IT01 - Information Technology (IT) Acceptable Use Policy

Introduction

1 This policy applies to any user (staff, students and guests) of all IT services located at or administered by Solent University. The University's IT services are coordinated and managed by Information and Communications Technology (ICT).

2 It is the responsibility of each individual user to ensure that they use University IT services in an acceptable manner 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3 University IT services may be withdrawn from individuals and disciplinary action may be taken if the terms of this policy are not observed. In severe cases, the Police may be notified.

Acceptable Use

4 University IT services may be used for any legal activity to support teaching, learning, research, administration and approved business activities of the University.

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 Head of School to the Head of IT and Library Services (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 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 any user discovers or suspects a breach of University IT policy then they 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 any user becomes aware of or suspects a breach of University IT security then they must report it as soon as possible to the ICT Service Desk. This is to minimise any potential damage to the University (including reputational) and to reduce the risk of heavy fines. For example, fines up to £20,000,000 for breaches of the General Data Protection Regulation or the Data Protection Act 2018. Where deemed necessary (for example, in the event of a data breach) the ICT Service Desk will send this information to the Data Protection Officer.

11 Users are responsible for the security of any University accounts allocated to them. Accounts must not be used by anyone except the allocated account holder. Users must keep their passwords confidential and not disclose them to others, including to University IT staff, or attempt to obtain or use anyone else's account logon details. If users believe that a password to one of their allocated accounts is known to others then they must change that password immediately.

12 Users must treat any password provided to them as temporary and change it on first use. An online password self-service system is available to change the regular University password (as used for logging on to University computers and most University web services) and can be accessed via:

https://www.solent.ac.uk/password

13 Users must follow good security practices in the selection and use of passwords/passphrases. Passphrases are composed of a sequence of words or text so are, generally, preferable to passwords as they are longer in length. All users must adopt the following guidelines for allocating and managing their passwords/passphrases.

i Choose something that is easy to remember by you and you can type accurately.

ii Avoid basing passwords/passphrases on anything that could be easily guessed by someone who knows you or obtained publically.

iii For passwords, avoid words contained in a dictionary.

iv For passphrases, avoid famous quotations.

v Where possible, passwords must have a minimum length of eight characters, using characters selected from at least three of the following categories:

a English uppercase letters (A to Z);

b English lowercase letters (a to z);

c Digits (0 to 9);

d Non-alphanumeric for example: ! , $ ^ or).

vi Select passphrases with a minimum of 14 characters and, ideally, using characters selected from at least three of the categories defined for passwords (as above).

vii For privileged/administrative accounts, allocate unique passwords/passphrases with a minimum length of 14 characters using characters selected from at least three of the categories defined for passwords (as above).

viii Avoid keeping a paper record of passwords/passphrases, unless this can be stored securely.

ix Passwords/passphrases must not contain the account username and must not be passwords/passphrases you have used before on any IT system, including non-University systems.

x Your University password must not be used as the password for accounts on non-University managed IT systems.

14 Do not include passwords/passphrases in any automated logon process, e.g. stored in a script file, macro or function key unless it can be appropriately secured/encrypted against discovery and misuse.

15 Users should ensure that unattended equipment has appropriate security protection:

i For mobile computing equipment, please ensure that it is appropriately secured against theft and unauthorised use (e.g. password protected).

ii For University computing equipment provided for staff use, if you are leaving it unattended 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 when your session is finished. Do not just switch off the equipment.

16 Users must not use any technologies which directly or indirectly interfere with the University's services or are designed to bypass University Policy.

17 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 a user decides to upload an image then the user must be clearly recognisable in the image, the content must not contravene any aspect of University Policy, and 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.

18 If a user has uploaded a photograph of themselves to their Office 365 profile then that profile image will be visible to other users of the University's Office 365 service which may include partner organisations. The Office 365 profile image will not be visible to anyone outside of the University's Office 365 service unless the user has:

i created and included a Business Card as part of their email signature;

ii used the Outlook Social Connector (or similar) to link their Outlook account to Social Media;

iii accepted an external contact request via Skype for Business.

19 Users who use personally-owned devices to access University IT services must ensure that their usage is compliant with all University policies. It is recommended that all such devices use, where possible, a device password (or equivalent) and data storage encryption to prevent unauthorised access.

20 The use of personally-owned devices by staff for University business purposes should be avoided. Staff must not use personally-owned devices to hold any University data that is sensitive, personal, confidential or of commercial value.

21 Some University IT services mandate the use of Mobile Device Management (MDM) software before the service can be accessed. By agreeing to install this MDM software on personally-owned devices you authorise the University to remotely manage 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

22 Information from the People and Development 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 School or Service administration.

23 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.

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

25 Staff or student accounts may be locked or have their access to University IT services restricted by authorisation of the Head of IT and Library Services (or appropriate deputy).

26 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 necessary, ICT will work with Schools and Services to provide access.

27 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 relevant Head of School, Director or Head of Service to the Head of IT and Library Services (or appropriate deputy).

Monitoring, Auditing and Administrative Access

28 All usage of University IT Services (including cloud-based 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.

29 Only ICT staff authorised by the Head of IT and Library Services (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.

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

31 Any requests for investigation in to a named individual’s account must be made by the relevant Head of School, Director or Head of Service to the Head of IT and Library Services (or appropriate deputy).

32 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 Head of School or Director or Head of Service and on the authorisation of the Head of IT and Library Services (or appropriate deputy), ICT may locate and make available the data for access by a nominated member of staff. The owner of the data will be notified in due course.

33 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.

34 If the University is apprised of content on University-administered 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

35 The University's Internet connections are provided by JANET (Joint Academic Network). It is not permitted to provide access for third parties without the prior agreement of ICT.

Off-Site Access

36 Off-site access is provided for specific University IT services. Such services are limited for licensing or security reasons.

Personal and Shared Data Storage

37 The University provides both personal and shared data storage for storing content for University-related work/study use. Examples of personal storage include the u:\ drive and OneDrive for Business and examples of shared data storage include the r:\, s:\ and t:\ drives, myCourse and SharePoint Online.

38 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 should be used instead. University data that is sensitive, personal, confidential or of commercial value must only be stored on University-approved data storage.

Legal Compliance

39 It is the responsibility of each individual user to ensure that they do not break the law. 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;

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 Regulation of Investigatory Powers Act 2000;

xii The Human Rights Act 1998;

Other Sources of Information

40 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.

https://portal.solent.ac.uk/support/official-documents/policies-procedures-guidelines/information-communication-technology.aspx

41 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://portal.solent.ac.uk/support/official-documents/policies-procedures-guidelines/policies-procedures-guidelines.aspx

42 The University's Internet connections are governed by JANET policies:

https://community.ja.net/library/janet-policies

Appendix A – Personal Use of University IT Services

43 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.

44 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

45 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.

46 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 or 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;

47 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.

48 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
Owning committee:	Management Information and Technology Committee
Approved by:	Paul Colbran, Director of ICT
Date of approval:	18 May 2016
Version:	4.1
Next review date:	August 2019