University College of Osteopathy

ICT Acceptable Use Policy

University College of Osteopathy

Core Documentation Cover Page					
ICT 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 UCO Management Team	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

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

ICT Acceptable Use Policy

CONTENTS

1. SCOPE

1.1 This policy is applicable to all students, employees and visitors of the University College of Osteopathy (UCO) and informs them about the proper and expected use of all ICT (Information, Communication and Technology) facilities and systems to protect the integrity of the UCO's electronic resources.

1.2 For the purposes of this policy, ICT facilities and systems include:

a) Computer & Internet Use (including hardware, software, network storage, data and resources and Wifi services)

b) Email Use (including the acceptable use of the UCO's email system)

c) Website Use

1.3 There are a number of laws that govern the use of computers, internet and email and this policy aims to alert students, employees and visitors to these laws and to ensure that they abide by these at all times.

2. COMPUTER & INTERNET USE

2.1 Computer Use includes the use of UCO hardware, software and network storage, data and resources and use of the internet accessed through a UCO's computers or Wifi connection.

2.2 The UCO permits all students, staff and visitors to have access to the Internet, either through the UCO's computers or through the UCO's Wifi Service, for legitimate educational or business use. Limited personal use of the Internet is permitted, provided it does not contravene any of the other provisions specified within this policy.

2.3 ICT equipment and facilities are provided for the UCO's activities and all communications should portray the highly professional nature of the UCO.

2.4 The Computer Misuse Act 1990[1], which is intended to protect the integrity of computer systems, identifies the following as offences:

a) Unauthorised access or attempts to gain access to computers by hackers, or by 'insiders' who are authorised to use some parts of a computer system, but who go beyond their remit. To commit this offence, the action must be intentional and not merely the result of being inattentive, careless or incorrectly informed. The penalty for this offence can include imprisonment, or a fine of up to £2,000, or both.

b) Unauthorised access with the intent to commit or facilitate a further more serious crime; this offence can carry a maximum penalty of five years' imprisonment or a fine or both.

c) The unauthorised modification of data or programmes held in computers; erasure of information or the circulation of discs which are infected by a virus designed to impair the performance of the computer, are criminal offences and can carry a maximum penalty of up to ten years' imprisonment or a fine or both.

2.5 Internet access and related services are provided to the UCO by JANET (the Joint Academic Network) which supplies the UCO with a reliable and high bandwidth network to support research and learning and enable national and international communication and collaboration. All users must comply fully with JANET's Acceptable Use Policy[2].

2.6 In addition to the offences listed above, unacceptable use of the UCO's computing and internet facilities includes but is not limited to:

a) Creating, transmitting, storing or displaying offensive, indecent or obscene material.

b) Creating, transmitting, storing or displaying material that deliberately and unlawfully discriminates, or encourages deliberate and unlawful discrimination, on the grounds of race, ethnicity, gender, sexual orientation, marital status, age, and disability, political or religious beliefs.

c) Creating, transmitting, storing or displaying defamatory material.

d) Obtaining, transmitting, storing or displaying material that contravenes the Copyright, Designs and Patents Act 1988[3], including downloading and sharing of word, image, video and music files without the proper authorisation or permission.

e) Creating, transmitting, storing or displaying of material with the intent to defraud.

f) Corrupting or destroying another user's data or violating their privacy.

g) Using the ICT services in a way that denies services to other users.

h) Deliberately introducing, executing or transmitting malware.

i) Deliberately disabling or compromising the UCO's ICT security systems.

j) Causing deliberate physical or other damage to the UCO's ICT facilities or systems.

k) Downloading of programs from the Internet without prior approval from the ICT Manager; where downloading of a program is necessary in order to carry out your role / studies, the ICT Manager should be contacted to assist in the process and ensure that virus protection is sufficient.

l) Illegally copying CDs or DVDs.

m) Publishing, copying for re-sale, or distribution, of UCO course information to any external person or organisation, without prior consent of the Vice-Chancellor.

n) Accessing, creating, transmitting, storing or displaying terrorist or extremist material in line with the Counter-Terrorism and Security Act 2015[4] and Prevent Duty Guidance for England and Wales[5].

3. Email Use

3.1 All students and employees are provided with a UCO email account and email address for valid UCO use and should comply with the Conditions of Use & Code of Conduct for the Use of the UCO's Email Policy outlined below.

3.2 Although email is seen as an informal communication channel, it does have the permanence of written communications and should therefore be controlled to ensure that it meets the same standards as other published documents, i.e. representing the UCO in an appropriate and professional manner.

3.3 External email is not private or secure and employees should be aware that recipients can redistribute messages without the sender's knowledge.

3.4 Senders should avoid making inaccurate or defamatory statements using email, as it is traceable and accepted as evidence in courts of law. Once an email is sent, it may not be possible to un-send it.

3.5 Email that is exchanged between UCO and non-UCO entities must not contain any statements that imply contractual obligations. Where such obligation is required, electronic authentication is necessary and the advice of the Finance Director should be sought. The UCO deems that no contract made on the Internet or through email is legally binding to the UCO.

3.6 Care must be taken to ensure that email and other files are only sent to the intended recipient. If an email message is wrongly delivered, it should be immediately redirected to the correct person. If the message contains confidential information, use must not be made of the information nor must it be disclosed.

3.7 Communications sent or received over the Internet and to an external email address is generally not private or secure. Reasonable measures should be taken when transmitting confidential or sensitive material, or customer or supplier information.

3.8 Personal email services used outside of the UCO's premises such as Microsoft Hotmail should not be used to convey business messages, as security cannot be guaranteed.

3.9 There are many discussion forums available on the Internet, from academic institutions, research institutions to recreational sites. If these are used, information that is legally or commercially sensitive to the UCO or any of its trading partners must not be exchanged.

3.10 Sending offensive email internally or externally will not be tolerated by the UCO and the sender shall be subject to disciplinary action.

4. Acceptable Use of the UCO's Email System

4.1 All students and staff are provided with a UCO email account and email address.

4.2 Outlined below are the conditions of use and code of conduct for all UCO email users that must be abided by.

A) Conditions of use for the University College of Osteopathy's Email System

4.3 By using the UCO's email system each user accepts and agrees to abide by the conditions set out below. The UCO, through the ICT Director, reserves the right to exclude from the UCO's email system anyone who fails to comply.

4.4 The UCO's email system is provided for education, research and administration. Commercial use of the UCO's email system is forbidden. Those using the UCO's email system are personally responsible for their contributions to the system (as they would be for any written communication which is sent to others) and shall indemnify the UCO against any liability incurred by the UCO (including liability in defamation and for breach of copyright), which arises out of any such contribution.

4.5 Email communications must not consist of, or contain, illegal or offensive material. Any material which is considered by a conference moderator or other nominee of the board of the UCO, to be illegal or offensive may be removed from the system. For this purpose the expressions 'illegal' and 'offensive' include (without limitation) material:

a) The publication of which is defamatory;

b) That would infringe the copyright of a third party;

c) Which contravenes data protection legislation[6] or the Telecommunications Act[7];

d) Which constitutes incitement to racial hatred or which is offensive or obscene (see also the Legal Footnote below).

4.6 The originator of any such material may be excluded from further use of the UCO's email system by the ICT Director.

4.7 Each UCO email system user undertakes that he or she will not hold the UCO liable for any material contributed to a conference by another person, which is defamatory of that user.

4.8 Each individual is responsible for the security and use of their Username and Password. The use of someone else's account, Username (or password) is not allowed. Any user found using someone else's Username, or impersonating another user of the system, may be excluded by the ICT Director from further use of their UCO email account. Any user whose account is repeatedly being used by another user may also be excluded by the ICT Director from further use of their UCO email account.

4.9 Administrators of the UCO's email system may need to access any areas of users' email account in order to investigate technical problems, or in response to a complaint. This may include a necessity to access private mail. This data may be passed to the UCO's Data Protection Officer(s) in response to an official request.

4.10 UCO email accounts are not provided for personal purposes but if private mail messages are so used and intended to be private, they should be marked accordingly. Any personal information in such messages, provided the facility is properly used, will not be provided to non-recipients. Messages sent to any distribution list, cannot be deemed as private personal information.

4.11 Information regarding your use of the the UCO's email system may be used to generate statistics on system usage. These statistics may be used in UCO research or publications. Information about individuals will not be referenced in such material without their prior consent.

4.12 All users must comply with the Code of Conduct for the Use of the UCO's Email System.

B) Legal Footnote

4.13 Relevant legislation includes:

a) The Regulation of Investigatory Powers Act 2000

b) The Human Rights Act 1998

c) The General Data Protection Regulation

d) The Data Protection Act 2018

e) The Copyright, Designs & Patents Act 1988

f) The Computer Misuse Act 1990

g) The Criminal Justice and Public Order Act 1994

h) The Counter-Terrorism & Security Act 2015

i) All subsequent legislation pertaining to these areas.

4.14 Laws relating to theft would also apply in cases of "stolen" software (the Criminal Justice and Public Order Act 1994, for example, amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the telecommunications Act 1984, to extend their provisions to transmission over a data communications network; the potential 'let out' of transmission in coded form is ruled out by the concept of a 'pseudo photograph', i.e. electronic data that can be rendered into an image that has the appearance of a photograph.)

C) Code of Conduct for the use of the UCO's Email System

4.15 This Code of Conduct applies to all electronic and non-electronic communications systems supplied by the UCO and apply to staff and students alike.

4.16 The UCO's general rules and regulations apply to users of the UCO's email system (and all other electronic communication systems) just as they do in any other UCO environment. Specifically, the UCO has a published policy on harassment and has an equal opportunities policy. These policies are published on the UCO's website[8]. These rules, policies, regulations and the disciplinary procedures associated with them apply within the UCO's email system and breaches of them, or this Code of Conduct, may result in restrictions being placed on your use of the system and ultimately your removal from the system (in addition to the penalties referred to in the general policy statements).

4.17 The UCO's email system is a social environment. Normal rules of social interaction are in force. The remoteness of the recipients must not be used as an excuse to communicate in an anti-social manner. Examples of such anti-social behaviour are:

a) Harassment or intimidation of another user;

b) Person to person aggression within conferences;

c) Deviation from the spirit of a conference;

d) Excessive or inappropriate use of jargon, banter or graffiti;

e) The sending of SPAM (this includes sending one email to more conferences than is necessary to reach the intended audience).

4.18 None of these is considered acceptable behaviour.

4.19 UCO email users should address messages to ONLY the ONE all-encompassing group that includes their target audience (i.e. not to an all-encompassing group and also to sub-groups of that all-encompassing group).

4.20 Personal exchanges should be directed to a user's mailbox (i.e. an e-mail).

4.21 Copying or forwarding of private messages to another person without the author's explicit permission is a breach of confidentiality.

D) Complaint Procedures

4.22 If you feel that other users are not following this Code of Conduct, refer to the relevant Complaints Procedure.

5. Website Use

5.1 The UCO's website is used to promote the UCO's activities and to publish appropriate information that informs the wider public about the UCO and its business.

5.2 Care must be taken to ensure that all website content is published in an appropriate and professional manner and does not impinge on the integrity of the UCO or that of its customers or suppliers or other stake-holders.

5.3 The Vice-Chancellor must approve all material and content before it is published on the website.

5.4 The publishing of UCO information to any Internet service other than the approved UCO site(s) requires prior approval and any such proposal should be referred, in the first instance, to the Vice-Chancellor.

6. Employer's Liability

6.1 Information on an organisation's website or in an organisation's email can give rise to legal action against that organisation. The UCO is responsible for its employees' activities when using the Internet or external email. This applies even if the employee was acting without the UCO's knowledge or permission (the principle of vicarious liability).

6.2 An employee can also be held to be acting as an 'agent' of the employer if they tie the organisation in to a legally binding contract by appearing to have the necessary level of authority.

6.3 The UCO is also responsible if employees send email messages which are defamatory or which breach confidentiality or contract. Any such messages will be disclosable for the purposes of any legal action. The UCO will hold the employee personally and severally liable in any action against the UCO.

7. Monitoring of ICT Systems & Facilities

7.1 All electronic mail, files and other data stored, used or transmitted by the UCO equipment are the property of the UCO.

7.2 The UCO uses an internet filter that will alert the ICT department should an inappropriate website site be accessed, including those related, but not limited to: terrorism, extremism, indecent and offensive content.

7.3 The UCO reserves the right to monitor, intercept, access, copy, disclose or record such data without prior notice or permission, in order to ensure compliance with this policy.

7.4 Monitoring may be periodic, random or continuous.

8. Breach of Policy

8.1 If you discover inappropriate material on a UCO computer or system or witness any breach of this policy, please inform the ICT Department immediately (Helpdesk@uco.ac.uk). You should leave any discovered inappropriate material in its original state in order that an investigation into its origin can be conducted.

8.2 Anyone found to have breached this policy shall be subject to the UCO's relevant Disciplinary Procedures, may have their access revoked and may be reported to the police as appropriate.

[1] Computer Misuse Act 1990: http://www.legislation.gov.uk/ukpga/1990/18/contents
[2] JANET Acceptable Use Policy: https://community.jisc.ac.uk/library/acceptable-use-policy
[3] Copyright, Designs and Patents Act 1988: http://www.legislation.gov.uk/ukpga/1988/48/contents
[4] Counter-Terrorism and Security Act 2015: http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted
[5] Prevent Duty Guidance for England and Wales: https://www.gov.uk/government/publications/prevent-duty-guidance
[6] The GDPR (https://eur-lex.europa.eu/eli/reg/2016/679/oj) & Data Protection Act 2018 (http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)
[7] Telecommunications Act 1984: http://www.legislation.gov.uk/ukpga/1984/12/contents
[8] https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy