls. These protective measures include:

1. The presence of host-based software agents on University systems that monitor and protect systems, data, and users from malware and malicious activity.
2. Network monitoring capabilities to detect malicious activity.
3. Multi-Factor Authentication (MFA) which may require, by the user, the installation of an application or receipt of a message on a personal device (typically a mobile phone) to confirm the user's identity when accessing ICT facilities.
4. Access controls to restrict the use of removable media to prevent the spread of malware or the theft of data through USB keys and other removable media. Various levels of flexibility may be assigned depending on your job or academic requirements, but these should not be exceeded without authorisation.
5. The blocking of unauthorised communication, file sharing, and other websites and/or protocols.
6. Unless specifically authorised, users are not to have local administrative privileges on University issued systems.

University Email

Staff and Associate Email

When provided, University of Salford email accounts should be used as the primary mechanism for email communication with the University and for University duties by staff and associates.

Student Email

Students should endeavour to use their university email addresses whenever possible for any university function. Any non-automated requests for services or support through the help desk should be performed via University email or over the phone with the Service Desk.

Alumni Email

The provision of an Email for Life account for each alumnus is at the discretion of the University. Where provided, Alumni email is subject to the following conditions:

1. Alumni Email for Life accounts may be terminated immediately at any time and without prior notice 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.
2. Email for Life accounts may be terminated if they have not been accessed for 90 or more days (or any shorter period which the University may notify to alumni).
3. The contents of Email for Life accounts that are terminated will be irretrievably deleted. The University will not be held liable for any loss of alumni data resulting from such deletion.

Wi-Fi Access

University issued and managed devices are configured to use the on-Campus Wi-Fi.

Guest Wi-Fi access is provided for use by guests, visitors, and students to access the internet. Staff and associates may use the guest Wi-Fi on their personal devices.

Personal devices that are suspected to be infected with malware, are consuming excessive Wi-Fi resources or are otherwise being used in an unsecure or inconsiderate manner may be removed from the Guest Wi-Fi network without notice and may be prevented from reconnecting to the network until assurance can be given that the activity of concern has been addressed.

User Responsibilities

General Behaviour

Users are responsible for all activity performed under their user username.

Users must:

1. Lock their computer's screen using the CTRL-ALT-DEL or WINDOWS-L key combinations (or the equivalent for non-Windows systems) whenever it is left unattended. University computer accounts must not be left unlocked, logged-in, and/or unattended in a way that risks unauthorised access to the account, system, or information displayed on screen.
2. Not permit unauthorised persons, including family members, to use University equipment
3. Shutdown or restart their devices regularly, and at least once per week, to allow security updates and configuration changes to be applied.
4. Schedule communication intensive operations such as large file transfers, for outside working hours.
5. Undertake security awareness training and familiarise themselves with security communications shared on the Hub or by email.
6. Follow security guidance and instructions given by or on behalf of the Information Security team.

User Account

Users must:

1. Be responsible for their University ICT accounts and not share access or credentials to these accounts. Passwords must be changed as soon as possible if the user suspects the password is compromised.
2. Follow Digital IT password complexity standards, as published on the Hub, on any system that supports them.

The selling of credentials or deliberately allowing your credentials to be used for malicious or unauthorised purposes is expressly forbidden.

Use of Personal Devices

Users must:

1. Ensure personal devices used to access University systems and information have access controls such as passwords, PIN codes and biometrics like those used on University (Digital IT) issued devices.
2. Ensure personally owned devices used to access University systems or data have up to date and patched operating system and active anti-virus protection.

Email, Web and Social Media

Users must:

1. Be vigilant with regards to phishing emails requesting credentials or other information. If you are at all suspicious of files or links do not open or run the files or click the links.
2. Disconnect immediately from any website accidentally accessed that contains sexually explicit or offensive material.
3. Take care to ensure use of social media, whether personal or work related, does not negatively impact on the reputation of the University, its staff, students, alumni, or partners.
4. Follow the Social Media Guidelines published on the Hub.

Physical ICT Devices and Clear Desk

Users must:

1. Use reasonable care and security measures to prevent loss or theft of IT equipment and information. Do not leave IT equipment or files unattended in a public area. Keep them in a secure access-controlled area when not in use and avoid leaving sensitive information unattended on your desk.
2. Notify the Digital IT Service Desk of University IT equipment changes related to office moves, role changes, or any other reason.
3. When traveling with IT equipment. ensure devices, including laptops, are placed in the boot of the vehicle before the start of the journey. Precautions are to be taken when re-fuelling or taking breaks to prevent devices being stolen from the vehicle.

Data Handling and Storage

Users must:

1. Understand the sensitivity 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.
2. Ensure data is adequately protected in storage and in transit. This will include the use of encryption where appropriate.
3. Where possible, use University provided or approved storage (on-premise shared drives and cloud storage) to store University data.
4. Not store University information in cloud storage facilities not specifically approved by the University's Digital IT department. This typically means using the University's Microsoft 365 services. Instances of prohibited storage include personal drives such as Google drive, Dropbox, and iCloud.
5. Obtain authorisation from the System Owner and Data Owner before University information is transferred outside the University or extracted from University managed storage and/or systems. Where data is extracted or transferred outside the University users must ensure it

is the minimum information necessary, is temporary and is deleted as soon as the information is no longer required.

6. Not transfer University information through file transfer facilities not specifically approved by the University (Digital IT). This typically means using the University's Microsoft 365 services. Instances of prohibited file transfer facilities include, but are not limited to WeTransfer, TransferNow and WeSendit.

Remote Working

Users must:

1. Ensure they take the necessary precautions when working from remote / off campus locations and processing University data, including but not limited to:
    a. Being aware that using personally owned mobile devices to carry out University work can create risks including, data protection issues, vulnerability to virus infection or malware, and unintentional or unlawful compromise of data.
    b. Where possible, use University issued computers/devices to access and process University information from remote locations. Ensure equivalent protections are in place when non-University devices are used.

Leaving the University

Users must:

1. Return all University IT equipment to Digital IT at the end of employment, contract, or use period.
2. Irreversibly delete University information from any personally owned IT equipment before leaving University employment or when selling, transferring or disposing of the device. Note that simply deleting files typically does not render them unrecoverable. Contact Digital IT for advice on thoroughly deleting or sanitising data/drives. You will be held liable for any University data leaked through your personal device.

Unreasonable Use of ICT Facilities

The following uses are explicitly defined as unreasonable use of the University's ICT facilities. Users must not:

1. 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 Microsoft Corporation.
2. Sell, redistribute, repurpose, or dispose of any part of the ICT facilities belonging to the University without explicit authorisation and only if doing so is part of the individual's job role.
3. Carry out activities that unreasonably waste network or computing resources, deny ICT facilities to authorised users, or continue to carry out activity after a designated Digital IT authority has requested that use ceases.
4. Deliberately or intentionally receive, access, create, change, store, download, upload, share, use, transmit, or otherwise facilitate:

a. Any terrorist related or extremist material, or any data capable of being resolved into such material as per 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. Anyone witnessing such material should report it to University authorities.
b. Any illegal, obscene, or indecent images, data or other material, or any data capable of being resolved into such material. Anyone witnessing such material should report it to University authorities.
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, deliberately causing offense, 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); 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.
g. Any 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. Falsify emails to make them appear to have originated from someone else or send anonymous messages without clear indication of the sender.
6. Carry out activities that criticise or harm individuals or that violate the privacy of other individuals.
7. Deliberately or unintentionally attempt to circumvent the University's ICT facility controls and policies through VPNs, TOR, or any other technical or non-technical method, or access any University system by circumventing the network authentication processes
8. Gain or attempt to gain unauthorised access to non-University ICT facilities.
9. Carry out unauthorised modification to the University's ICT facilities.
10. Connect any non-approved or personally owned ICT equipment to the University physical (wired) network points without written authorisation of Digital IT Services (via the Digital IT Service Desk).
11. 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.
12. Install any software without authorisation of Digital IT (via Digital IT Service Desk).

Reporting Security Problems

Any technical problems, requests, or concerns regarding a suspected breach of this policy should be reported as quickly as possible to the Digital IT Service Desk.

Report loss/theft/breach of University information or IT equipment to the Digital IT Service Desk immediately. The Service Desk will advise you of any actions you may need to take.

You should report phishing and spam emails by clicking the 'Report Message' button in Outlook. This will delete the email and report the email to Digital IT.

Policy Enforcement and Monitoring

Networks, computers, internet usage and email usage may be monitored, and usage logged. The University may inspect all files stored on any University issued or managed devices, and monitor communications to determine the existence of facts, detect unauthorised use of its ICT facilities and to confirm that policies are being followed and the law isn't being broken.

Breaches of the ICT Acceptable Use Policy may be investigated by Digital IT, relevant School or Professional Service in line with the appropriate University disciplinary policy. The initiating School or Professional Service will be responsible for communications with the user and should make it clear to the user under which policy action is being taken. Sanctions for violations of the ICT AUP may include:

1. Suspension or withdrawal of University ICT facilities.
2. Disconnection, seizure, and inspection of any ICT equipment that is in violation of this policy.
3. 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.
4. 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).

Policy Exceptions

Where an exception to this Policy is required, the request should be made following the Security Exceptions Process. We recommend first contacting the Digital IT Service Desk in case solutions that may meet your requirements are already in place.

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.

The undersigned confirms to have read, understood the ICT Acceptable Use Policy V7.0 and agrees to abide by its terms and the possible disciplinary action(s) listed should they violate said policy.

Name (in block letters):	
Signature:	
Date (DD-MM-YYYY):	

It is strongly suggested to keep a copy of the latest ICT Acceptable Use Policy for personal reference.

Document Control

Document History

Version	Date	Reason for change	Author
5.0	20/12/2019	New document	Greg Van der Gaast
6.0	13/07/2021	Updated to reflect updates to framework approach	Adam Clayton
7.0	11/05/2022	Restructured and minor grammatical changes to make more readable. Added sections on administrative access, general behaviours, and wi-fi use. Made monitoring capabilities more explicit	Adam Clayton

Approvers

Name	Role	Date
Adam Clayton	Head of Information Security	22/06/2022
DIT Executive	DIT management	21/06/2022
Melanie Horrocks	Data Protection	21/06/2022
	Human Resources	21/06/2022