# ICT Acceptable Use Policy

August 2015

| Document title | | | |
|---|---|---|---|
| ICT Acceptable Use Policy<br>August 2015 | | | |
| **Document author and department** | | | **Responsible person and department** |
| Robbie Walker,<br>Information Security Architect,<br>Information Services | | | Bernie Topham,<br>Chief Operating Officer |
| **Approving body** | | | **Date of approval** |
| University Executive Board (UEB) | | | 13 July 2015<br>16 October 2015: Minor changes made to section 7 and Appendix 3 |
| **Review date** | **Edition no.** | **ID Code** | **Date of effect** |
| August 2018 | 2 | 51 | 1 August 2015 |
| **EITHER**<br>**For public access online (internet)?**<br>*Tick as appropriate* | | | **OR**<br>**For staff access only (intranet)?**<br>*Tick as appropriate* |
| **Yes** ☐ | | | ☐ |
| **For public access on request copy to be mailed**<br>*Tick as appropriate* | | | **Password protected**<br>*Tick as appropriate* |
| **Yes** ☐ ☐ | | | ☐ **No** ☐ |
| External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk<br>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:

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

# Contents

# ICT Acceptable Use Policy

## Summary

### What is this Policy about?
This Policy sets the 'ground rules' for what the University of Portsmouth regards as acceptable use of Information Communications Technology (ICT) facilities.

### Who is this Policy for?
The Policy applies to all staff, students and authorised users of our ICT facilities .

### How does the University check this Policy is followed?
Subject to UK legislation (any monitoring will take place within the terms permitted under the Regulation of Investigatory Powers Act (RIP) 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000), the University reserves the right to monitor, scan or otherwise probe its ICT facilities, systems and networks, in order to detect potential problems, investigate security issues and maintain an efficient service.

The University also reserves the right to inspect any items of computer equipment connected to the network. Any ICT equipment connected to the University's network will be removed if it is deemed to be breaching University policy or otherwise interfering with the operation of the network.

### Who can you contact if you have any queries about this Policy?
The Information Systems Services website **ithelp.port.ac.uk/** gives further guidance and advice on the use of ICT facilities, as well as additional rules and guidelines which may be issued from time to time. Alternatively please email **servicedesk@port.ac.uk**.

## Executive summary

The University allows reasonable personal use of its ICT facilities, subject to the discretionary limits outlined in Appendix 2. The key elements of this Policy are as follows:

- University ICT 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 individuals using, or suspected of using, its ICT facilities in a manner it decides is unacceptable.
- Any misuse of the system may cause the instigation of formal disciplinary procedures and, in some instances, the police authorities may be notified. If a user is subject to University disciplinary procedures or a police investigation, then access to ICT facilities may be blocked .
- All authorised users of University ICT facilities are subject to same laws and policies that apply to other forms of communication.

# 1. Introduction

The vast majority of students and staff of the University of Portsmouth are conscientious users of ICT. 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 University Secretary. 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 Code of Student Behaviour. All users[1] of University ICT 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 3 for a list of the main pieces of legislation and applicable University of Portsmouth policies that have a bearing on the acceptable use of University ICT facilities.

# 4. Scope of the Policy

The principles and obligations described in this Policy apply to all users of University ICT facilities, including staff, students and third parties having access to University ICT facilities in whatever form. University ICT 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 fax services, CCTV, door 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 and pointing devices;
- 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.

# 5. Acceptable use

5.1 University ICT 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. Occasional and limited personal use of University ICT facilities by staff is permitted, but such use is a privilege and not an automatic right. Personal use of University ICT facilities must not hinder or interfere with an individual's contractual or professional duties, and must not prevent the legitimate use of these facilities by others. Examples of acceptable use of University ICT facilities are given at Appendix 1.

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, 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 authorisation of the relevant Head of Department and Departmental Ethics Committee (Appendix 2, section B also refers).

# 6. Control of ICT facilities and monitoring

Subject to UK legislation[2], the University reserves the right to monitor, scan or otherwise probe its ICT facilities, systems and networks, in order to detect potential problems, investigate security issues and maintain an efficient service. The reasons for undertaking such monitoring include:

- investigating or detecting unauthorised use of ICT facilities;
- detecting security vulnerabilities;
- preventing or detecting criminal activities;

1 Users include all staff, students, contractors and third parties with access to University systems.

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

- ensuring compliance with University policies;
- ensuring effective system operation.

The University also reserves the right to inspect any items of computer equipment connected to the network . Any ICT equipment connected to the University's network will be removed if it is deemed to be breaching University policy or otherwise interfering with the operation of the network.

## 7. Unacceptable use

Unacceptable use of University of Portsmouth ICT 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[3];
- misuse of electronic messaging and social media;
- carrying out unauthorised personal legal and business transactions.

Unacceptable use extends to staff or student behaviour which may impact upon the University by virtue of the association between an individual and the University. Examples of unacceptable use of University ICT facilities are given at Appendix 2. This list is not exhaustive.

## 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 ICT 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 student.

Where there is evidence of a criminal offence, the matter will be reported to the police. The University will co-operate 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 Director of Information Services may temporarily suspend the authority of any user of any system where there are reasonable grounds to suspect that a user has breached this Policy, pending an investigation.

## 9. Further information

The Information Systems Services website **ithelp.port.ac.uk/** gives further guidance and advice on the use of ICT facilities, as well as additional rules and guidelines which may be issued from time to time.

3 This is a duty under section 26 of the Counter-Terrorism and Security Act 2015.

# Appendix 1

## Acceptable and reasonable use of ICT facilities

The University allows staff reasonable personal use of ICT. It is important to understand what constitutes reasonable use – both in terms of scale and activity.

For example, reasonable use might include:

1. Personal electronic communications and recreational use of internet services, (e.g. email, instant messaging, micro blogging, online shopping and web surfing). These are permitted, provided that these activities remain within expected norms of behaviour and are not excessive in that they do not interfere with one's duties, or the work of others.
2. Advertising via electronic notice boards, intended for this purpose, or via other University approved mechanisms .
3. Storing non-work related information on University systems – for example, eBooks, music, home videos, photography. Such storage must not be excessive and it must not infringe copyright and data privacy legislation. The University cannot be held responsible for loss, damage, backup or recovery of non-work related information.

# Appendix 2

## Unacceptable and prohibited use of ICT facilities

The University of Portsmouth reserves the right to block, disconnect or otherwise prevent what it considers to be unacceptable use of its ICT equipment, services or facilities. Unacceptable use of University ICT 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 ICT facilities for unauthorised personal, commercial or financial gain, or for unauthorised 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. Staff must not disclose 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 ICT 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.[4] University ICT 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 ICT 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.

4 Exceptions to this will require the explicit authorisation of your Head of Department and your departmental ethics committee. Information Services must also be informed.

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 ICT 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 Director of Information Services.

### 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 ICT 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.

### E. Security

The University operates and maintains a large and extensive networked computer system to support teaching and learning. These vital information processing and communication resources 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 ICT 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 a supervisor, line manager or Head of Department is not permitted.

22. Causing damage to University ICT 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 ICT facilities, user accounts or data is not permitted.

### F. Disruption and mischief

Information systems provide a platform from which communication to your immediate circle of friends, professional peers, or global community is easily achievable. With this power comes responsibility.

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

25. Using University ICT 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/

**It should be noted that the examples of unacceptable use in Appendix 2 are not exhaustive and no attempt has been made to define the items in order of seriousness.**

# Appendix 3

## Other sources of information

**1. Information Services Advisory Publications**

The IS Advisories are subject focused documents, providing clear guidance in support of the Information Security Policy and Acceptable Use Policy. All IS Advisories are approved by the IS Board and available through the IT Help pages at

https://articlehub.port.ac.uk/portal/articles/2711

**2. Other policies and procedures including but not limited to the following:**

- Disciplinary
- Staff Access to University Facilities and Leavers Procedures
- Data Protection
- Safeguarding Policy

**www.port.ac.uk/accesstoinformation/policies/**

**3. External guidelines/legislation**

You must comply with all relevant external guidelines, laws, policies and procedures which affect your use of University IT facilities, including:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright, Designs & Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Counter-Terrorism and Security Act 2015

The University of Portsmouth's network connection is governed by:

- JANET Connection Policy
- JANET Security Policy
- JANET Acceptable Use Policy

University of Portsmouth
Information Services
St Andrew's Court
St Michael's Road
Portsmouth PO1 2PR
United Kingdom

T: +44 (0)23 9284 3348
F: +44 (0)23 9284 3700
E: corporate-governance@port.ac.uk
W: www.port.ac.uk