IT01 - Information Technology (IT) Acceptable Use Policy

Introduction

1 This policy applies to all use of University IT services by students, staff and third-party individuals who have been given access for specific purposes. The term University IT services refers to all computing, telecommunication, and networking services owned, leased, hired or otherwise provided by Solent University; whether these services are provided or arranged by Information and Communications Technology (ICT), by Faculties/Schools, or by other Professional Services.

2 It is the responsibility of each individual user to ensure that their behaviour and activities when using University IT services is in accordance with all University policies and current legislation.

3 University IT services may be withdrawn from individuals and disciplinary action may be taken if the terms of this policy are not observed. Where appropriate, breaches of the law will be reported to the authorities.

Acceptable Use

4 University IT services are provided to support teaching, learning, research, administration and approved business activities of the University. University IT services must be used responsibly, in accordance with the law and not bring the University into disrepute.

5 Occasional and limited personal use is permitted but such use is a privilege and not a right. See Appendices A and B for guidance on acceptable and unacceptable personal use.

6 If, for legitimate teaching or research purposes, access is required to material normally deemed as unacceptable (see Appendix B for examples) then a request for such access must be made by the relevant Dean/Director/Head of Faculty/School to, and approved by, the Director of Digital Transformation (or appropriate deputy).

Unacceptable Use

7 Unacceptable use includes:

i any illegal or unlawful activity.

ii unauthorised use of IT services.

iii any activity or behaviour which compromises security.

iv any activity or behaviour which adversely affects IT services.

v any activity or behaviour which adversely impacts on the University.

vi any activity or behaviour likely to draw people into terrorism or extremist ideologies. This is a requirement of the University's statutory duty (PREVENT) under section 26 of the Counter-Terrorism and Security Act 2015.

8 Examples of unacceptable use of University IT services are given in Appendix B.

User Responsibilities

9 If you discover or suspect a breach of University IT policy then you must report it as soon as possible to the ICT Service Desk or IT support staff (who must then inform the ICT Service Desk). Any inappropriate material found on a University computer or University IT service must be left in its original state in order that an investigation into its origin can be conducted by ICT.

10 If you believe that you have received a phishing email/message in Microsoft Outlook/Teams then please report it as 'Phishing' using the built-in "Report as" functionality within Microsoft Outlook/Teams. If you have engaged with a phishing email/message - replied to it, forwarded it, clicked on any links in it, or opened any attachments – then you must report it as a suspected information security incident.

11 Suspected or actual information security incidents must be reported as soon as possible, by completing the Information Security Incident Notification form and emailing it to InfoSec@solent.ac.uk. More guidance can be found in the Information Security Incident Management Policy.

12 If you become aware of or suspect a personal data breach then you must report it immediately to Information Rights (Information.Rights@solent.ac.uk or 023 8201 3229). This is to minimise any potential damage to the University (including reputational) and to reduce the risk of heavy legislative fines. Note that a personal data breach under the General Data Protection Regulation (GDPR) is defined as a '*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.

13 You are responsible for the security of any University IT accounts allocated to you. You should not, under any circumstances, allow anyone else to use University IT accounts that have been allocated to you on a personal basis.

14 Where possible, all passwords must meet the following minimum requirements:

i Passwords for regular user accounts must be at least 12 characters long.

ii Passwords for administrative accounts or user accounts with administrative privileges must be at least 15 characters long.

15 Your University password must:

i Be changed by you immediately on first use, if possible, from any default or temporary password provided to you by the University.

ii Be kept confidential and never disclosed to anyone else, not even to University IT staff.

iii Never include personal information or anything that could be easily guessed, including your account username or famous quotations.

iv Never be, or include, just a single word from a dictionary, or include words where knowing part of the password would allow someone to guess the rest of the password.

v Never have been used by you before, including personal accounts you use outside of the University.

vi Never be used as your password for personal accounts you use outside of the University.

vii Be protected, where possible, by the University's multi-factor authentication service.

16 If you believe that your password is known by someone else then you must change it immediately.

17 The University provides a self-service system for users to change their password and Multi-Factor Authentication details. It can be accessed via the following link:

https://myaccount.microsoft.com/

18 Generally, the longer the password then the more secure it is. Using a combination of words to make the password longer can make the password more resistant to common attacks, especially if those words are random, misspelt, use a mixture of upper/lower-case characters and are used in conjunction with numeric and/or special characters (as found on a standard keyboard).

19 You must not include your password in any automated logon process unless it is appropriately encrypted against discovery and misuse. For example, using a password manager with a master password that is at least 16 characters long.

20 You should ensure that any computing equipment you use has appropriate security protection:

i For mobile computing equipment (supplied by the University or your own personal device), please ensure that it is appropriately secured against theft and unauthorised use (e.g. password/PIN protected and data storage encryption).

ii For University computing equipment provided for staff use, if you are leaving it unattended (even for a short period of time) then you must either log off your session or lock the session until you return.

iii For University computing equipment provided for student use, you must log off if you are leaving it unattended.

iv Log off or use the computer shutdown option when your session is finished. Do not just switch off the equipment.

21 You must not use any technologies which directly or indirectly interfere with the University's services or are designed to bypass University policy.

22 Where facilities exist for users to upload a photograph of themselves to a University IT service, please be aware that the image will be seen by all University users and should be consistent with representing the University. If you decide to upload an image then the image must adhere to the following guidelines:

i the image must be clear and in focus.

ii the majority of the image must be a close-up of the user's full head and shoulders with them facing forward and looking at the camera.

iii you must be clearly recognisable in the image.

iv the image content must not contravene any aspect of University Policy.

23 If you have uploaded a photograph of yourself to your Microsoft 365 profile then that profile image will be visible to other users of the University's Microsoft 365 service which may include partner organisations. The Microsoft 365 profile image will not be visible to anyone outside of the University's Microsoft 365 service unless you have:

i created and included a Business Card as part of your email signature.

ii used the Outlook Social Connector (or similar) to link your Outlook account to social media.

iii accepted an external contact request via Microsoft Teams.

24 If you use a personally owned device to access University IT services then you must ensure that their usage is compliant with all University policies. All such devices must be running an operating system version in support by the operating system's manufacturer, not jailbroken/rooted, kept up-to-date with all available security updates for the underlying hardware (BIOS/firmware updates), operating system and all installed applications/apps and, where possible, must use:

i a device password (or equivalent) which is not easily guessable.

ii up-to-date anti-virus/anti-malware software configured to update on at least a daily basis, or only run apps downloaded from the Google Play or Apple App store.

iii data storage encryption.

25 The use of personally owned devices by staff for University business purposes should be avoided. Staff must not use personally owned devices to store any University data that is sensitive, personal, confidential or of commercial value, unless those applications/data are protected by the University's Mobile Application Management service.

26 Some University IT services mandate the use of the University's Mobile Application Management (MAM) service before the IT service can be accessed. By agreeing to use this MAM service on personally owned devices you authorise the University to remotely manage university apps/data on your device in order to secure its usage of University IT services. If deemed necessary by ICT this may include the remote wiping of University data and applications from your device. The University

accepts no liability if personally owned data and/or applications are lost as part of this process.

Allowing and Disallowing Access to IT Services

27 Information from the HR/Payroll systems and affiliate user systems is used by ICT to automatically create and close staff and affiliate accounts. Associated passwords are issued directly to the end user or via Faculty/School/Service administration.

28 Student accounts are created automatically after enrolment of the student and remain active until the end of the course or receipt by ICT of notification of withdrawal. Student passwords are issued in accordance with the current procedures.

29 Student accounts may be automatically locked as part of sanctions applied in line with the Student Debtor Policy.

30 Accounts may be locked or have their access to University IT services restricted by authorisation of the Director of Digital Transformation (or appropriate deputy). The reasons for account restrictions include (but are not limited to) the account holder contravening any University policy, or suspected account compromise by a third-party.

31 Accounts will not be deleted purely on the instructions of the individual who is leaving. It is the responsibility of the appropriate line-manager to identify and protect any important business information stored and managed by the person leaving. Centrally controlled accounts will on the departure of a member of staff be disabled, and any associated files or emails kept for a period of 56 days. It is therefore essential that action be taken immediately upon receiving notification of leaving to identify and secure all information at risk of being lost. If required, ICT will work with Faculties/Schools/Services to assist with moving data to a suitable location. Such requests must be made by the appropriate Dean/Director/Head of Faculty/School/Service to, and approved by, the Director of Digital Transformation (or appropriate deputy).

32 Once a user has left employment or study with the University then they have no legal right to continue to use any accounts on the University's computer systems that had been allocated to them, such as email. Additionally, licensing restrictions may forbid such access. Any request to extend account access beyond the end of employment or study must be made by the appropriate Dean/Director/Head of Faculty/School/Service to, and approved by, the Director of Digital Transformation (or appropriate deputy).

Monitoring, Auditing and Administrative Access

33 All usage of University IT Services by any user is logged and may be subject to monitoring. Subject to UK legislation, the University reserves the right to inspect at any time and without notice all data stored in or transmitted by University IT Services for the following purposes:

i Ensuring effective service operation.

ii Ensuring service usage is compliant with University policy.

iii Detection and prevention of security vulnerabilities.

iv Investigation or detection of unauthorized use of IT facilities.

v Prevention or detection of criminal activities.

vi Fulfilling other legal duties, such as responding to Data Subject Access Requests.

34 Only ICT system administrators or cyber security staff authorised by the Director of Digital Transformation (or appropriate deputy) are permitted to conduct monitoring. Any knowledge thus obtained will not be communicated to others, unless required for system administration purposes or an infringement of University policy is discovered.

35 Audit logs will be retained in accordance with the ICT retention schedule.

36 Any requests for investigation of the usage of a named individual's account must be made by the relevant Dean/Director/Head of Faculty/School/Service to, and approved by, the Director of Digital Transformation (or appropriate deputy).

37 ICT will endeavour to maintain privacy of users' data. However, there may be special cases where it is essential that data is accessed due to, for example, illness of the owner. In these instances, on the request of the relevant Dean/Director/Head of Faculty/School/Service to, and approved by, the Director of Digital Transformation (or appropriate deputy), ICT system administrators will attempt to locate and make available the specific data requested for access by a nominated member of staff. The owner of the data will be notified in due course.

38 ICT reserves the right to take special actions in administering users' data if this is essential to preserve the integrity or functionality of the system. This may include the deletion of users' data.

39 If the University is apprised of content on University IT services that is in breach of the law or University Policy then the University will follow its procedures and will take all reasonable steps to remove or deny access to it.

Third-Party Access

40 The University's Internet connections are provided by Jisc. It is not permitted to provide access for third parties without the prior agreement of ICT.

Off-Site Access

41 Off-site access is provided for specific University IT services. Such services are limited for licensing or security reasons. Only authorised ICT services are allowed to be used to remotely access the university network.

Personal and Shared Data Storage

42 The University provides both personal and shared data storage for storing content for University-related work/study use. An example of personal storage is your allocated OneDrive for Business site and examples of shared data storage include the network-mapped drives, Solent Online Learning, and the University's

SharePoint Online sites (such as Solent Drive and file storage in Microsoft Teams sites).

43 University-provided personal storage should be used for storing University-related work/study content where only you require access to that content or for occasional, ad hoc, sharing of that content with others. If you are sharing University-related work/study content with others on more than an occasional, ad hoc, basis then appropriate University-provided shared data storage must be used instead.

44 University data that is sensitive, personal, confidential or of commercial value must only be stored on University-approved data storage. It is the user's responsibility to ensure that data on University-approved data storage is not transferred to unapproved data storage. Users must be particularly careful with any use of automated file synchronisation technology.

Legal Compliance

45 It is the responsibility of each individual user to ensure that they do not break the law when they use University IT services. Examples of the key areas of legislation are, but not limited to, the following:

i The Computer Misuse Act 1990 (amended by the Police and Justice Act 2006).

ii The Copyright, Designs and Patents Act 1988 and The Copyright (Computer Programs) Regulations 1992.

iii The General Data Protection Regulation and the Data Protection Act 2018.

iv The Freedom of Information Act 2000.

v The Defamation Act 1996.

vi The Obscene Publications Act 1959 (amended by the Obscene Publications Act 1964).

vii The Criminal Justice and Immigration Act 2008.

viii The Communications Act 2003 and The Privacy and Electronic Communications (EC Directive) Regulations 2003.

ix The Equality Act 2010.

x The Counter-Terrorism and Security Act 2015.

xi The Investigatory Powers Act 2016.

xii The Human Rights Act 1998.

Other Sources of Information

46 Other University IT policies:

i IT02 – IT Security Policy.

ii IT03 – Internet Usage Policy.

iii IT04 – Email and Instant Messaging Usage Policy.

iv IT05 – Telephone and Mobile Phone Usage Policy.

v IT06 – IT Hardware and Software Policy.

vi IT07 – Disposal of IT Equipment and Media Policy.

vii IT08 – Application Systems Policy.

viii IT09 – Identity Management Policy.

ix Information Security Incident Management Policy.

https://students.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines

https://staff.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines&department-owner=information-and-communications-technology

47 Other University policies, including but not limited to, the following:

i University Ethics Policy.

ii General Data Protection Regulation (GDPR) Policy.

iii Freedom of Information Policy.

iv Confidentiality Markers Policy.

v Records Management Policy.

vi Disciplinary Procedure Policy.

vii Management of Information Policy.

viii Web Publishing Policy.

ix Student Debtor Policy.

https://students.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines

https://staff.solent.ac.uk/documents?document-type=strategy-policies-procedures-and-guidelines

48 The University's Internet connections are governed by Jisc's network and technology policies:

https://community.jisc.ac.uk/library/janet-policies

Appendix A – Personal Use of University IT Services

49 The use of University IT Services for personal purposes must not:

i conflict with University Policy.

ii directly or indirectly interfere with the University's systems or burden the University with any incremental costs.

iii be for any personal, commercial or monetary gain.

iv conflict with the University's objectives or interests.

v conflict with an employee's obligations to the University as their employer.

vi be used for private confidential correspondence.

vii have a negative impact on the University or other users.

50 Subject to the above, occasional personal use of University IT services is allowed but it must not be excessive or interfere with one's duties, the work of others or other users' access to University IT services. Examples of acceptable use are as follows:

i Occasional, limited, personal use of the University email or instant messaging systems. Such messages must be clearly marked as "Personal".

ii Recreational use of the Internet by a member of staff at agreed break times or outside their normal work hours.

iii Recreational use of the Internet on a University computer in an open-access area during off-peak times when neighbouring computers are freely available for use by other users.

iv Storing non-work or non-study related content for access by yourself only on University IT services designated for your personal work or personal study use. Such storage must not be excessive in comparison to your stored work or study content, it must not infringe copyright or data privacy legislation and it must be stored under a folder marked "Personal". The University cannot be held responsible for any loss to such content, and it may be removed without prior notice if its storage contravenes University Policy. The user will be notified in due course.

Appendix B – Unacceptable usage

51 The University reserves the right to block, disconnect or otherwise prevent any usage of University IT services which it considers unacceptable. Unacceptable usage includes, but is not limited to, the examples given below. Please also see Appendix A for examples of unacceptable personal usage.

52 University IT services may not be used for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities:

i creation, access, attempted access, storage, transmission or downloading of any terrorist related or extremist material. The definition of such material is as defined by the Home Office.

ii creation, access, storage, transmission or downloading 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.

iii creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

iv creation or transmission of material with the intent to defraud, including attempting to disguise the identity of the sender/origin of an electronic communication.

v creation or transmission of defamatory material.

vi creation, access, storage, transmission or downloading of material such that this infringes the copyright of another person/institution or infringes the copyright laws of the UK and/or other countries.

vii transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is authorised and relates to the academic or administrative activities of the University or the Students Union and/or embedded within, or is otherwise part of, a service to which the user has chosen to subscribe.

viii deliberate unauthorised access to networked facilities or services, including unauthorised access to unsecured or unattended network equipment.

ix deliberate or reckless activities having, with reasonably likelihood, any of the following characteristics:

a wasting staff effort or University IT resources, including time connected to accessible systems and the effort of staff involved in the support of those systems.

b corrupting or destroying other users' data.

c violating the privacy of other users.

d disrupting the work of other users.

e any form of denial-of-service attack.

f continuing to use an item of software or hardware after it has requested that use cease because it is causing disruption to the correct functioning of University IT services or any connected network service.

g the introduction of computer “viruses” or other harmful software or hardware, including, but not limited to, packet-sniffing and key loggers.

h unauthorised use of another user’s logon credentials.

i unauthorised network port or vulnerability scanning.

j unauthorised remote access of any equipment.

53 Examples of unacceptable activities or behaviours which adversely impact on the University include, but are not limited to, the following:

i committing the University to a contract unless officially authorised to do so.

ii any activities that compete with the University in business.

iii the creation or transmission of material that brings the University into disrepute.

iv the representation of any views and opinions held personally by the user as the views of the University unless the user is explicitly authorised to do so.

v unauthorised transmission to a third party of confidential material concerning the activities of the University.

vi activities that unfairly criticise or misrepresent others.

vii the registration of any domain name which includes the name of Solent University or any similar name which may mislead users of that domain into believing the domain name refers to Solent University.

54 Examples of unauthorised access to IT services include, but are not limited to, the following:

i allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the University’s IT services.

ii modifications to any University network, including the connection of networking hardware to the University network, made without the knowledge and authorisation of networking specialists within ICT.

Author(s):	Keith Baker, ICT Security and Standards Manager
Approved by:	Gareth Roberts, Director of Digital Transformation
Date of approval:	29 April 2024
Version:	6.0
Next review date:	September 2025