IT Acceptable Use Policy v1.0

Organisation	Oxford Brookes University
Title	IT Acceptable Use Policy
Creator	Gareth Packham - Head of Information Management
Approvals Required	1. Information Security Working Group 2. CIO 3. Executive Board
Version	Version 1.0
Owner	Chief Information Officer
Subject	The formal, approved, IT Acceptable Use Policy of Oxford Brookes University
Rights	Public
Review date and responsibility	Annually by Head of Information Management

Revision History			
Date	Author	Version Number	Comments
20/09/16	Gareth Packham	0.1 (draft)	Original draft
15/09/16	Gareth Packham	0.2 (draft)	Removal of duplicate sections; clarification of scope and addition of prevent duties and miscellania from General IT Regulations
28/11/16	Benedict Barry	0.3 (draft)	Minor revisions only
10/01/17	Gareth Packham	0.4 (draft)	Minor revisions only
20/03/17	Edwina Towson	0.5 (draft)	Re-ordering and streamlining mainly
31/03/17	Gareth Packham	0.6 (draft)	Minor revisions only
11/04/17	Edwina Towson	0.7 (draft)	Reformatting and minor revisions only
13/04/17	Gareth Packham	1.0 (live)	Transition to live version

1. Policy Objectives

1.1 The principal aims of this policy are to secure the University's compliance with its legal obligations, as an internet service provider, as a licensee and as a publisher, and to protect the value and integrity of the digital information held within or accessed through the University's IT facilities.

1.2 A further purpose of this policy is to provide authorised users of the University IT with a safe and acceptable working environment. The University does not intend to obstruct or limit the use of information without reason but makes rules to establish and maintain good practice and to deliver its policy objectives; this is done for the benefit of the University community as a whole.

1.3 The University possesses and uses computer systems, networks and allied hardware and other peripherals as an integral and pervasive part of its operations. In addition to protecting the considerable investment that the University has made to secure these facilities, the University's ability to function and its good reputation depends on the efficient and full operation of its IT capability; the security and preservation of the University systems and of its digital data are of paramount importance. This policy is part of the governance framework which provides rules for managing the risks arising from complex systems and a large number of users.

2. Scope

The policy applies to Governors, staff, students and other users authorised by the University and taking legitimate access to the University's systems. Examples of such authorised users include visiting academics, consultants whose work for the University requires access to the University's systems, representatives of suppliers engaged in work under their employer's contract with the University and associate staff engaged with the University's higher education or research functions.

3. Provision of service and basic service rules for the use of University IT including confidentiality

3.1 The University provides IT facilities primarily for academic reasons and for the conduct of legitimate University business, not for the purposes of entertainment, shopping or other private use.

3.2 Users must treat information that they access or see via the University's IT systems as confidential, unless the information is clearly intended to be public or disclosable in the context in which it is made available.

3.3 Users must contact the University's IT Services for any change or modification to hardware and software; any such change should be made only by authorised members of the University's staff.

3.4 Users are required to respect the legitimate access to the IT facilities by other users and must not obstruct this or remove or interfere with output created by any other user.

3.5 Users must be considerate when using the University's IT facilities, including keeping noise to a minimum and keeping behaviour to that appropriate to an academic or business setting; in other words, conduct should be quiet and orderly.

3.6 Although the University's IT facilities are provided primarily for legitimate academic and business purposes, the University permits limited personal use of email and of the internet subject to the rules set out in this policy and provided that such use does not conflict with the University's interests, such as the proper performance by staff of their work for the University.

3.7 Access to another person's emails will only be granted with the explicit consent of the University's Chief Information Officer or Chief Operating Officer.

3.8 The ownership of material created via the University's IT facilities is treated in accordance with the University's Intellectual Property Policy (see http://www.brookes.ac.uk/research/policies-and-codes-of-practice/)

3.9 Staff users are restricted in their access to the University's staff-only information systems. Each staff user is granted initial data access as determined by their line manager. Additional access, as required by staff users on a case by case basis, will be subject to the University's Access Control Policy

(http://www.brookes.ac.uk/obis/information-management/policies-procedures-legislation/)

4. Prohibitions and restrictions

Users shall not use the University's IT or network facilities for any of the following (the titles are prompts to assist reference only):

Password and identity integrity

4.1 Revealing any account password (or associated secret authentication information) to others or allowing use by another person, including family and other household members.

4.2 Circumventing user authentication or security of any host, network service or account.

4.3 Impersonating another user.

Hacking and similar misuse

4.4 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network session, via any means, locally or via the Internet/Intranet/Extranet.

4.5 Gaining unauthorized access to, or intentionally damaging, other computer systems, network services or the information contained within them, This includes erasing, altering, corrupting or tampering with any information other than in the legitimate conduct either of University business for staff or for the proper furtherance of academic study for students.

4.6 Executing any form of network monitoring that will intercept data not intended for the user's host.

4.7 Port scanning or security scanning unless being conducted by authorised members of

the University's IT Services (or third parties specifically authorised by IT Services.)

4.8 Introducing malicious programs into the network or server (e.g viruses, worms, Trojan horses, email bombs etc)

4.9 Effecting security breaches or disruptions of network communication. Examples of security breaches are accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Illegality

4.10 Any unlawful activity not otherwise covered. Examples of such unlawful activity include:

a) infringement of intellectual property rights including distributing or obtaining illegally copied software, media or other material
b) breaching another person's privacy
c) Harassment or bullying
d) defamation
e) sending unsolicited advertising or promotional material
f) conducting any corrupt practice
g) fraud
h) theft
i) gambling.

4.11 The creation, transmission, storage, downloading or display of any offensive, obscene, discriminatory (either on the grounds of sex, disability, colour, race, religion or belief, or sexual orientation), indecent, explicit or threatening data or other material (unless such access is necessary) for one or more of:

a) authorized research activity
b) investigatory or disciplinary process
c) whistleblowing
d) cooperation with the Police, Prevent or other official enquiry.

Users should be aware that the University takes its responsibility under the

Counter-Terrorism and Security legislation extremely seriously including those requirements detailed in law and referred to as the "Prevent Duty". Consequently, users must not deliberately create, display, produce, store, circulate or transmit material related to terrorism or extremist ideology in any form or medium except where required for the purposes set out at 4.11 a) to d) above.

Confidentiality including email forwards

4.12 Disclosing any information about, or providing lists of, University staff or students to any party not employed by the University (unless in the course of legitimate University business or authorised by a member of the senior management of the University.)

4.13 Storing any confidential information on any system other than one provided by the University, unless formally approved by the University's IT Services.

4.14 Sending any confidential information online by any means, without utilizing appropriate, approved, security methods. Online communications may be subject to interception by persons outside the University and such interception may not be detectable or perceptible by the user. Any encryption software used should be provided by or approved by the University's IT Services.

4.15 Using an automatic forwarding facility for email which takes email from a University account to an outside network unless, in the case of staff, this has been approved by an appropriate manager. Automatic email forwarding may result in the inadvertent transmission of sensitive information to external email accounts and users should therefore exercise utmost caution when sending any email from a University account to an outside network.

Miscellaneous prohibitions

4.16 Private profit, except to any extent authorized in writing under a user's conditions of employment or other express agreement with the University.

4.17 Connecting any unsecured, internet enable-able device to the University's IT systems.

4.18 Failing to read or adhere to the terms and conditions of any licence agreements relating to the relevant IT facilities including software, equipment, consumables, services, databases, platforms, publications and goods.

5. Monitoring, breach and enforcement

5.1 Although the University respects and appreciates the value of personal privacy, its IT systems are provided for academic and business purposes and users should have no expectation of privacy when using the University's IT facilities.

5.2 Any user becoming aware of any suspected, accidental, or intentional illegal action or misuse must report this immediately to the IT Service Desk or to an appropriate member of staff.

5.3 The University has the right to monitor all usage of the IT, communications and computer systems at any time and without notice. Examples of specific circumstances where the University may choose to monitor are:

a) to ensure the proper working of the systems or to assist troubleshooting
b) to ensure that all users comply with University policies, practices and procedures (including but not limited to this policy)
c) to investigate or detect the unauthorized use of OBU's systems.

5.4 The University may inspect, lock, block, scan, clone or remove any computer or drive or information at any time at its sole discretion.

5.5 Users should be aware that breach of these rules may constitute a criminal offence or result in disciplinary action under either the Student Conduct Regulations or the Staff Conditions of Service.

5.6 The University will cooperate with law enforcement authorities to prosecute offenders.

6. Related policies

6.1 Users accessing social media should refer to the Oxford Brookes University Social

Media Guidelines (available at http://www.brookes.ac.uk/services/hr/handbook/terms_conditions/social_media_guidelines.html)

6.2 Users should also refer to these related policies:

a) Security sensitive material

(http://www.brookes.ac.uk/research/policies-and-codes-of-practice/)

b) Information Security Incident Management Policy

(http://www.brookes.ac.uk/obis/information-management/policies-procedures-legislation/)

c) Access control policy for staff

(http://www.brookes.ac.uk/obis/information-management/policies-procedures-legislation/)

d) Intellectual property policy

(http://www.brookes.ac.uk/research/policies-and-codes-of-practice/)

7. Change procedure and notice of changes

7.1 This policy shall be reviewed at least annually by the Chief Information Officer or his nominee, currently the Head of Information Management.

7.2 Where the Chief Information Officer considers that one or more material changes have been made to the policy, the policy shall be presented to the University's Executive Board as a consultation document.

7.3 The Chief Information Officer is responsible for keeping the policy accessible to users and for bringing changes of significance to the attention of users by whatever means he thinks appropriate.

7.4 Changes to this policy are authorised with immediate effect by the Chief Operating Officer on the advice of the Chief Information Officer whether at a meeting of the University's Executive Board or otherwise.