University College of Osteopathy

Information Security Policy

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 the new Committees' 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

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

Information Security Policy

CONTENTS

1. Introduction

1.1 Information is a vitally important asset to the University College of Osteopathy (UCO) and as such we must ensure that this information is kept safe and used appropriately. We have therefore developed this Information Security Policy that complies with relevant legislative requirements to assure our stakeholders that data held and processed by the UCO is treated with the highest respect and appropriate standards to keep it safe and secure.

1.2 All staff and students of the UCO are required to comply with this policy to ensure that the risk of losing data, leaking data and breaching data protection legislation is avoided.

2. Scope of Policy

2.1 This policy is applicable to, and will be communicated to, all staff, students, other authorised users of the UCO and third parties who interact with information held by the UCO and the information systems used to store and process it.

2.2 This policy shall apply to:

a) All information systems (including servers, computer equipment, mobile devices, network equipment and telecommunications equipment) owned or operated by the UCO or connected to the UCO network by third parties.

b) All software (including operating systems, network services and application software) installed on applicable information systems by the UCO.

c) All information stored on the UCO's information systems.

2.3 Information security shall include protection of the following:

a) Confidentiality: Ensuring that information and systems are accessible only to authorised users.

b) Integrity: Safeguarding the accuracy and completeness of information and processing methods.

c) Availability: Ensuring that authorised users have access to information and systems when required.

3. Policy Objectives

3.1 The objectives of this policy are to:

a) Provide a framework for establishing suitable levels of information security for all UCO information systems (including but not limited to all computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

b) Ensure that all users are aware of and comply with all current and relevant UK and EU legislation related to Information Security.

c) Provide the principles by which a safe and secure information systems working environment can be established for staff, students and other authorised users.

d) Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

e) Safeguard the UCO from liability or damage through loss or breach of data.

f) Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

4. The UCO's Approach to Information Security

4.1 The UCO will use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives.

4.2 The UCO will use ISO 27001/BS7799: Information Security Management as a guide for determining policy and managing security.

4.3 This policy shall comply with relevant legal and contractual requirements including but not limited to:

- The Regulation of Investigatory Powers Act (2000)
- The Data Protection Act (1998)
- The Human Rights Act (1998)
- The Computer Misuse Act (1990)
- The Digital Economy Act (2010)
- The JANET Acceptable Use Policy.

4.4 This policy should be read in conjunction with the UO's ICT Acceptable Use Policy and will not unnecessarily limit academic or individual freedom.

5. Information Security Responsibilities

5.1 All users of UCO information systems are responsible for protecting information assets (see Appendix A: UCO Information Security Checklist).

5.2 Users must at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with the security policy.

5.3 The UCO's Senior Management Team through the Information Governance & Information Security Steering Group is ultimately responsible and accountable for ensuring that the objectives of this policy are met.

5.4 The Data Protection & Freedom of Information Officer (DPFIO) is responsible for implementation of the policy and is authorised to pursue activities to achieve the policy objectives.

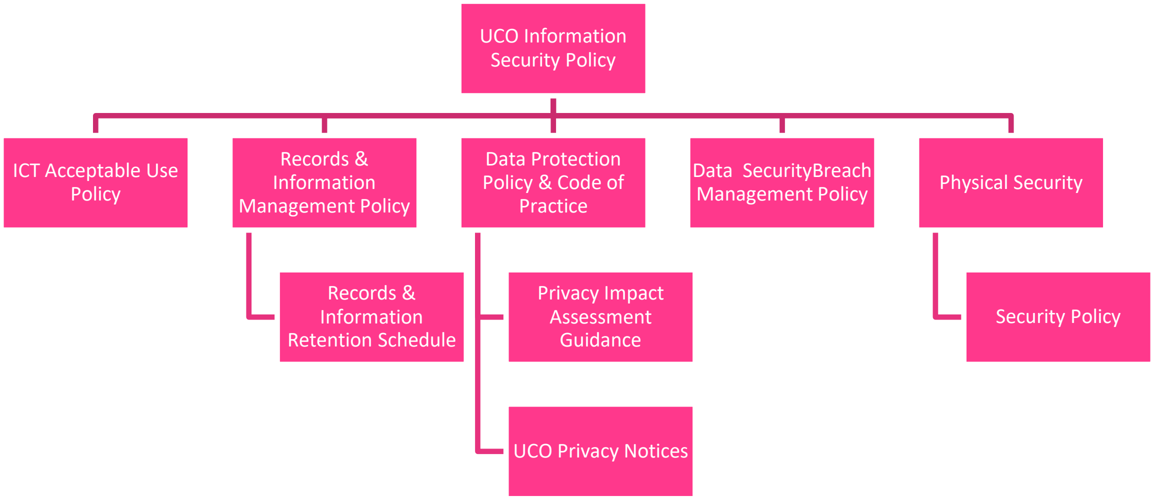
5.5 The ICT Team is responsible for advising users on security issues, preventative monitoring of information systems and investigating security incidents.

5.6 Users should report any breach in information security or suspected breach to the ICT Team (ict@uco.ac.uk) in accordance with the Data Security Breach Management Policy.

5.7 Information security best practice and the terms of this policy shall be considered at all points in the lifecycle of equipment, software and services developed by, specified by or purchased by the UCO.

6. Associated Policies

6.1 The following policies, guidance and practices are associated with this policy which must be followed at all times by all users of the UCO:


UCO Information Security Policy
ICT Acceptable Use Policy
Records & Information Management Policy
Data Protection Policy & Code of Practice
Data SecurityBreach Management Policy
Physical Security
Records & Information Retention Schedule
Privacy Impact Assessment Guidance
Security Policy
UCO Privacy Notices

6.2 The information security policy will be reviewed annually to determine whether it still meets the evolving needs of the information infrastructure.

7. Policy Awareness

7.1 The ICT Team will publicise this policy and any associated standards and guidelines to all UCO users.

7.2 Information security awareness will be provided through appropriate training courses and published documents.

8. Monitoring of Information Systems

8.1 ICT staff will monitor information systems and the UCO's network to detect unauthorised activity, identify potential weaknesses and pro-actively prevent security incidents.

8.2 The UCO uses web filtering software to detect attempted access or access to inappropriate websites and is able to identify the user attempting to do so. Such users may be subject to appropriate disciplinary action under the ICT Acceptable Use Policy.

8.3 Email correspondence and electronic files of staff and students may be monitored and accessed by the ICT Team for legitimate purposes, e.g. in response to a subject access request, police, disciplinary or complaint investigation. Users will normally be notified if access is required in such circumstances.

8.4 This policy and compliance with it applies to all UCO users and those who use the UCO's information systems.

8.5 Appropriate disciplinary action under the ICT Acceptable Use Policy may be taken against anyone disregarding the policy.

9. Exceptions to this Policy

9.1 Exceptions to this policy may be made at the discretion of the ICT Director or the UCO's Vice-Chancellor's Group.

10. Information Security Principles

10.1 The following Information Security Principles govern the security and management of information at the UCO:

a) Information should be classified according to an appropriate level of confidentiality, integrity and availability in line with our Information Asset Classification System and in accordance with relevant legislation (see The UCO's Approach to Information Security).

b) Staff with particular responsibilities for information management (see Information Security Responsibilities) must:

   a. Ensure and monitor the classification of that information.

   b. Handle that information in accordance with its classification level.

   c. Comply with any contractual requirements, policies, procedures or systems for meeting those responsibilities.

c) All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.

d) Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.

e) Information will be protected against unauthorised access and processing in accordance with its classification level.

f) All data breaches must be reported in line with the Data Security Breach Management Policy.

g) Information security and related policies shall be reviewed regularly in addition to annual internal audits.

11. Policy Terminology

11.1 This policy uses the following terminology:

Term	**Definition**
Must, Required or Shall	An absolute requirement.
Must Not or Shall Not	An absolute prohibition.
Should or Recommended	That there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully considered before choosing a different course.

Should Not or Not Recommended	That there may exist valid reasons in particular circumstances when the particular item is acceptable or even useful, but the full implications should be understood and the case carefully considered before implementing any behaviour described as such.
May	An item is optional.
Administrator	Any UCO user who is authorised to maintain or administer IT equipment, normally members of the UCO's ICT Team.
Computer Equipment	Any server, workstation, personal computer or laptop or mobile device.
Connected to the UCO's Network	Locally or remotely connected to the UCO's network (as defined below).
Department or Team	Any department, division or other organisational unit of the UCO.
Mobile Device	Any personal digital assistant, network-enabled mobile telephone or other small footprint device.
Information System	Any mechanism or method for storing information including but not limited to IT equipment.
ICT or IT	Information and Communication Technology, i.e. any computer equipment or technological process for storing information.
ICT or IT Equipment	Any computer equipment, network equipment, telecommunications equipment or handheld device.
ICT Team	The UCO's ICT Team.
Laptop	A portable personal computer.
Locally connected to the UCO's network	Connected to the UCO's network via a network access point from a UCO owned or operated building or via a wireless connection to a wireless network access point operating from a UCO owned or operated building.
Mobile Phone Computer	A portable electronic telecommunications device connected to a wireless communications network that makes and receives calls and connects to the internet.
Network Equipment	Any hub, switch, router or other equipment used to transport data across a network.
Personal Computer or PC	A small single-user computer based on a microprocessor.
Personal Data	Data that relates to a living individual that can be identified from that data, or data that when combined with other information that is in the possession of or likely to come into the possession of the data controller that can identify a living individual.
Remotely connected to the UCO's network	Connected to the UCO's network via a modem, ISDN terminal adaptor, broadband modem, cable modem or other communications

	device through a dial-up access facility or an internet account operated by an Internet Service Provider (ISP).
Responsible User	A user who normally operates a specific piece of IT equipment.
Server	A multi-user computer offering services over a network.
Single-user Computer Equipment	Any personal computer, workstation or laptop that is used by a single person at a time and does not provide significant services to other network users.
Tablet	A portable personal computer, typically with a mobile operating system and LCD touchscreen display.
Third Party	An individual or group who is not a member of the UCO, e.g. a visitor or guest.
User	Any UCO member or other person who is authorised to use IT equipment.
Workstation	A powerful single-user computer with high quality graphics.

12. Information Asset Security

12.1 In the context of this policy the UCO’s information assets are defined as:

a) Hardware assets: all IT equipment owned or operated by the UCO.

b) Software assets: all commercial software owned or licensed by the UCO and all open source software operated by the UCO.

c) Information assets: the contents of all databases, electronic mailboxes, word processing documents, spreadsheets, web pages, data files, configurations files and other information systems created by UCO members in the course of their duties are information assets of the UCO or its members.

12.2 Information assets are the ultimate product of the use of hardware and software assets.

12.3 The creation, manipulation and dissemination of information assets is fundamental to the business of the UCO and shall be protected by the secure installation, configuration and updating of information systems.

12.4 Secure installation, configuration and updating of hardware and software assets shall be verified, in part, by asset management and tracking.

A) Hardware Assets

12.5 The ICT Team shall maintain an inventory of all hardware assets connected to the UCO network as appropriate.

12.6 The following information shall normally be maintained as part of the inventory.

- Department
- Location
- Owner (or administrator)

- Media Access Code (MAC) address
- Internet Protocol (IP) address (if fixed)
- Hostname
- Domain name

B) Software Assets

12.7 The ICT Team shall maintain an inventory of all centrally licensed or owned commercial software.

12.8 The following information should be maintained as part of the inventory.

- Software product
- Version
- Number of licensed copies
- Number of installed copies
- Owners or locations of installed copies

C) Information Assets

12.9 The Security Information Risk Officer shall maintain the UCO's Information Asset Register that records and maintains an up to date inventory of the UCO's information assets.

12.10 Information assets shall be assigned an information classification based on the sensitivity of the information they contain in line with the information classification system below.

13. Information Asset Classification System

13.1 Table 1 defines the information classification system used by the UCO to classify the security level of information the UCO processes. This system aligns with the above Information Security Principles, incorporates the definitions of Personal Data and Special Categories of Personal Data as defined by the EU General Data Protection Regulation (GDPR) and aligns with our Information Asset Register.

13.2 If an information asset includes information from different categories, it should be classified as the most sensitive category.

13.3 Each information asset shall have an owner. By default the owner of information assets stored on IT equipment shall be the person responsible for the user account under which the asset is stored (i.e. the possessor of the asset).

13.4 Where the assets of multiple owners are collected into a common data store not under the control of a single person (e.g. a database), a notional owner should be assigned. The notional owner may be a leader or nominated individual of the group collecting information assets into the common data store or an administrator for the data storage package. By default the notional owner shall be the data store administrator.

13.5 Owners or notional owners of information assets should classify the relative value of their assets. Risk analysis should be performed for all assets that are critical to the operation of the core functions of the UCO, departments or administrative units.

Table 1: The Information Asset Classification System

Security Level	Definition	Examples (Not Exhaustive)
Highly Restricted	The information is of significant value. The information is defined under the Data Protection Act 1998 (DPA) as “Sensitive Data”. The information is defined under the GDPR as “Special Category Data”. Access to the information is restricted to only those who “need to know”. Unauthorised disclosure or dissemination could result in: • Severe financial damage, including fines of up to €20m or 4% of our global annual turnover of the previous financial year. • Severe reputational damage. • The revocation of contracts with third parties and the failure to win future contracts / research bids. If this classification of data is held on mobile devices such as laptops, tablets or phones, or in transit, the file / folder must be password protected and the device must be password protected and encrypted (AES 256-bit encryption at the device, drive or file level). Requires significant scrutiny before being disclosed as part of Freedom of Information Act (FOI) requests with consideration of FOI exemptions and public interest and legal considerations. Must be disposed of by shredding.	1. DPA “Sensitive Data” & GDPR “Special Category Data” include data relating to a living individual’s: • Race or ethnic origin. • Political opinion. • Religious beliefs or other beliefs of a similar nature. • Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992). • Physical or mental health or condition. • Sexual life or sexual orientation. • Commission or alleged commission of any offence. • Proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. • Genetics data. • Biometric data (where used for identification purposes). 2. Salary information. 3. Bank details of an individual. 4. Draft and final reports of a commercially / financially / controversially sensitive nature. 5. Passwords. 6. Large aggregates of personal data (e.g. held on student / staff / patient databases). 7. Research interview transcripts and databases. 8. Disciplinary proceeding records.
Restricted	The information is of especial value. Access to the information is restricted to a small group of staff. Unauthorised access to the information is prevented by password / login. The information is defined under the Data Protection Act 1998 as “Personal Data”. The information is defined under the GDPR as “Personal Data”. Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to the UCO. If this classification of data is held on mobile devices such as laptops, tablets or phones, or in transit, the file / folder must be password protected and the device must be password	1. DPA & GDPR “Personal Data” include data relating to a living individual’s: • Name. • Identification number. • Address. • Phone number. • Email address. • Schools attended. • Photographs. • Other personal identifiers such as locations data or online identifier. 2. Confidential meeting minutes. 3. Draft reports or meeting minutes. 4. Draft policy, regulation or course documents.

	protected and encrypted (AES 256-bit encryption at the device, drive or file level). Requires careful scrutiny before being disclosed as part of Freedom of Information Act (FOI) requests with consideration of FOI exemptions and public interest and legal considerations. Must be disposed of by shredding.	
Internal Use	The information can be disclosed or disseminated to members of the UCO, including UCO partners, as appropriate by information owners without any restrictions on content or time of publication. Requires careful scrutiny before being disclosed as part of Freedom of Information Act (FOI) requests with consideration of FOI exemptions and public interest and legal considerations. Must be disposed of by confidential waste.	1. Internal correspondence (that is not relating to Restricted or Highly Restricted matters). 2. Final reports / meeting minutes / focus group notes. 3. Committee papers. 4. Final policy and procedure documents. 5. Information held under License. 6. Teaching and learning material.
Public	The information can be disclosed or disseminated to the public without any restrictions on content or time of publication. Disclosure or dissemination of the information must not violate any relevant laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system. May be disposed of by normal waste / recycling.	1. Annual Reports & Financial Statements. 2. Minutes of statutory / other formal committees. 3. Pay scales. 4. Course information. 5. Publicity information. 6. Information published on the UCO website or through our Publication Scheme.

14. ANTI-VIRUS DETECTION & PROTECTION

14.1 The UCO ensures that appropriate action is taken for effective virus detection and prevention regarding:

a) All UCO owned or operated computer equipment connected to the UCO Network.

b) All Third-Party computer equipment connected to the UCO Network where possible.

c) All users or administrators of the above computer equipment.

14.2 The ICT Team shall ensure that appropriate anti-virus software is procured by the UCO and is maintained appropriately.

14.3 Third Party users and users using their own devices are recommended to install appropriate anti-virus software onto their devices; the UCO is not responsible for users' own devices.

A) Use of Anti-Virus software

14.4 The UCO's ICT Team shall ensure that all computer equipment identified by the scope of this policy shall have anti-virus software installed that is operational and maintained.

B) Workstations, Personal Computers and Laptops

14.5 For workstations, Personal Computers and laptops, the ICT Team shall ensure that anti-virus software provides an 'always on' background process and that this is turned on.

14.6 The ICT Team shall ensure that anti-virus software provides an automatic, scheduled virus scanning capability is turned on.

14.7 The ICT Team shall ensure that regular, full virus scans are undertaken for all workstations, personal computers and laptops procured by the UCO.

14.8 For computer equipment with 'always on' virus scanning, full virus scans shall be scheduled at least once a month. For computer equipment without 'always on' virus scanning, full virus scans shall be scheduled at least once a week.

14.9 All users must ensure that any suspicious or unknown files received via email, network download, disk, CD or other media from unknown or untrusted sources are forwarded to the ICT Team before they are opened.

C) Servers

14.10 For servers, the ICT Team shall ensure that the anti-virus software 'always on' background process option is turned on if this does not significantly affect the performance or operation of the server.

14.11 The ICT Team shall ensure that regular, full virus scans of all UCO servers are undertaken at least once a month; where a full virus scan affects performance or operation of the server the virus scan shall be performed out of regular office hours, at weekends or during scheduled downtime.

14.12 Users must report any suspicious files found on a server or that come from an unknown or untrusted source to the ICT Team before being opened.

D) Updating Virus Signatures

14.13 The ICT Team shall ensure that virus signature files are updated regularly and where the anti-virus software provides automatic checking for new virus signatures, ensure that this is turned on.

14.14 For computer equipment with automatic checking, the ICT Team shall ensure that the software is scheduled to check for new virus signatures at least once a day.

14.15 For computer equipment without automatic checking the ICT Team shall make manual checks at least once a week.

E) Disinfecting Computer Equipment

14.16 If a virus is detected or suspected the ICT Team must be informed immediately (ict@uco.ac.uk).

14.17 If a virus is detected the ICT Team shall be responsible for disinfecting, deleting or quarantining the file/s affected.

F) Creation or Distribution of Viruses

14.18 Any activities undertaken with the intention of creating and/or distributing viruses or other malicious code are prohibited in accordance with the UCO's ICT Acceptable Use Policy.

G) Exceptions

14.19 Exceptions shall only be made in the following circumstances:

a) No anti-virus software is available for the particular platform.

b) All available anti-virus software conflicts with essential services or applications running on the computer equipment causing the system to crash or become unusable.

H) Responsibilities

14.20 The ICT Team shall be responsible for ensuring that anti-virus software is installed and operating on all computing equipment and servers owned by the UCO.

14.21 Users are responsible for ensuring that anti-virus software is installed and operating on their own devices.

14.22 Users are responsible for ensuring that they take every precaution to prevent the distribution of viruses or other malicious code by:

- Ensuring that they do not open any email attachments or click on links to websites within emails received from unknown origins.
- Ensuring that they do not download or attempt to download anything from

15. UCO Computer Equipment Security

A) Ownership & Management of UCO Computer Equipment

15.1 All users of UCO-procured computer equipment are responsible for their appropriate use and must inform the ICT Team of any known or suspected security-related problem with the computer equipment by emailing ict@uco.ac.uk immediately.

B) UCO Computer Equipment Requirements

15.2 UCO computer equipment shall be configured with a currently supported version of the operating system, so that security patches or critical updates that protect against new vulnerabilities are provided by the manufacturer and that the version has not been designated as 'end of life'.

15.3 Computer equipment shall be configured with currently supported versions of software so that security patches or critical updates that protect against new vulnerabilities in a timely manner are provided by the manufacturer or developer.

15.4 Computer equipment shall be configured to provide only the services and resources required by the users; services and applications that are not required must be removed or disabled.

15.5 Information, services or resources that are not intended for general public access shall be protected by access-control mechanisms (e.g. passwords and encryption) and access shall be restricted to authorised users only on a "need to know" basis.

15.6 If the computer equipment provides a security event logging mechanism, this mechanism shall be turned on to assist auditing and if the computer equipment provides other event logging capabilities, this mechanism should be turned on to assist with problem diagnosis.

15.7 Security patches must be installed on the system as soon as they are available. If an automated facility to check for patches and updates is available it should be used. The only exception to immediate patching is when this would adversely affect an application or service in use by a user.

15.8 Anti-virus detection and prevention software shall be implemented as described above.

15.9 Services shall be run from non-privileged rather than administrator accounts where it is feasible to do so.

C) UCO Laptops & Mobile Devices

15.10 Users should be aware that laptops and mobile devices are at greater risk of exposure to security threats than fixed location (desktop) computer equipment permanently connected to the UCO network due to:

- Maintaining the physical security of a laptop and mobile device in-transit or at an off-site location may be more difficult.
- Theft or loss of laptops and mobile devices is more likely which increases the risk of unauthorised access to data stored on them.
- Laptops and mobile devices may be connected to home or third party networks that are less secure than the UCO network leading to higher risk of exposure to cyberattacks.

16. Transmission & Publication of Information

A) Use of Encryption

16.1 Network communications that involve the transmission of passwords, authentication secrets, confidential or highly confidential information as defined in the Asset Management Policy must be encrypted, if a suitable encryption mechanism is available.

B) Removing Metadata

16.2 Metadata is data that provided information about other data, e.g. who authored an electronic document, the file size and when it was created or modified. As such personal information may be included as metadata in documents that are circulated or published.

16.3 Before transmitting or publishing a document metadata must be removed using the relevant commands for the file being transmitted / published. The ICT Team may be contacted to assist in this.

17. Dial-Out Service

A) Purpose & Scope

17.1 A dial-out service allows users to connect directly to other networks and telecommunication services without using UCO network services (e.g. mail relays, web caches) and without passing through the UCO network gateways; in this context this does not include internet-enabled mobile telephones, PDAs or other mobile devices unless they are also used to connect locally to the UCO network.

17.2 Dial-out access bypasses the security checks and safeguards (e.g. firewalls, virus checkers) provided for the UCO's network and may allow malicious code or individuals to gain access to the UCO's network unseen and unchallenged and is therefore a high security risk.

17.3 Dial-out service users include:

- Those using UCO owned or operated computer equipment with an internal or external modem or an alternative telecommunication capability that is not operated as part of the core UCO network by Information Services.
- Those using third party (i.e. their own) devices locally connected to the UCO network that has an internal or external modem or an alternative telecommunication capability that is not operated as part of the core UCO network by Information Services.

17.4 Dial-out access from the UCO campus via a modem, IDSN, ADSL, broadband or any other telecommunications service shall not be permitted, except by special waiver from the ICT Director or a designated representative.

B) Special Waivers for Dial-Out Service

17.5 A special waiver for dial-out service shall be granted only where the connectivity required cannot be achieved via the normal UCO network services and where there is a legitimate business or academic reason for it.

17.6 IT equipment granted a special waiver and allowed dial-out access shall be registered with the ICT Team.

17.7 All IT equipment permanently connected to the UCO network without a dial-out waiver but with a dial-out capability, whether enabled or not, shall be registered with the ICT Team.

17.8 IT equipment permitted dial-out access shall be configured with a firewall. The firewall shall be configured to allow only the services required in support of the dial-out access.

17.9 IT equipment permitted dial-out access shall be installed with anti-virus software and comply with the requirements and recommendations as described above (see Anti-Virus Detection and Prevention).

17.10 IT equipment permitted dial-out access should be disconnected from the UCO network either permanently or temporarily while dial-out is active, unless this interferes with its normal operation.

18. Email Security

A) Purpose & Scope

18.1 Ensuring the security of email communications is the responsibility of all users at the UCO who send or receive email via the UCO's network or from the official UCO email system, whether accessed from on or off UCO premises.

18.2 The UCO shall ensure that all email entering or leaving the UCO's network is subject to sufficient checks and filters to minimise spam messages, malicious code and safe transfer of information by email.

B) Email Filtering Service

18.3 All email entering or leaving the UCO network shall pass through an email filtering service and mail relays operated by the ICT Team or designated third parties. This includes email passing to or from departmental or group mail relays.

18.4 Email travelling entirely within the UCO network is not required to pass through the email filtering service.

18.5 The email filtering service shall provide automated scanning of email to detect potential malicious code and to identify spam.

18.6 Malicious code signatures, spam identification rules, blacklists and other mechanisms required by email scanning tools to identify new or modified threats shall be kept up to date by the ICT Team who shall checks for updates at least once a day.

C) Identification & Reporting of Malicious Code

18.7 Malicious code is defined as any executable, script, macro or other programmable feature that has the potential to damage, control or otherwise compromise the security of a user’s computer. This includes viruses, trojans, worms and spyware.

18.8 Malicious code is developed and released on a regular basis therefore users must remain vigilant for new threats which automated scanning tools may not yet be able to detect and report any suspected emails containing malicious code to the ICT Team immediately.

18.9 Email attachments from unknown sources must be scanned for malicious code before being opened; since some malicious code can fake the sender of an email, messages from known senders that are unexpected or in any way unusual must be forwarded to the ICT Team and scanned for malicious code before being opened.

18.10 Email items or attachments identified as containing malicious code or suspected of containing malicious code shall be prevented from reaching the intended recipient; the intended recipient of an infected or suspected email should be informed that the email did not reach its destination.

18.11 Users must not create or modify malicious code under any circumstances and must not knowingly send malicious code through the email system or otherwise allow it onto the UCO network by other means.

18.12 Users should report any concerns regarding malicious code to the ICT Team (ict@uco.ac.uk).

D) Identification & Reporting of Spam

18.13 Spam is defined as indiscriminate, unsolicited, bulk commercial email. It is often about subject matter that is of no interest, or offensive, to the intended recipient.

18.14 Email items identified as spam or suspected of being spam shall, where possible, be quarantined before reaching the intended recipient’s mail client.

18.15 Quarantined email items shall be reported to the intended recipient at regular intervals so that they may confirm the items have been classified correctly.

18.16 Incorrectly quarantined email items shall be released to the intended recipient when requested.

18.17 Users must not send, forward or otherwise distribute spam or chain letters.

18.18 Users should report any concerns regarding spam messages to the ICT Team (ict@uco.ac.uk).

E) Identification of Phishing

18.19 Phishing is a targeted email that requests information such as usernames and passwords from the user purporting to come from a source of authority.

18.20 Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or Information Services are commonly used to lure the unsuspecting.

18.21 Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

18.22 The UCO will never request password information via email or telephone and any such request should be reported immediately to the ICT Team (ict@uco.ac.uk).

F) Proper Use of UCO Email

18.23 Users conducting UCO business or communications via email must use a UCO provided email account.

18.24 Personal email accounts must not be used for conducting UCO business or communications.

18.25 Staff must not configure their UCO email accounts to automatically forward incoming email to services not operated by the UCO or to third party services with which the UCO has no formal agreement.

G) Emailing more than one Person

18.26 Careful thought should be given before an email is sent to more than one person in order to avoid a data security breach.

18.27 If more than one person is being sent the email and consent has not been obtained for their email address to be shared with others or shared other than for the purpose described in the UCO's Privacy Notices the email should be sent to those individuals using the Blind Carbon Copy (Bcc) field.

19. Passwords

A) Purpose & Scope

19.1 All users of UCO IT equipment are required to comply with the following minimum standards for passwords selection and use.

B) General Use of Passwords at the UCO

19.2 All IT equipment and software that supports an access control mechanism based on user accounts and passwords or PINs shall have the mechanism enabled.

19.3 All user accounts must have a password or PIN set.

19.4 Passwords for staff and students must be changed every 180 days.

C) Passwords for Multiple User Accounts

19.5 Users with multiple user accounts for different services or multiple computers should set a different password for each account.

19.6 Users should not use the same passwords for UCO and non-UCO user accounts in order to limit the damage should any one user account be compromised.

D) User Password Protection

19.7 Users must not reveal their own passwords to anyone including IT staff or system administrators. If IT staff require access to your user account they will be able to accomplish this through an administrator account or by changing your password.

19.8 All passwords must be treated as sensitive, confidential UCO information. If someone demands a password, refer them to this document or ask them to contact the ICT Team (ict@uco.ac.uk).

19.9 Users must not use the "Remember Password" feature of any operating system or application.

19.10 Users must not store passwords in a file on any computer without encryption.

19.11 Users must not write down or store passwords in any location easily accessible to others.

E) System Password Protection

19.12 IT equipment access control mechanisms shall enforce the password length, password complexity and password change requirements to ensure user compliance. In addition, IT equipment access control mechanisms shall further limit the risk of password compromise by enabling the following features where available:

- Password History Control: The access control mechanism shall prevent the reuse of a user's last eight passwords.
- Account Lockout: The access control mechanism shall prevent any further logins after multiple failed login attempts. The lockout should be for a fixed period of time or until the account is reset.
- Concurrent Connections: The access control mechanism shall prevent an excessive number of concurrent connections by the same user above and beyond those reasonably required to access authorised and necessary Information Systems.
- Grace Logins: The access control mechanism shall allow the user seven login opportunities to change their password when the password age limit is reached after which the account shall be locked.

F) Setting Passwords

19.13 Passwords must contain at least seven characters. It is recommended however that passwords contain at least twelve characters to reduce the chance of compromise by a brute-force password-cracking attack.

19.14 Passwords shall contain a combination of numbers, and upper and lower case letters.

19.15 If the access control mechanism allows it, a password should contain at least one special character (e.g. underscore, dollar, ampersand).

19.16 Passwords must not be words found in a dictionary, personal information that can be associated with the owner (e.g. birthdays, telephone numbers) or simple patterns (e.g. abc123).

19.17 The recommended process for choosing a password is:

- Think of a memorable phrase on which to base the password.
- Replace words by meaningful numbers or special symbols (e.g. to, too = 2, for = 4, and = &, money, cash = £).
- Use the first letters of the remaining words in the phrase.
- Capitalise some of the first letters.
- Replace letters by numbers or special characters that look similar (e.g. l = 1, o = 0, s = 5 or $).

20. Encryption Requirements

A) Purpose & Scope

20.1 Encryption is the process of disguising data so as to hide its substance from any casual observer gaining access to it. This is done by applying a mathematical function, known as a cryptographic algorithm or cipher, to the data to render it unreadable. A mathematical function that reverses the encryption process is used to decrypt the data. One or more unique keys are used in conjunction with the cipher to perform the encryption or decryption.

B) Information required to be Encrypted

20.2 The following types of information are required to be encrypted:

- Information that is classified as confidential, as defined in the Information Classification System, should be encrypted.
- Information that is classified as highly confidential, as defined in the Information Classification System, should be encrypted.
- Information requiring an integrity guarantee should be encrypted.
- Users requiring strong authentication of a person, service or data item should use encryption as part of the authentication technique.
- Files containing passwords or encryption keys.

C) When Encryption should be Used

20.3 Encryption should be used when information is:

- Being transferred from one device to another via USB.
- Being shared between users via email.

D) Encryption Types & Recommended Products

20.4 Only tools and products based on proven, mathematically sound cryptographic algorithms, subjected to peer review by the cryptographic community, shall be used for encryption. These may include:

- Block Ciphers: A block cipher is a cipher that is applied to a block of data (a number of characters or bits) at the same time. This is different from older ciphers which are applied to a single character at a time. For block ciphers, a minimum symmetric key length of 128 bits should be used. For long term security a symmetric key length of 256 bits is recommended. Recommended products include: 3DES, IDEA, RC5, AES, CAST, Blowfish.
- Public Key Ciphers: A public key cipher is a cipher that uses different keys for encryption and decryption. A public key is used for encryption and a private key is used for decryption. The public key cannot be used to decrypt the data and so can be freely published or given to correspondents that need to send you confidential data. For public key ciphers, a minimum asymmetric key length of 2048 bits should be used. For long term security an asymmetric key length of 4096 bits is recommended. Recommended products include: RSA, Diffie-Hellman.
- Hash Functions: A hash function is a cipher that produces a unique sequence of characters or numbers (the hash) for any different collection of input data. A hash function can be used to verify that the data has not changed since the hash was generated. Recommended products include: MD5, SHA.

- Keys: A key is a sequence of characters or numbers, like a password, that is used with a cipher to encrypt or decrypt data. All keys shall be stored safely. Where a key is secured by use of a pass phrase, the pass phrase shall be at least 12 characters in length.
- Pass Phrases: A pass phrase is a sequence of characters or numbers, like a password, that is often used to gain access to a stored key. The requirements and recommendations for password selection and password protection described in the Password Policy shall apply for pass phrases.

21. Physical Security

A) Purpose & Scope

21.1 In addition to the security of electronic information all users of the UCO are required to comply with the following minimum standards for ensuring the physical security of information systems and assets. This also applies to all third party IT equipment locally connected to the UCO network.

B) IT Equipment

21.2 Information systems shall be housed in a secure area protected by a defined security perimeter with entry controls with restricted access to ICT staff and physically sound to prevent possible break-in.

21.3 Entry control mechanisms should be enforced at all times when IT equipment is left unattended.

21.4 Where IT equipment is left unattended for significant periods (e.g. overnight or at weekends), additional security measures such as door or window alarms or motion detectors may be used.

21.5 Unauthorised personnel should be permitted into secure areas only when accompanied by authorised personnel.

21.6 Secure areas shall be operated and maintained so as to minimise the risk from theft, fire, explosion, smoke, water, dust, vibration, chemical effects, electrical supply interference or radiation.

21.7 IT equipment performing critical services or containing critical information assets should be fitted with an uninterruptible power supply to allow continued operation or controlled shutdown in the event of electrical supply interruption.

21.8 IT equipment should be maintained in accordance with the supplier's recommended service intervals.

21.9 IT equipment containing critical or important information assets shall have those assets backed up as described below (see Data Backup).

C) Servers

21.10 Servers that provide a service available to users external to the UCO network shall be configured and maintained by qualified IT staff only.

21.11 Servers that provide critical or UCO-wide services in support of teaching, research or business functions shall be configured and maintained by qualified IT staff only.

21.12 Server administrators must keep abreast of security issues for the operating systems, services and applications they are maintaining. They shall be expected to subscribe to any freely available email or other service that provides them with timely information on security issues or patches.

21.13 Servers shall be located in secure areas with a defined security perimeter with entry controls with restricted access to ICT staff and physically sound to prevent possible break-in.

21.14 Servers providing services to external users or providing critical services to internal users shall be configured with a recognised and generally accepted server operating system.

21.15 Servers shall be configured with a currently supported version of the server operating system. Currently supported means that the manufacturer provides security patches or critical updates that protect against new vulnerabilities and that the version has not been designated as ‘end of life’.

21.16 Servers shall be configured with currently supported versions of software. Currently supported means that the manufacturer or developer provides security patches or critical updates that protect against new vulnerabilities in a timely manner.

21.17 Servers shall be configured to provide only the services and resources for which they are intended. Services and applications that will not be required must be disabled.

21.18 Servers that provide access to services, resources or information that is not intended for general public access shall be protected by access-control mechanisms (e.g. passwords, firewalls). Access shall be restricted to authorised users only.

21.19 If a server or service provides a logging mechanism, access to the service shall be logged as described below (see Information Security Monitoring).

21.20 Security patches must be installed on the system as soon as is practical. The only exception to this requirement is when immediate installation would interfere with business requirements or adversely affect the service being offered.

21.21 If a security patch cannot be applied within seven days of release, the ICT Team shall be informed so that alternative security arrangements can be investigated.

21.22 Trust relationships between systems shall be avoided if other suitable authentication mechanisms are available.

21.23 The principle of “least required access” shall be used to provide services and resources.

21.24 Services shall be run from non-privileged rather than administrator accounts where it is feasible to do so.

21.25 Network communications that involve the transmission of passwords, authentication secrets or restricted information shall be encrypted, if a suitable encryption mechanism is available.

D) Data Backup

21.26 To minimise the risk of losing data in the event of a systems failure the UCO regularly backs up its data as part of its disaster recovery / business continuity plan (i.e. the ability to recover recent live data in the event of a partial or total loss of data).

21.27 Data backup covers all systems managed by the ICT department.

21.28 All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the network drives provided or UCO email services.

21.29 The data backup system has been designed to ensure that routine backup operations require no manual intervention.

21.30 The ICT department monitor backup operations and the status for backup jobs is checked on a daily basis during the working week.

21.31 Any failed backups are re-run immediately the next working day.

21.32 Full backups of all UCO data are performed weekly and are retained for 1 week before being overwritten.

21.33 Incremental backups of all UCO data are performed daily and are retained for 1 week before being overwritten.

21.34 Where possible backups are run overnight and are completed before 8am on working days.

21.35 Upon completion of backups, media copies are moved automatically to a secure remote site for disaster recovery purposes.

21.36 Backups are stored in secure locations to which a limited number of authorised personnel have access to the backup application and media copies.

21.37 Requests for backup data from 3rd parties must be approved by the Vice-Chancellor.

E) Restoring Data

21.38 Data is available for restore within a few minutes of a backup job completing on the daily schedule.

21.39 Data will be available during the retention period of each backup job which is currently defined as 1 week.

21.40 If data from more than 1 week is required to be recovered, the last full backup may be used to restore the data.

21.41 Requests for data recovery should be submitted to the ICT Team (ict@uco.ac.uk).

F) Location of & Access to Information Assets

21.42 The location of all information assets must be recorded on the UCO's Information Asset Register in line with the Information Asset Register Guidance.

21.43 Access to information assets must be restricted to users on a "need to know basis" and this must also be recorded on the Information Asset Register.

21.44 Information assets in paper format and categorised as Highly Restricted or Restricted according to the Information Classification System must:

- Be stored securely within a locked location where access is restricted to staff on a "need to know" basis.
- Not be left unattended.

21.45 All staff must "lock" their IT equipment whenever they leave their workstation throughout their working day.

21.46 All staff must sign out, log off or shut down their IT equipment at the end of their working day.

G) Clear Desk Policy

21.47 All staff must ensure that their desk / work area is cleared of paper at the end of their working day / period and ensure that this is stored and disposed of appropriately (see Information Classification System).

22. Third Party Access

A) Purpose & Scope

22.1 To ensure that information security is maintained when third parties are provided access to the UCO's information systems the minimum standards described below must be followed.

22.2 Third parties include:

- Guest-access to UCO systems.
- Third party support, maintenance & development.

B) Risks Associated with Third Party Access

22.3 It is acknowledged that there are risks associated with allowing access by third parties to the UCO's information systems including:

- Who the third party is.
- Whether they require supervision.
- What computing equipment they may have access to.
- What information they could potentially access.
- How user data may be used.
- Where user data is stored.
- Security of user data.
- Availability in the short, medium & long term.
- Whether user data is recoverable in the event of a disaster.
- Availability of support in the event of a problem.
- How the facility may change in terms of the user interface or nature of the service.
- Whether any further steps can be taken to mitigate risk.

C) Managing Risks Associated with Third Party Access

22.4 Use of informally outsourced services to store sensitive or personal data may be in breach of data protection legislation and therefore informally outsourced services must not be approved or promoted for handling confidential information.

22.5 A Privacy Impact Assessment (PIA) must be undertaken in line with the UCO's PIA Guidance at the outset of any project that will potentially involve personal data being accessed by a third party.

22.6 The EU General Data Protection Regulation (GDPR) requires that personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Only countries verified as adequate by the Information Commissioner's Office or companies registered with the US-EU Privacy Shield scheme (or equivalent) shall normally be considered for third party access.

22.7 All third parties must agree to comply with this policy.

D) Third Party Guest Access

22.8 Where third parties are providing support and maintenance of UCO information systems it may be necessary for them to access these systems at the highest level of privilege.

22.9 It is therefore essential that:

- All such privileged access to or via the UCO network is approved by the ICT Director.
- A member of UCO staff is responsible for managing the access in terms of scope, level and duration.
- All access by third parties should be monitored or logged.
- Remote access to information systems must only be permitted via secure encrypted network protocols.
- The third party should provide the UCO with the code of practice that their staff or agents must follow when handling the customer's information. It is preferable that this code of practice forms part of the agreement with the third party for provision of service

22.10 UCO members must not permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to UCO information systems.

E) Formal Outsourcing

22.11 Where the UCO is considering engagement of a third party to supply a service that may involve third party access to the UCO's information assets the project must be managed by a relevant Senior Manager and a PIA must be undertaken at the earliest opportunity.

22.12 The process of selecting a third party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that the UCO is not exposed to undue risk. This process may involve advice from members of the UCO with expertise in contract law, IT, information security, data protection and human resources.

22.13 This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to the UCO and all third parties who are given access to the UCO's non-public information or systems must agree to follow the information security policies of the UCO.

22.14 Confidentiality clauses must be used in all contractual arrangements where a third party is given access to the UCO's non-public information.

22.15 Contracts must also contain the support arrangements with third parties, especially in the event of a security breach. These will include hours of support, emergency contacts and escalation procedures.

22.16 Use of third party services must not commence until the UCO is satisfied with the information security measures in place and a contract has been signed.

22.17 All contracts with external suppliers for the supply of services to the UCO must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

F) Informal Outsourcing

22.18 Extensive IT services are available to UCO members via the internet which the UCO will have no formal agreement or contract in place with, for example email services and cloud storage providers. Users of such services are required to accept the provider's set terms and conditions which the UCO has no control over which to negotiate.

22.19 The use of such services for storing or transferring UCO information present a real risk to information security as there is no way the UCO can ensure the confidentiality, integrity and availability of the information without a formal agreement in place.

22.20 The storage of personal data with such providers is likely to be a breach of the Data Protection Act and the GDPR for which the UCO could be penalised by the Information Commissioner. Therefore wherever possible, UCO members must only use services provided or endorsed by the UCO and for the specific purpose listed in Appendix B for conducting UCO business.

22.21 The UCO acknowledges, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

22.22 UCO data which is subject to the Data Protection Act or which has a classification of Highly Restricted or Restricted must be stored using UCO facilities or with third parties subject to a formal, written, legal contract with the UCO. Those wishing to engage third parties in this way must have a formal contract in place before data is transferred.

22.23 In cases where it is necessary to remove data from the UCO, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss.

23. Retention of Information

23.1 Information shall be retained in line with the UCO's Records & Information Retention Schedule.

24. Disposal of Information

24.1 Information shall be of disposed in line with the UCO's Records & Information Retention Schedule.

25. Remote Access and Use of the Virtual Private Network (VPN)

A) Purpose & Scope

25.1 To ensure information security when working remotely and using the UCO's VPN all users are required to comply with the following minimum standards if they:

- Are remotely connecting to the UCO network from an off-site location.
- Are employing VPN technology to remotely connect to the UCO network from off-site locations via the UCO's VPN gateway.
- Require a VPN connection from the UCO network, through the firewall, to a VPN terminator outside the UCO network and operated by a third party.
- Are IT staff configuring VPN connections between UCO site locations.

25.2 "Remote access" in this context includes, but is not limited to, access achieved by dial-in modems, ISDN, ADSL and cable modems which provide narrowband or broadband access to the UCO network via the Internet.

B) Remote Access User Requirements

25.3 Remote access users should note that by connecting to the UCO they become part of the UCO network and must treat any computer connected in this way as if it were on the UCO's premises. In particular they must follow the requirements and recommendations of the ICT Acceptable Use Policy and all parts of this policy.

25.4 If remote access is used to connect to the internet via the JANET gateway, the requirements of the JANET Acceptable Use Policy must also be followed.

C) Remote Access

25.5 Remote access allows users to connect to the UCO network from an internet account provided by an Internet Service Provider (ISP) or third party network provider. The operation and maintenance of an internet account is a matter for the user and their ISP. The UCO plays no part in provision of the service.

25.6 Users should connect to the UCO network through the VMWare Horizon Client made available by the UCO for this specific purpose.

25.7 Remote access to the UCO network should be made over a secure, encrypted connection whenever this is available. Acceptable secure communication services include VPN, secure sockets layer (SSL), secure shell (SSH) and remote desktop. Insecure communications services shall be restricted but may be allowed in exceptional circumstances.

25.8 Access to services that do not provide a secure, encrypted connection should be made through a secure connection whenever possible. It is recommended that a Virtual Private Network (VPN) be used if one is available.

25.9 Users shall only attempt to connect to computers or services on the UCO network for which they are authorised.

25.10 Connections from remote locations shall be logged and may be monitored (see Information Security Monitoring).

25.11 Remote access to the UCO network is provided to allow UCO members to perform legitimate academic or administrative activities in conjunction with their work. Use of the connection shall be limited to authorised users only. The facility must not be used by family members, housemates or other persons at the off-site location.

26. Information Security Monitoring

26.1 The Regulation of Investigatory Powers Act (2000) allows authorised ICT staff to monitor network traffic for operational and security reasons.

26.2 The primary aims of network monitoring are:

- To maintain the integrity and security of the UCO network, IT equipment and information assets.
- To collect information to be used in network design, engineering, troubleshooting and usage-based accounting.

26.3 Specifically, the ICT Team may intercept network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime, gross misconduct or unauthorised use, and ensuring the efficient operation of UCO communications systems.

26.4 Information security monitoring applies to:

- All IT equipment locally connected to the UCO network.
- All IT equipment remotely connected to the UCO network whilst the equipment is connected to the UCO network.
- Email communications.

- Internet use.
- All users of the above equipment and services.

26.5 Users should also be aware that the Information Security Audits also allows for the auditing of IT equipment to investigate security breaches and monitor compliance with UCO policies and legal or contractual requirements.

27. Information Security Audits

A) Purpose & Scope

27.1 The ICT Team are authorised to conduct security audits on IT equipment in order to investigate security breaches or ensure compliance with other UCO policy, legal or contractual requirements.

27.2 Security audits shall apply to:

- All UCO owned or operated IT equipment.
- All third party IT equipment permanently or temporarily connected to the UCO network.
- All users or administrators of the above IT equipment.

27.3 Reasons for conducting information audits shall include the following:

- To investigate known or suspected security breaches.
- To monitor compliance with this policy and other legal or contractual requirements.

B) Authorisation of Information Security Audits

27.4 Information security audits shall be authorised by the ICT Director or a member of the Vice-Chancellor’s Group within the scope of this policy.

27.5 Audits shall normally be conducted by an independent auditor who is normally a member of the Senior Management Team.

27.6 All users are expected to assist and comply with authorised information security audits.

27.7 Audits should only investigate those aspects of IT equipment related to its security functions and its compliance with policies and legal or contractual requirements.

C) Types of Audit

i. Security Breach Audit

27.8 A security breach audit shall be conducted to investigate a known or suspected security breach in line with the Data Security Breach Management Policy.

27.9 An inspection of the IT equipment shall be made to attempt to discover how it was compromised and what damage was caused.

27.10 The user or administrator shall facilitate access to the system for the auditor and provide administration level access if requested.

27.11 The auditor may request that the inspection be undertaken by the administrator or a suitably knowledgeable user under the supervision of the auditor if physical access or other circumstances require this.

27.12 Information collected by authorised network monitoring activities may also be used in conjunction with information collected during the audit to draw conclusions.

ii. Policy Compliance Audit

27.13 A policy compliance audit shall be conducted to show conformance with this policy.

27.14 The auditor may require that the administrator or user provide evidence that the IT equipment complies with policy.

27.15 An inspection of the IT equipment is not required unless the evidence requested is not provided or is inconclusive.

27.16 Automated auditing tools may be used in place of manual audits to facilitate the audit process.

27.17 Information collected by authorised network monitoring activities may also be used to confirm the evidence provided.

iii. Special Audits

27.18 A special audit may be conducted in the following special circumstances:

- Where an audit is instigated at the request of a law enforcement agency investigating a criminal matter.
- Where there is a suspicion that child pornography, terrorist-related activity or other criminal activity is involved.
- Where a normal audit uncovers potential criminal activity.

27.19 In the above special circumstances at least two auditors must be present during any inspection of IT equipment or during the examination of other information collected by authorised network monitoring.

27.20 Detailed notes of the investigatory steps taken must be made within the Information Security Audit Report and signed by both auditors on completion of the audit.

27.21 Where a normal audit uncovers potential or suspected criminal activity, the audit must be stopped immediately and the IT equipment quarantined if possible.

27.22 The ICT Director or a designated representative must be informed and the Police notified immediately.

D) Outcomes of Information Security Audits

27.23 The appointed auditor shall produce an information security audit report describing the findings of the audit and the required actions, if any, to recover from a security breach or ensure compliance with policy.

27.24 The administrator or user responsible for the IT equipment shall complete all required actions at the earliest opportunity.

27.25 Information Security Audit Reports shall be considered and monitored by the Information Governance & Information Security Steering Group.

27.26 Compromised or non-compliant computers may be disconnected from the network or have their access to the UCO’s network or IT equipment restricted if their continued use is deemed to present a serious and significant threat to the security or normal operation of the UCO.

APPENDIX A: UCO INFORMATION SECURITY CHECKLIST

Key Point	✓
I only use the email address provided by the UCO for conducting all UCO business and communications.	
I do not use my personal email account for conducting UCO business.	
I have not configured my UCO email account to auto-forward incoming email to services not operated by the UCO or to third party services with which the UCO has no formal agreement.	
I ensure that I use the Bcc function to send emails to multiple people if their consent has not been obtained for their email address to be shared with others or shared other than for the purpose described in the UCO's Privacy Notices, i.e. to individuals with an external or personal email address.	
I keep my passwords secure.	
I change my passwords on a regular basis and they are a combination of numbers, letters and symbols.	
I never share my passwords or write them down on paper.	
I ensure that when my computer is not in use, it is electronically locked.	
I understand that leaving my computer open and unattended is presenting itself for a potential data breach to occur.	
I log off from my computer at the end of my working day.	
I shred any personal data that is no longer in use or dispose of it in a confidential waste bin in line with the UCO's Records & Information Retention Schedule.	
I am vigilant when opening emails from unknown senders or visiting unknown websites, as not doing this can cause the introduction of viruses and other potential harmful malware into the UCO.	
I will not send, forward or otherwise distribute spam or chain letters.	
I adopt a clear desk policy and ensure that at the end of my working day my desk is cleared of confidential information and the information is securely locked away.	
I ensure that any visitors visiting our premises should sign in and out whilst on our premises and that they are accompanied in all areas normally restricted to UCO students and staff only.	
I try to point my computer screen away from windows or doors to prevent accidental disclosure of information. If this is not possible, I ensure that I fit my screen with a privacy attachment.	
I encrypt all information that is being removed from my office or transferred to another individual as it will: • Cause damage or distress if it is lost or stolen, both to the UCO and the data subjects who may be affected. • Risk reputational damage to the UCO. • Risk heavy financial damage to the UCO in the form of a fine or compensation to those affected.	
I only use the recommended software to remotely access the UCO's network as provided by the UCO.	
I understand that I may only use cloud based storage providers that have been endorsed by the UCO as to do so otherwise presents a real risk to information security since there is no way the confidentiality, integrity and availability of the information can be assured.	
I understand that my email and internet use may be monitored and accessed by the ICT Team for legitimate purposes, e.g. in response to a subject access request, police, disciplinary or complaint investigation.	
If I discover a potential, suspected or confirmed information security data breach I will report it immediately to the Data Protection & Freedom of Information Officer (dpfio@uco.ac.uk).	

APPENDIX B: THIRD PARTY SERVICES PROVIDED OR ENDORSED BY THE UCO

N.B. This list is not exhaustive.

Third Party Service	Acceptable Use of Service	Adequacy Check
Dropbox (Dropbox Inc.)	For staff to share large volumes of documents for meetings which must be deleted once the meeting has taken place.	EU-US Privacy Shield
SurveyMonkey (SurveyMonkey Inc.)	For students and staff to carried out online surveys after which the data must be deleted.	EU-US Privacy Shield
SunSystems (Finansys Solutions Ltd)	As the UCO's financial management system.	Registered Data Controller with the Information Commission Registration Number: PZ8477178
TM2	As the UCO's Clinic Appointment system.	Hosted by the UCO
MailChimp (The Rocket Science Group LLC d/b/a MailChimp)	Marketing Communications	EU-US Privacy Shield
Podio (Citrix Systems, Inc.)	Fundraising Management	EU-US Privacy Shield