University of Southampton

University of Southampton ISMS: Acceptable Use Policy

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.

Document Control

Title	Acceptable Use Policy
Primary Author	Mark Watts

Version History

Version	Date Issued	Author(s)	Notes
1.0	09/11/2022	Mark Watts	Initial version.
1.0a	31/12/2024	Mark Watts	Update to clause 3.4 to reference 3.3.1(e)

Document Sign-Off

Name	Role	Version	Date	Signature
Wendy Appleby	Vice President Operations	1.0a	31/12/2024	
Mark Watts	Head of Cyber Security	1.0a	31/12/2024	
Sophie Ferguson	Head of Information Governance	1.0a	31/12/2024	

1 Purpose

1.1 This policy forms part of the Information Security Management System (ISMS) of the University of Southampton as part of the University's Information Governance Framework; the set of policies, standards, processes and guidance which define the University's approach to information security.

1.2 This document defines the University's policy towards the acceptable use of the University's digital systems and data. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.3 This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service. The University also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people from being drawn into terrorism.

2 Related Documents

2.1 It is intended that this policy be used in conjunction with other policies published as part of the University's Information Security Management System, in particular the Information Security Policy, which sets out the formal scope for all policies and other documents within the ISMS.

2.2 For further information on the University's ISMS, please refer to the Cyber Security SharePoint site: https://sotonac.sharepoint.com/teams/CyberSecurity/

3 Policy Statements

3.1 This policy is intended to address the requirements of ISO 27001 Annex A objective A.8.1.3:

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

3.2 General Principles

3.2.1 You must use the University's information technology and communications facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues, and students and for the University and in accordance with this policy and the University's other rules and procedures.

3.2.2 In particular, you must abide by the policies comprising the University's Information Security Management Systems (ISMS), of which this policy forms a part.

3.2.3 Information relating to students, staff and the University's affairs must only be held on the facilities and systems provided or authorized by the University and must not be disclosed to unauthorized parties. You must treat our paper-based and electronic information with utmost care.

3.2.4 Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

3.2.5 Particular care must be taken when using digital communications systems (such as email, text messaging, blogging and social media) because all expressions of fact, intention and opinion may bind you and/or the University and can be produced in court in the same way as other kinds of written statements.

3.2.6 Internet-based messaging systems are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent via these systems should demonstrate the same professionalism as that which would be taken when writing a letter.

3.2.7 All digital communications may be subject to disclosure to either the public, via Freedom of Information Legislation, or to individuals, via a Subject Access Request.

3.2.8 You must not use University systems to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If you are in doubt about a course of action, take advice from your supervising line manager.

3.2.9 University systems are provided for academic and business purposes related to work or study at the University. Use of these systems for personal purposes are permitted on the condition that all procedures and rules set out in this policy are complied with, as well as those in the related polices referred to above.

3.2.10 Be aware however that if you choose to make use of our facilities for personal purposes, while the University will respect items marked as ‘personal’ as far as possible, all communications and information held on the University facilities are the responsibility of the University and as such, subject to oversight from the University.

3.2.11 The University reserves the right to undertake monitoring of all activity undertaken on University computing equipment for the purposes of ensuring compliance with activities prohibited in 3.3, as well as preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems. Monitoring of individual usage will be undertaken where it is identified as reasonable, situation specific, minimal and controlled (i.e. in line with an investigation as outlined in 3.5.3 of this policy)

3.2.12 Nothing in this policy shall be interpreted as precluding a member of staff from making a protected disclosure.

3.3 Prohibited Activities

3.3.1 You must not, without the prior authorization of either the Executive Director of iSolutions, Executive Director of Governance, Legal and Strategy Implementation, or their delegates where appropriate, perform any of the following activities on University equipment:

(a) Introduce packet-sniffing, password-detecting, or key-logging software, or perform any other activities related to computer hacking

(b) Seek to gain access to restricted areas of the university's network for which you have not been granted explicit permissions

(c) Unless you have been authorized to do so, access or try to access data which you know or ought to know is confidential

(d) Intentionally or recklessly introduce any form of malware, spyware, computer virus or other potentially malicious software

(e) Intentionally introduce any software related to crypto-currency mining

3.4 For your information, breach of items 3.3.1(a) to 3.3.1(e) (inclusive) above, would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under the Computer Misuse Act 1990, which creates the following offences:

(a) Unauthorised access to computer material i.e. Hacking;

(b) Unauthorised modification of computer material; and

(c) Unauthorised access with intent to commit or facilitate the commission of further offences.

3.5 Misuse of the University's Computer Systems and Networks

3.5.1 Misuse of the University's computer systems and networks in breach of this policy will be treated seriously and dealt with in accordance with the University's disciplinary procedure.

3.5.2 In particular, viewing, accessing, transmitting, posting, downloading or uploading any of the following materials in the following ways, or using any of the University's facilities, may amount to gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

(a) Material, which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;

(b) Offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to the University and any of its staff or bring the reputation of the University and any of its staff into disrepute;

(c) Material related to terrorism or terrorist activities;

(d) Any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;

(e) Any material which, by intent or otherwise, harasses the recipient;

(f) Any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;

(g) Any material which violates the privacy of others or unfairly criticises or misrepresents others;

(h) Confidential information about the University and any of its staff or students;

(i) Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the university);

(j) Material in breach of copyright and/or other intellectual property rights;

(k) Material in breach of any contract undertaken by or on behalf of the University;

(l) Impersonation of another individual or purporting to be representing the University or another administrative entity, whether real or fictitious.

(m) Online gambling; or

(n) Unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

3.5.3 If the University has evidence of the examples of misuse set out above it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

3.6 Exceptions

3.6.1 An exception may be allowed for material that has genuinely been obtained for the purposes of legitimate academic research that is related to your area of study and where the acquisition of such material has been made known to the University in advance.

3.6.2 It is recognised that academics will sometimes need to download material that could fall into one of the categories stated above. A member of staff involved in such research areas would be acting sensibly in making clear his or her intention to download such material and the reasons for this before proceeding, to reduce the possibility of criminal investigation by an external body.

3.6.3 Any potential research involving material which contravenes this policy should be raised with the University's Information Governance and Information Security teams.

3.7 Breaches

3.7.1 If a member of the University community believes they may have encountered breaches of any of the above, they should report this to the University's Legal Services team and/or Executive Director of iSolutions.

3.7.2 If a member of the University community believes they may have encountered a breach of personal data, they must report this within 72 hours of discovering the breach, using the University's Breach Reporting Form: http://go.soton.ac.uk/breach