College of Osteopaths
Information Communication Technology
Acceptable User Guide

This Guide describes the acceptable computer use at the College of Osteopaths.

Scope

The College's **ICT Policy** describes acceptable computer use at the College and should be read in conjunction with this guide.

Breach of the ICT Policy will lead to investigation and may lead to disciplinary action against the offender via existing disciplinary procedures. The College reserves the right to report to the Policy any action/activity considered to be unlawful. Criminal proceedings may follow as a result.

As the College has partnership arrangements with other Universities all users of partner institutions' computer or communication systems, should be fully aware of the scope and acceptable use guides for these individual Institutions.

Definitions

"Computer", "workstation" or "system" refers to any computer or communications equipment, including data or telephone network equipment, portable computers, smartphones, etc. that belongs to or was issued by the College. If connected (including wirelessly) to the College's network, it doesn't matter to whom it belongs.

General Use

The College's computer systems are to be used for teaching, study, research and administration purposes only. As stated in the College's ICT Policy, there is limited access to PCs and laptops at the College's premises.

In line with the College's legal Prevent Duty, it is strictly prohibited to use the College's computer system to access, create, transmit, store or display terrorist or extremist material.

In order to use the College's ICT facilities, you must be an authorised member of staff and/or registered at the College. Our Service Provider (Quarry House) is responsible for issuing usernames and a password to authorised staff users. Our partner University institutions are responsible for issuing student usernames and passwords.

Commercial or distribution activities are prohibited unless formally sanctioned by the College's Senior Leadership Team,

Activities likely to damage the good name of the College are prohibited.

You must respect the rights of others and conduct yourself in a professional manner when using the College's computer systems.

You may be required to show proof of identity when onsite particularly at partner venues. Please keep your College &/or University ID card with you and be prepared to show it if asked.

Monitoring

The College's system is monitored periodically. This includes the monitoring or interception of system logs, web pages, E-mail messages, network account or any other data on any computer system owned by the College for the following reasons:

- To prevent or detect crime or to ascertain compliance with regulatory standards.
- To monitor communications in order to establish whether they are business related.
- To investigate or detect unauthorised use of telecommunication systems,
- To secure effective system operation.

All such monitoring or interception will be performed in compliance with legal guidelines, including the General Data Protection Act.

The College reserves the right to inspect and validate any items of College owned equipment connected to the network.

Any other computer equipment connect to the college's network can be removed if it is deemed to be interfering with the operation of the network.

For security /legal purposes the College's IT service provider may be asked by the College to record and keep audit data generated when users access computers and other systems at the College.

The College is legally obliged to report to the police the discovery of certain types of electronic data, if that data is found on the College's equipment or transmitted across its networks.

Prohibitions

Internet/Network

You must not try to gain unauthorised access to (hack) the College's computer system. It is a criminal offence.

You must not allow unauthorised access to occur by negligence.

You must not disseminate any information which enables others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate unauthorised access).

You must not disseminate any information which may lead to any unauthorised modification of computer materials.

You must not disseminate any material which may incite or encourage others to carry out unauthorised access or modification of computer materials.

When you use the College's computer system to gain access to remote sites it is your personal responsibility to ensure that only approved links are used. It is also your responsibility to ensure that your activities confirm to the local regulations of the site.

You must not try to access any information which you are not permitted to access.

You must not introduce any harmful or nuisance programs, files or macros onto any computer system; or take action to circumvent any precautions taken to prevent this.
You must not register any domain name, which includes the name of the College or any name, which may mislead the public into believing that the domain name refers to the College.

You must not generate, change, store, view, print or transmit information, programs or any other data that can reasonable be judged to be inappropriate or offensive to others. This includes material, which is designed to or is likely to cause annoyance, inconvenience or needless anxiety, particularly if of a threatening nature or which is intended to harass, frighten promote or encourage racism or any other discriminatory or offensive behaviour.

You must not place links to bulletin boards, which are likely to publish defamatory materials or contain discriminatory statements.

You must not connect any computer equipment (e.g. PCs, laptops) to the College network without permission.

You must not attempt to circumvent any firewall systems of the College.

Security

You must not let other people use our username or reveal your password(s) or username to anybody.

For your own security you must not leave your workstation logged in and unlocked when unattended.

General

You must not modify or delete files on the hard disks of College computers.

You must not interfere with the use by others of the computer systems. You must not remove or interfere with output belonging to others.