THE COLLEGE OF OSTEOPATHS

ICT Policy & Acceptable ICT User Guide

ICT Policy:
October 2023
Review: October 2024

Introduction

The College of Osteopaths is a small independent College, providing a service to the public and a part-time course for adult learners training to be registered osteopaths. Students attending the College are expected to have their own home access to broadband, a laptop or PC as an essential part of course registration so that they can access essential College materials that are provided online.

Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a statutory duty on Higher Education Institutions– this is known as the Prevent Duty. The 2023 update of the guidance clarified the expectations. These are to tackle the ideological causes of terrorism, by supporting and advising those at risk, through our engagement with other specialist organisations The College's compliance with this duty is monitored by the Office for Students (OfS).

Board of Governors and Trustees are ultimately responsible for ensuring compliance and are trained along with other staff to ensure that they are aware of their roles and responsibilities in relation to the Prevent Duty.

The College's Information Communication and Technology (ICT) Policy, when read in conjunction with the **'Acceptable ICT User Guide'** below sets out expectations for staff and students. The policy covers employees and regular contractors such as the clinical educators delivering training for students at the College.

The ICT policy is reflective of the limited access to equipment on site, professional healthcare expectations and the mode and delivery of the programme.

1. **Hardware**

The College's IT systems are limited in terms of computer availability and access. Access to desktop PCs is limited and use restricted to professional purposes. Desktop PCs for this purpose are in the clinics and offices.

The College provides network facilities for students to use and access resources using their own equipment. There is a separate protected network for staff. Students are unable to access the staff network.

2. **Software**

The College outsources the maintenance of the IT system to an external company who maintain and service the system and machines. They have remote access to the College networks, server and all College machine's including laptops. They manage and monitor security and can block access to unsuitable websites and report inappropriate use to the College.

3. **Email**
   3.1. Staff

The College gives designated employees access to an email facility to improve business communication and efficiency which includes communications to students. This is the primary purpose of this facility and although personal emails are permitted, The College expects staff not to abuse the facility. It is important that emails are not used to spread gossip or to distribute information, jokes or graphics that are or could be said to be, any of the following:

- sexist or sexual in nature,
- racist or otherwise discriminatory,

- obscene,
- offensive,
- defamatory,
- malicious and/or unacceptable nature,
- in conflict with any of the Colleges' policies e.g. Safeguarding and Prevent Policies
- in conflict with the interests of the College.

The distribution of chain letters or similar by email is expressly forbidden.

Staff are expected to abide by GDPR and not use emails to distribute information that is confidential in nature, unless appropriate permission has been sought or role allows.

Staff must not use emails to distribute anything that is copyright protected or to pursue or promote personal business interests. If in doubt, guidance should be sought from the appropriate line-manager

Messages sent by email could give rise to legal action against the College. It is therefore important that thought is given to the content of all emails and that hard copies are taken when necessary.

The College reserves the right to retrieve messages to assess whether the facility is being used for legitimate purposes, to retrieve information following suspected computer failure or to investigate alleged acts of wrongdoing. The College will not however, monitor emails as a matter of course.

Misuse of the email facility could result in an allegation of misconduct and disciplinary action.

3.2. Students

The University partners provide the students with an email address and this is the email the College uses to communicate with them. This email is also used to log-in to both College and University Blackboard systems. Student use of the University email address is subject to the relevant university IT use policy: and **University of Derby IT Regulations**. This account is expected to be used to communicate matters related to the programme, and learning on the course, and will be used to communicate to students. It is important that it is accessed on a regular basis.

The College emails should not be used to spread gossip or to distribute information, jokes or graphics that are or could be said to be, any of the following:

- sexist or sexual in nature,
- racist or otherwise discriminatory,
- obscene,
- offensive,
- defamatory,
- malicious and/or unacceptable nature,
- in conflict with any of the College's policies e.g. Safeguarding and Prevent Policies

- in conflict with the interests of the College.

Misuse of the email facility could result in an allegation of misconduct.

4. Social media

4.1. Staff

The use of social networking sites during working time is not permitted, unless it is for work purposes i.e. adding posts to the College Social Media platforms.

Integrity and professionalism are of upmost importance, so staff are asked to be conscious about any personal social media and online activity that could intersect with their business persona.

The College of Osteopaths respects the **Freedom of Speech and Academic Freedom** of all of its staff, but ask staff to remember that patients, colleagues, students and professional bodies often have access to any online content posted. This includes information that can be seen by more than friends and family, and Information that can easily be shared, screen shot or simply passed on.

Staff are reminded never to disclose non-public information about The College of Osteopaths (including confidential information), and to be aware that taking public positions online that are counter to the College's interests and policies might cause conflict and referral through the appropriate disciplinary channels.

Staff should never befriend a student who is studying on the programme. This can be misconstrued and give rise to conflicts of interest, as it can potentially put the member of staff in a position of power over the student.

Writing or posting anything that would embarrass or compromise The College of Osteopaths, or use of any social networking site that brings the College into disrepute, breaches the Employee Handbook, Harassment Policy or Safeguarding and Prevent, will be regarded as misconduct and could result in dismissal.

4.2. Students

Integrity and professionalism are of upmost importance for healthcare workers. Students are asked to be conscious about the social media persona that they project at the pre-registration stage as this could have a detrimental impact any future business and professional life.

The College of Osteopaths respects the Freedom of Speech and Academic Freedom of all of students but remind students that professional bodies often have access to any online content posted. Inappropriate activity or professional claims, linked to students at the College can be picked up and reported even before registration.

Writing or posting anything that would embarrass or compromise The College of Osteopaths, or use of any social networking site that brings the College into disrepute, beaches the Student Conduct & Disciplinary Policy, Harassment Policy or Safeguarding and Prevent policies, could result in an allegation of misconduct, and could result in dismissal.

5. Online behaviour

The College has certain expectations of staff and students which should be adhered to when attending virtual meetings and taught sessions. The College is using Zoom and MS Teams for teaching and meeting purposes and there is a detailed **Online Teaching Policy** covering students and staff.

This Policy includes details about expectations around:

- accessing meetings and sessions
- recording
- sending and responding to invites
- accessing recordings

Acceptable ICT Use Guide October 2023

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.