UNIVERSITY OF PORTSMOUTH

IT ACCEPTABLE USE POLICY

June 2023

Contents

Document title
IT Acceptable Use Policy
Document author and department
Rob Walker Information Services
Approving body
UEB
Date of approval
5 June 2023
Review date
5 June 2024
Edition no.
3
ID Code
051
Date of effect
6 June 2023

Document title	
For a) public access online internet or b) staff only intranet?	b)
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk	

The latest version of this document is always to be found at:

https://policies.docstore.port.ac.uk/policy-051.pdf

Summary

What is this document about?

This Policy sets out what the University of Portsmouth regards as acceptable use of its Information Technology (IT) facilities.

The Policy ensures that all users understand the way in which the University's IT systems and information should be used. This Policy provides clear guidance about what constitutes unacceptable activities using the University's IT equipment or information and which, if misuse is attributed to an individual or a group of individuals, can lead to disciplinary action and/or the immediate cessation of their user access.

Who is this for?

This Policy applies to all staff, students and other users of University IT systems and technology.

How does the University check this is followed?

Subject to UK legislation, the University reserves the right to monitor, scan or otherwise probe its IT facilities, systems and networks, in order to detect potential problems, investigate security issues and maintain and protect an efficient service.

Monitoring will take place within the terms permitted under the Regulation of Investigatory Powers Act (RIPA) 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations) 2000.

The University also reserves the right to inspect any items of computer equipment connected to the University network. Any IT equipment connected to the University's network will be blocked if it is deemed to be in breach of this Policy or otherwise interfering or having the potential to interfere with the operation of the University network.

Who can you contact if you have any queries about this document?

Any questions or concerns relating to the terms or implementation details associated with this Policy should be addressed to the Governance Risk and Compliance Group within Information Services.

Executive summary

The key elements of this Policy are as follows:

• University IT facilities are provided to authorised individuals to support learning, teaching, research, administration and approved business activities of the University.

• The University reserves the right to take appropriate action against those using, or suspected of using, its IT facilities in a manner it decides is unacceptable.

• Any misuse of the system may result in formal disciplinary action and, in some instances, the police or other enforcement authorities may be notified. If a user is subject to University disciplinary procedures or a police investigation, then their access to IT facilities may be blocked.

1. Introduction

The vast majority of students and staff of the University of Portsmouth are conscientious users of IT. However, experience has shown that a small minority of individuals occasionally challenge our expected norms of acceptable use, either deliberately or unintentionally. The purpose of this Policy is to provide guidance on what constitutes 'acceptable use' and 'unacceptable use'.

2. Responsibilities

Responsibility for reviewing and updating this Policy lies with Information Services in conjunction with the Executive Director of Corporate Governance. Line managers have a responsibility to ensure that their staff are made aware of this Policy. Students will be made aware of this Policy through the Student Conduct Policy. All users of University IT facilities are expected to comply with this Policy. Breach of this Policy constitutes a breach of University regulations.

3. Legislation and related policies

Please refer to Appendix 2 for a list of the current legislation and applicable University of Portsmouth policies that have a bearing on the acceptable use of University IT facilities.

4. Scope of the Policy

The principles and obligations described in this Policy apply to all users of University IT facilities, including all staff (permanent, fixed term or temporary), students and third parties having access to University IT facilities in whatever form. University IT facilities include, but are not restricted to:

- Network infrastructure, including the physical infrastructure whether cable or wireless, network servers, firewalls, switches and routers;
- Network services, including internet access, web services, broadband, email, wireless, messaging, network storage, telephony and access control;
- Computing hardware, both fixed and portable, including personal computers, workstations, laptops, tablets, PDAs, mobile devices, smart phones, servers, printers, scanners, disc drives, monitors, keyboards;
- Software and databases, including applications, web applications, virtual learning environments, video-conferencing, language laboratories, software tools, e-library services, electronic journals and eBooks;
- Social networking media or services provided by the University.
- Services hosted in the cloud or provided by a 3rd party as a managed service.

5. Acceptable use

5.1 University IT facilities are provided by the University to authorised users for University purposes – primarily to support teaching, learning and research and to support professional and administrative activities.

5.2 In certain teaching or research activities, staff or students might require the creation of, or access to, offensive material for the purposes of legitimate study or research, for example, in studying racism it might be necessary to look at racist material. In such cases where unusual access is required, this requires the explicit, prior and written authorisation of the relevant Head of Department and Departmental Ethics Committee.

6. Control of IT facilities and monitoring

Subject to UK legislation, the University reserves the right to monitor, scan and block access to its IT facilities, systems and networks; and block access to external web content, in order to prevent potential problems, investigate security issues and maintain an efficient, safe and secure service. The reasons for undertaking such monitoring include:

- Investigating or detecting unauthorised use of IT facilities;
- Detecting security vulnerabilities;
- Preventing or detecting criminal activities;
- Ensuring compliance with University policies;
- Ensuring effective system operation.

The University also reserves the right to monitor and inspect any items of computer equipment connected to the University network. This includes personally owned devices, equipment supplied by the University and equipment supplied under a research grant or award. Any IT equipment connected to the University network will be disconnected if it is deemed to be breaching University policy or otherwise interfering with the operation of the network or having the potential to do so.

7. Unacceptable use

Unacceptable use extends to staff or student behaviour which may impact upon the University by virtue of the association between an individual(s) and the University. Examples of unacceptable use of University IT facilities are given at Appendix 1. This list is not exhaustive.

Unacceptable use of University of Portsmouth IT equipment, services or facilities includes:

- Illegal and unlawful activity;
- Unauthorised use of services and facilities;
- Breach of copyright;
- Compromising security;
- Causing disruption and mischief;
- Negatively affecting the reputation of the University;
- Activities likely to draw people into terrorism or extremist ideologies;
- Misuse of electronic messaging and social media;
- Carrying out unauthorised personal legal and business transactions.

8. Possible consequences of unacceptable use

Violations of this Acceptable Use Policy may be investigated under the University's disciplinary procedure. The following actions may be taken by the University in response to a breach of this Policy:

- Withdrawal of University IT facilities;
- Blocking or limiting network account access;
- Disconnection and seizure of equipment that is in violation of this Policy;
- Initiation of relevant disciplinary procedure for staff or students.

8.1 Where there is evidence of a criminal offence, the matter will be reported to the police. The University will cooperate with the investigating authorities and disclose copies of any relevant data stored, appropriate logs and any hardware used (relevant to the investigation) to the police in line with current legislation.

The Chief Information Officer or the Executive Director of Corporate Governance (or their authorised nominees) may temporarily suspend or otherwise block access from any user of any University IT system where there are reasonable grounds to do so. This applies if there are grounds to suspect that a user has breached this, or any other Policy, pending an investigation.

9. Further information

The Information Systems Services website https://myport.port.ac.uk/guidance-and-support/pc-availability-it-support/account-security

gives further guidance and advice on the use of IT facilities, as well as additional rules and guidelines which may be issued from time to time.

Appendix 1: Some examples of unacceptable use of IT facilities

The University of Portsmouth reserves the right to block, disconnect or otherwise prevent what it considers to be unacceptable use of its IT equipment, services or facilities.

Unacceptable use of University IT facilities includes, but is not limited to, the examples given below.

A. Illegal or unlawful

Several pieces of UK legislation define acceptable computer use, chief amongst these being the Computer Misuse Act 1990. This Act created offences, including using another person's username or identifier (ID) and password without proper authority to access (or attempt to access) data; to alter, delete, copy or move a program or data, or to impersonate another person using email, online chat, web or other services. Subsequent exploration may be illegal if it leads to entry to parts of the system for which access is not authorised.

1. Publishing material or making statements which the University may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene, or offensive or otherwise causing annoyance, inconvenience or needless anxiety.

2. All activities that are illegal or in conflict with University of Portsmouth policies, procedures, processes and regulations.

3. All actions which breach regulations and policies applied to the University by external bodies – including, but not restricted to, the Joint Academic Network (JANET) Acceptable Use Policy.

4. Using University IT facilities for unauthorised personal, commercial or financial gain, or for personal legal and business transactions.

5. Committing the University to a contract unless officially authorised to do so.

6. All activities of a nature that compete with the University in business.

7. All activities that waste staff effort, time or network resources, or deny service to other users.

8. Publishing material or making statements which unlawfully discriminate or which promotes unlawful discrimination.

9. Any activity which is in breach of the University's Data Protection Policy.

10. Disclosure of restricted information relating to his/her employment at the University.

11. Any activity which promotes or encourages acts of terrorism or attempts to draw people into terrorism, terrorist groups, terrorist activities or extremist ideologies.

Note: The UK government has defined extremism as: 'vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces' .

B. Indecent or offensive

The Obscene Publications Act 1959 and 1964 makes it illegal to publish material that tends to deprave and corrupt those viewing it. Under the 1964 Act, it is an offence to possess obscene material with an intention to publish for gain. So no attempt to publish is required for the crime to have been committed. All of this then applies equally to the electronic world.

University IT facilities must not be used for access, creation, modification, storage, download, hosting or transmission of material that could be considered offensive, obscene, pornographic, or otherwise inappropriate .

University IT facilities must not be used for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material. Exceptions to this will require the explicit authorisation of your Head of Department and your Departmental Ethics Committee. Information Services must also be informed.

C. Unauthorised access

It is an offence to use or access another person's account without proper authority. Even if the initial access is authorised, subsequent exploration may be illegal if it leads to entry to parts of the system for which access is not authorised.

12. Unauthorised access (or attempted unauthorised access)to facilities or services provided by the University network or accessible from the University network is not permitted.

13. Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the University's computer facilities; or to carry out unauthorised modification to the University's computer facilities, is not permitted.

14. Connecting any non-approved IT equipment (including wireless access points) to the University network or setting up any network services, without the written permission of the Information Services department is not permitted.

15. Registering any domain name which includes the name of the University of Portsmouth or any similar name which may mislead the public into believing that the domain name refers to the University of Portsmouth is not permitted.

16. Unauthorised transmission, distribution, discussion or disclosure (e.g.on message boards, email or similar media including social media sites) to a third party of any restricted data (i.e. sensitive, confidential or commercially sensitive information) is not permitted .

17. University IT facilities must not be used for outside work by staff, students or third parties, whether paid or unpaid, without the explicit permission of the Head of Department and the CIO.

D. Breach of copyright and IP

Copyright gives the creators of certain kinds of material rights to control the ways their material can be used. These rights start as soon as the material is recorded in writing or in any other way. Copyright applies to any medium. This means that you must not reproduce copyright protected work in another medium without permission.

18 . University IT facilities must not be used to make, use, install, distribute, sell, hire, re-direct or otherwise process any copies of computer software, radio, TV, film or music for any purpose (either here or elsewhere) without licence or without the permission of the copyright owner.

19. You must treat as confidential any information to which you gain access in using University IT facilities and which is not on the face of it intended for unrestricted dissemination.

The UoP Copyright Policy provides further clarification (https://policies.docstore.port.ac.uk/policy-086.pdf)

E. Security

The University operates and maintains vital information processing and communication resources to support teaching and learning. These must be adequately protected so that the integrity and availability of these systems can be assured and the privacy of individual users protected.

20. Attempting to circumvent, remove or thwart University IT security controls is not permitted.

21. Interfering with, or modification or alteration of software, computer configurations, settings, equipment, data files or websites without the written authorisation of the CIO is not permitted.

22. Causing damage to University IT facilities, or moving or removing such facilities without authorisation is not permitted.

23. Downloading, creating or using any program, tool or item of software designed to monitor damage, disrupt or interfere with the functioning of IT facilities, user accounts or data is not permitted.

F. Disruption and mischief

24. Acting in a way which directly or indirectly causes disruption to others' use of University IT facilities, or using University IT facilities to disrupt the use of IT facilities elsewhere is not permitted.

25. Using University IT facilities to defame, harass, offend or hinder another person, by creation, transmission, storage, download or display of materials, or by any other means is not permitted.

G. Electronic messaging

Impersonating another person using email, online chat, web or other services is an offence under the terms of the Computer Misuse Act 1990.

26. Sending anonymous emails or electronic messages or messages that do not correctly identify you as the sender, or messages which appear to originate from another person is not permitted.

27. Intentional transmission of unsolicited or unauthorised commercial or advertising material within the University or to other individuals or organisations is not permitted. Such material includes unsolicited email(spam), chain letters, hoax virus warnings, pyramid letters or other junk mail of any kind.

H. Social media

28. The Marketing and Communications Department have provided more guidance on social media which can be found at:

https://staff.port.ac.uk/departments/services/marketingandcommunications/socialmedia/

Appendix 2: Current legislation and applicable University policies

The key cybersecurity laws that apply in the UK include the following:

- Network and Information Systems Regulations 2018 ("NIS Regulations") (implementing the Network Information Systems Directive 2016/1148 (NISD))
- Communications Act 2003
- Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") (implementing ePrivacy Directive 2002/58/EC)
- Data Protection Act 2018 ("DPA")
- Computer Misuse Act 1990
- Counter-Terrorism and Security Act 2015 (The "Prevent Duty")
- Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 ("UK eIDAS Regulation") (implementing the eIDAS Regulation (EU) 910/2014)

University security policies of relevance:

- UoP Information Security Policy
- UoP Identity and Access Management Policy
- UoP Secure Systems Policy
- UoP Copyright Policy

University of Portsmouth
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3199

E: corporate-governance@port.ac.uk
W: www.port.ac.uk