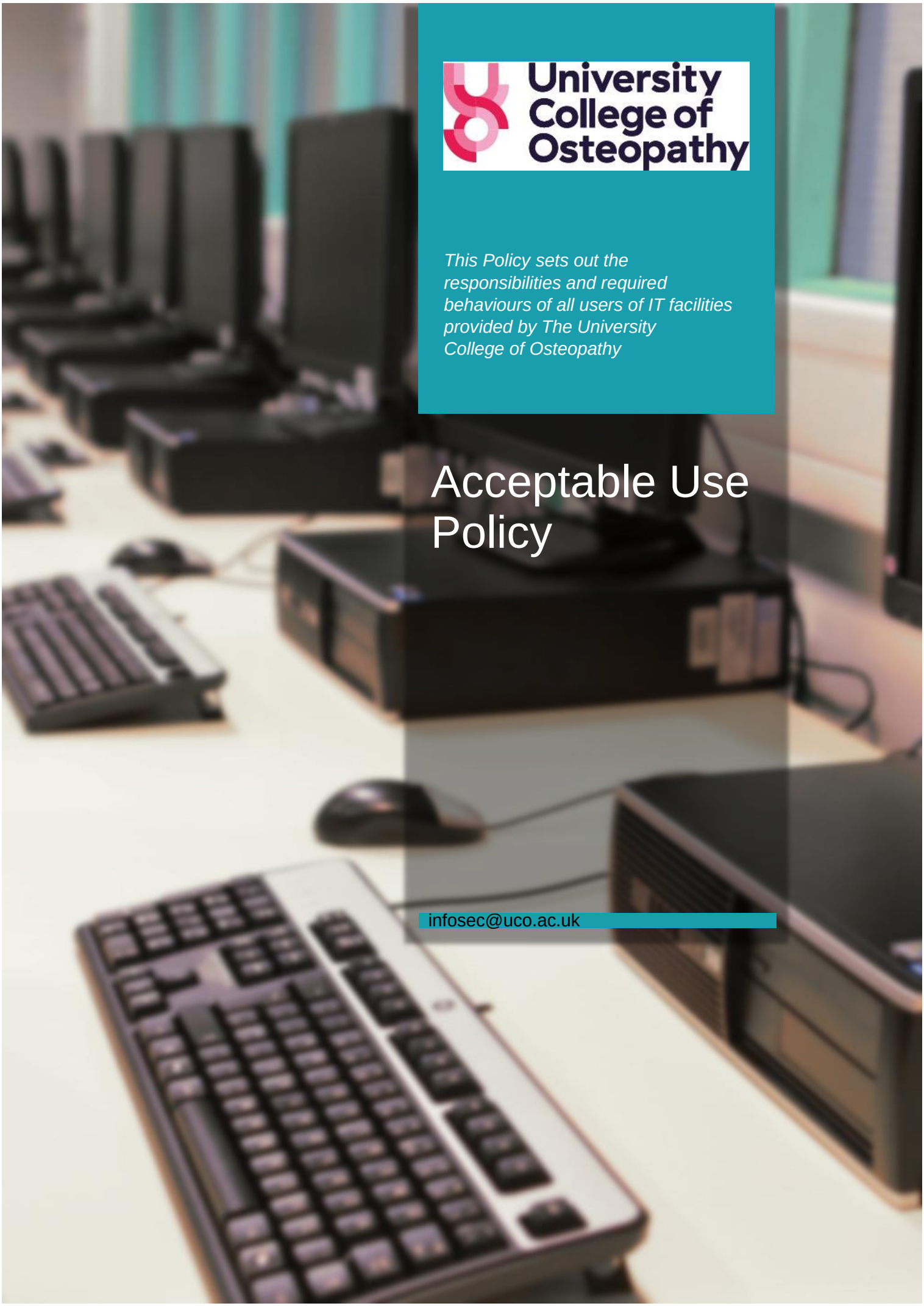

University College of Osteopathy

This Policy sets out the responsibilities and required behaviours of all users of IT facilities provided by The University College of Osteopathy

Acceptable Use Policy

infosec@uco.ac.uk

Document Control

Core Documentation Cover Page					
Acceptable Use Policy					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	Oct 2016 SMT	To include reference to the statutory Prevent Duty and to combine the Computer Misuse, Email and Internet and FirstClass Code of Conduct policies.	ICT Manager	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	Oct 2018
V2.0	Jul 2017 PRAG Chair	Administrative Amendments to update institution name change from British School of Osteopathy to University College of Osteopathy.	Head of Quality	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	Oct 2018
V3.0	May 2018 PRAG Chair	Administrative Amendments to reflect title changes (i.e. from Principal to Vice-Chancellor, etc.)	Head of Quality	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	Oct 2018
V4.0	Sep 2018 PRAG Chair	Administrative Amendments to reflect new email system, update staff role titles and correct typographical errors.	Head of Quality	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Oct 2018
V5.0	Jan 2024 SMT	V4 revised in entirety to assure the security of information processed by the UCO in line with legislative requirements.	IT Director	All master versions will be held in: Quality Assurance SharePoint Area	Jan 2027 Or in response to legislative changes

Equality Impact	
Positive equality impact (i.e. the policy/procedure/guideline significantly reduces inequalities)	
Neutral equality impact (i.e. no significant effect)	x
Negative equality impact (i.e. increasing inequalities)	

If you have any feedback or suggestions for enhancing this policy, please email your comments to: quality@uco.ac.uk

Contents

1. Purpose

The purpose of this policy is to explain the responsibilities staff, students and authorised third parties have in relation to their use of all electronic communications facilities, equipment and services provided by the UCO.

It forms part of the Digital Information Security Toolkit and underpins the overarching Information Security Policy. This policy provides everyone with guidance, so they have clear understanding of the requirements that UCO places on them, and the standards of behaviour expected.

2. Scope

The policy applies to all students, staff and other third-party users authorised UCO. It relates to the use of all electronic communications facilities owned, leased, hired or otherwise provided by UCO, connected directly or remotely to UCO infrastructure or used on UCO premises.

3. Responsibility

It is the responsibility of all students, staff and authorised third parties to ensure that their behaviour and activities when using UCO facilities is in accordance with the requirements of this policy.

4. Consequences of Policy Violation

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply may lead to the immediate cancellation of a contract. Where appropriate, breaches of the law will be reported to the authorities.

5. User Accounts

Those authorised to use UCO IT facilities are assigned an account for their individual use, under the following conditions:

- This account may not be used by anyone other than the individual to whom it has been issued.
- The assigned account password must be changed immediately and not divulged to anyone, including UCO IT staff, for any reason.
- For security reasons, this password must not be used as the password for any other account.
- Individuals must remember their password and change it if there is any suspicion that it may have been compromised.
- UCO reserves the right to change an account password at any given point in time if there is sufficient evidence to suggest that the account in question has been compromised.
- Individuals will also be assigned an individual email address for their use. The use of generic (role based) accounts is restricted under the JANET acceptable use policy.
- Individual email addresses are for the sole use of the assignee but remain UCO assets and their use is subject to all UCO policies covered by the UCO Digital Information Security toolkit.

6. Equipment

The following statements define restrictions around use of personal and UCO provided equipment when using UCO networks or information.

- Equipment not provided and managed by the UCO IT Department must not be connected to UCO internal networks (through any network ports) without the prior agreement of the IT Director.
- Equipment on any UCO site that is connected to the UCO network or otherwise managed by UCO IT Department may not be relocated without permission received via a request to the UCO IT Helpdesk.
- Staff and students are responsible for ensuring that all devices used in connection with UCO activity are password protected to safeguard any information held in the event of loss or theft.
- Computers and other equipment used to access UCO facilities must be locked if left unattended while logged in.
- Staff must ensure that they have up-to-date Anti-Virus software installed as well as ensuring that the latest security updates have been applied. In addition, individuals should ensure that there is a firewall always running on equipment connected to the UCO network, including equipment not owned by or supplied by the UCO.
- Any device that is not compliant with the above criteria is liable to physical or logical disconnection from the network without notice.
- Serious damage or the theft of electronic communications equipment should be reported to the UCO IT Helpdesk as soon as possible.

7. Staff / Student Software Licences

UCO makes Office 365 software available to staff and students for use on personal devices. These licences must be used within the terms of the vendor's licence agreements and:

- Can be installed only on devices owned by staff and UCO students or a device provided to an individual member of staff or UCO student.
- Must not be used for other personal, business or commercial purposes.
- Must be used only by the named individual.
- Must be removed when no longer a UCO student or member of UCO staff.

8. Personal Use of UCO Facilities

UCO provides IT facilities, including email addresses and computers, for academic and administrative purposes related to work or study. Reasonable personal use is however permitted under the following conditions:

- It is used in a manner which does not obstruct the work of other students or staff and which encourages a scholarly atmosphere to be maintained.
- It does not breach or undermine any UCO policies or codes of conduct.
- It is not excessive in its use of resources e.g., crypto currency related activities.

Members of staff and students should use only their UCO-provided email account when conducting UCO business. UCO computing facilities must not be used for the storage of data unrelated to the business or functions of the UCO. In particular, these facilities should not be used to store or share copies of personal photographs, media or personal emails.

9. Use of Third-Party IT Services

Wherever possible, users should always attempt to use only IT services provided or endorsed by UCO for conducting UCO business. However, if a requirement arises that is not met by existing solutions, discuss this with the IT Director in the first instance. An alternative solution may already be available or it may, subject to regulatory and procedural requirements, be possible to make use of services provided by third parties. Further information is available in the Information Handling Policy.

10. Unacceptable Use of UCO Facilities

Whilst not exhaustive, the following activities are considered to be unacceptable uses of UCO facilities. These restrictions are consistent with the JANET acceptable use policy (by which the UCO is bound) and the law.

- Any illegal activity or activity which knowingly breaches any UCO policy.
- Any attempt to knowingly gain unauthorised access to facilities or information.
- Any attempt to knowingly undermine the security or integrity of UCO facilities (including any unauthorised penetration testing or vulnerability scanning of any UCO systems).
- Providing access to facilities or information to those who are not entitled to access.
- Any irresponsible or reckless handling or unauthorised use or modification of UCO data (see the Information Handling Policy).
- Any use of UCO facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam).

- Creating, storing or transmitting any material which infringes copyright.
- Creating, storing, accessing or transmitting defamatory or obscene material.
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- Using UCO facilities for commercial gain without the explicit authorisation of the appropriate authority, such as crypto mining related activities.
- Failing to comply with a request from a member of UCO IT Department to desist from any activity which has been deemed to be detrimental to the operation of UCO IT facilities.
- Knowingly failing to report any breach or suspected breach of information security to the Digital Information Security Team (infosec@uco.ac.uk) or the UCO's Data Protection Officer (dpfio@uco.ac.uk) (further information on incident reporting is available in the Information Security Policy).
- Failing to comply with a request from a member of the UCO IT department for you to change your password.

11. Compliance with Legislation

In addition to the above requirements, UCO has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Individuals must also be aware of their responsibilities under the regulations listed below, and understand the fact that any infringement may result in action taken against them in accordance with UCO procedures:

- Counter Terrorism and Security Act 2015
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Wireless Telegraphy Act 2006
- UK GDPR
- Data Protection Act 2018

12. Monitoring

Monitoring of individual usage of the electronic communications facilities will not be undertaken as a matter of course. However, this may be necessary when concerns arise about the level or nature of personal use of the systems. Disciplinary action may be considered appropriate in such circumstances. Further information is available in the Information Security Policy.