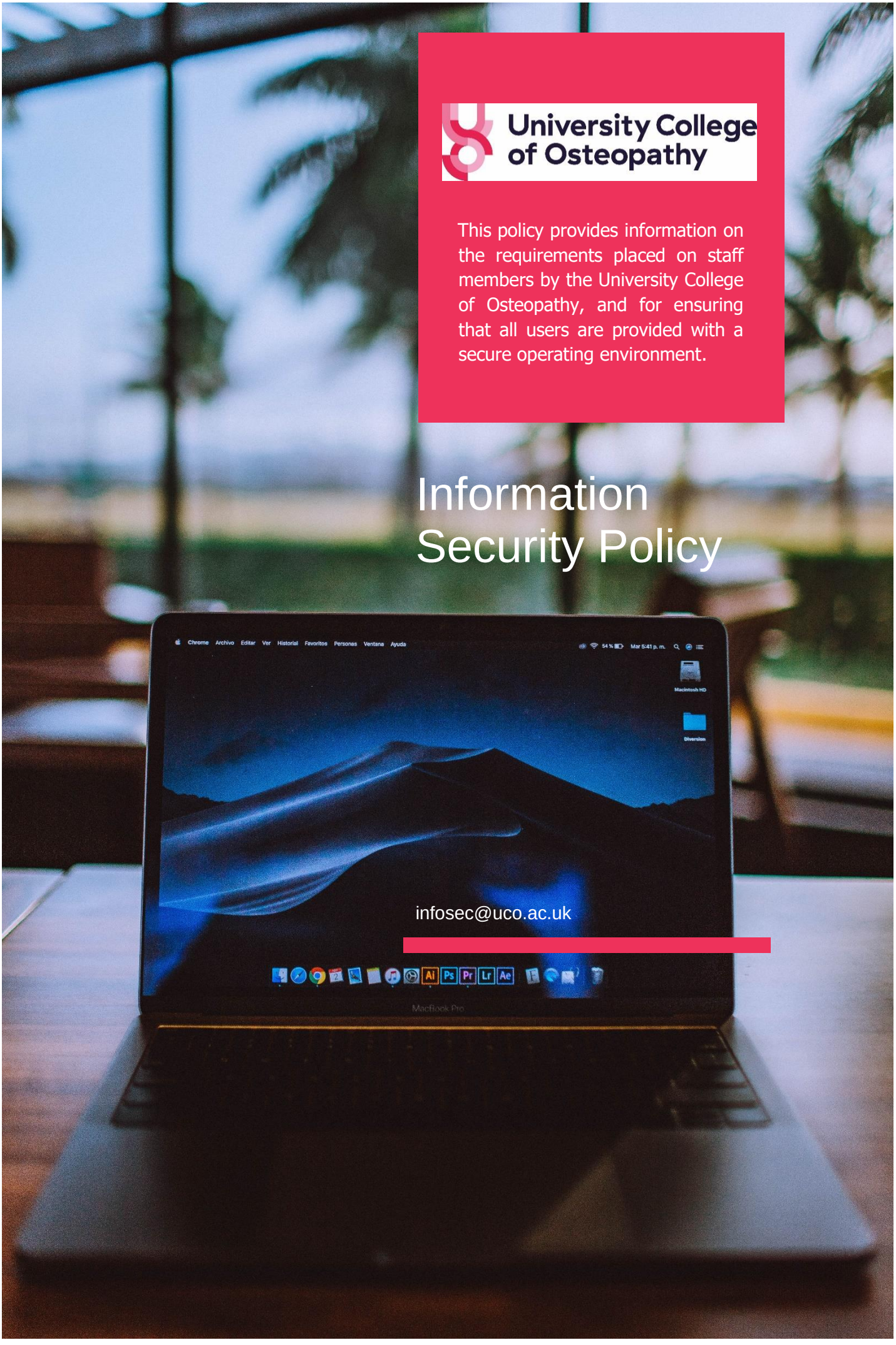
University College of Osteopathy

This policy provides information on the requirements placed on staff members by the University College of Osteopathy, and for ensuring that all users are provided with a secure operating environment.

Information Security Policy



infosec@uco.ac.uk

Document Control

Core Documentation Cover Page					
Information Security 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	April 2018 SMT	Produced to assure the security of information processed by the UCO in line with legislative requirements.	Head of Quality	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	April 2020 Or in response to legislative changes
V2.0	Dec 2019 PRAG Chair	Administrative Amendments to reflect new Committee structure	Head of Quality	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	April 2020 Or in response to legislative changes
V3.0	Jan 2024 SMT	V2 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

This policy ensures that all technology and information assets provided and managed by UCO are adequately protected against security threats including compromise, loss, unauthorised disclosure, and other misuse.

It provides guidance to everyone who uses UCO IT facilities to ensure they are aware of, and able to comply with, the requirements placed upon them by all associated Information Security policies, and are also aware of and are able to work in accordance with the relevant procedures, legislation, and codes of practice.

2. Scope

The policy applies to any individual authorised by UCO or any department thereof. It relates to the use of all UCO IT facilities; to all private systems (whether owned, leased, rented or on loan) when connected to the UCO Infrastructure; to all UCO owned or licensed data and technology; and to all data and technology provided to UCO by partners or external agencies, including cloud services. The policy also relates to paper files and records created or held by UCO.

3. Consequences of Policy Violation

A copy of this policy will be issued to all account holders upon activation of their user account.

Existing students and staff of UCO, as well as authorised third parties with access to IT facilities will be advised of the existence of this policy and the availability of the associated policies, procedures, guidance and training. It is strongly recommended that individuals refamiliarize themselves with this, and all other, UCO Information Security policies at least annually. 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.

4. Education and Awareness

To ensure that students and staff are provided with the necessary information to allow them to make informed decisions on security, UCO is committed to providing training and guidance on security issues and best practice recommendations. Students and staff are entitled to training, and UCO reserves the right to mandate specific security training (e.g. NCSC Cyber security Training) as a criteria of continued access to provided IT facilities. Any such training will be introduced in line with UCO agreed processes.

5. Responsibility for Information Security

All users of UCO IT facilities have a personal responsibility to manage and protect information under their possession and may be personally liable for any incidents that arise from a failure to take appropriate protective measures. Individuals also have a responsibility to act in a vigilant and professional manner, by refraining from any action that may jeopardise the integrity or security of UCO systems, and promptly reporting any suspected security violations. It is the responsibility of every student, staff and authorised third party to understand and act in accordance with all Information Security policies and procedures instituted at a UCO wide or departmental level.

Staff with line management responsibilities must ensure that their supervised staff members are aware of, and comply with, security best practices.

All members of SMT within the UCO are responsible for ensuring that Information Security policies are implemented and complied with across their respective areas. This includes promoting security awareness and best practices among staff and maintaining full oversight over activities that have the potential to influence the confidentiality, integrity or availability of UCO information or infrastructure.

The Information Governance & Security Steering Group (IGSSG) are responsible for the review and approval of all policies relating to Information Security at UCO. However, it is the Digital Information Security Team that consult with relevant stakeholders annually to review operational and strategic Information Security activities. As such, the team can also advise on matters related to compliance with these policies, and may introduce supplemental information, guidance, or procedures with respect to these policies. The team are also responsible for regularly assessing Information Security policies to ensure their usability and accuracy.

6. Legislative Compliance

Students and staff have an obligation to abide by all UK and relevant EU legislation. With respect to information security, of particular importance are the Computer Misuse Act 1990, the Data Protection Act 2018 and UK GDPR, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000.

Failure to comply with data protection legislation could lead to the UCO breaking the law. This can result in large fines and other legal sanctions. Data breaches can also cause significant distress to individuals and have an adverse impact upon the UCO's reputation with the media and other key stakeholders such as prospective students. Deliberate misuse of personal data is also a criminal offence for which you can be personally liable.

Personal data is any information attributable to an identifiable individual, including names and email addresses. For example, details of a student’s academic performance and qualifications constitute personal data.

Sensitive personal data ("Special Category data") includes disability status, ethnicity, medical information (both physical and mental) and details of criminal convictions and may require heightened security measures such as encryption and stricter access controls.

7. Monitoring

Monitoring of individual usage of the electronic communications facilities will not be undertaken as a matter of course. However, many UCO systems maintain transaction and event logs, which record information about each transaction being carried out. The content of these records vary but may contain the following information:

- the date and time of the transaction;

- the number of bytes transferred in the transaction;
- the unique source and destination IP address of data packets;
- the type of process;
- the Universal Resource Locator (URL);
- the login identity of the person making the transaction;
- the source and destination address of E-mail transactions.

These logs are essential to the efficient running of IT systems and are maintained by the UCO IT Team for the following reasons: capacity planning; traffic and/or transaction flow monitoring; system monitoring; transaction tracking; fault diagnoses; system security; virus detection and auditing.

In cases of security breaches, system malfunctions, the receipt of substantiated complaints from other organisations and virus or hacking attacks, these logs may be used as part of an investigation to trace transactions through the system to a particular PC or individual.

Internet 'web caches' are used to improve the retrieval times of frequently accessed web pages and store a complete copy of accessed pages for a predetermined period of time. All internet traffic from all UCO sites is monitored with access to certain classifications blocked as standard. In some circumstances, such as the detection of virus attacks or investigations into computer abuse, authorised personnel from within the UCO IT Team may search the content of any web filtering or web caches.

8. Digital Information Security Policy Toolkit

This policy relates to, and is supplemented by, a number of policies that pertain to the confidentiality, integrity and availability of UCO information and technology assets. These policy documents form the Digital Information Security Policy Toolkit, and a list of the supplementary policies is given below. Acceptance and compliance of this policy is contingent upon compliance with all policies provided in the Toolkit.

- Information Handling Policy
- Acceptable Use Policy
- Password Policy
- Data Protection Policy
- Personal Data Breach Management Policy
- Records & Information Management Policy

Each of the policies within the Toolkit contain high-level descriptions of requirements and principles. They are not intended to provide detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents, guidance articles, and supplementary information which will be made available in conjunction with the relevant policy document. Any substantive changes made to any of the policies within the Toolkit will be communicated to all relevant personnel.

9. Reporting Information Security Incidents

It is our responsibility to ensure we follow the correct steps to protect the security of staff and student data. Potential, suspected and actual personal data breaches must be reported immediately. The following guide outlines the steps you must take to report any potential information security breaches straight away:

1. Report any potential information security breaches to the Digital services Information Security Team infosec@uco.ac.uk This is essential to control the risk to you, data subjects and the UCO.
2. For IT-related breaches (e.g., response to a phishing email or lost device) contact the UCO IT helpdesk by phone on +44 (0)207 89 5300 or e-mail helpdesk@uco.ac.uk, if this is outside of IT department hours, as a precaution change your Microsoft Office 365 password immediately.
3. If the suspected data breach concerns lost or found physical information (e.g. a box of paper records) or a mobile device, contact the relevant head of department, estates department or again the IT Helpdesk.
4. Report any potential, suspected or actual personal data breaches to the UCO's Data Protection Officer immediately (dpfio@uco.ac.uk). A personal data breach includes the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed by the UCO. Please refer to the UCO's Personal Data Breach Management Policy for further information.