IT Policy

Policy Purpose

This policy applies to all staff who have access to the IT services including the internet, e-mail, telephones and computer equipment, including those who are home-based.

IT services operated by the College of Health are for business use. However, staff are permitted to use College of Health equipment, email and the internet for reasonable personal use. This personal use must not impact on the staff member’s work, and any excessive use may result in disciplinary action.

The College of Health reserves the right to monitor Internet, telephone and email usage by its staff to ensure that the College of Health policy is being followed. Breaches of this policy will be dealt with using the College of Health’s Disciplinary Procedure and may result in termination of employment.

Personal Responsibility

Staff who have been supplied with IT equipment are responsible for the safety of the equipment, the security of software and data stored on it and on systems accessed remotely.

If any College of Health equipment is lost or stolen, staff should contact their Line Manager and the HR Lead immediately. College of Health equipment should not be left in vehicles. Where this is not possible equipment should be stored away so it is not visible and the car locked. Under no circumstances should College of Health equipment be left in vehicles overnight. Laptops unattended overnight in the office must be locked securely away.

Staff are not to install or download unauthorised software for use on the College of Health’s IT equipment. The Chief Operating Officer determines what is authorised software. All specialist business software and apps on College of Health equipment should be used for College of Health purposes only.

Staff should at all times keep their personal passwords confidential. For example, password details should not be left on post-it notes. When changing passwords staff should adopt a complex password which does not use personal data. Passwords should be changed regularly and must never be shared or divulged to any unauthorised person.

When leaving IT equipment unattended staff should ensure equipment is password or pin code locked. When leaving the office, staff should ensure they shut down their laptops and PCs to prevent unauthorised users accessing the system, as well as conserving energy.

Staff are only authorised to use College systems and have access to College information including material on the World Wide Web which is relevant to their job. Staff should neither seek information nor use systems outside of these criteria.

Staff should be aware that they may be criminally liable by breaching the College of Health's policies in respect of the use of IT equipment, software, e-mail and the internet. The College of Health will contact the police immediately if they believe any criminal activity has taken place on College of Health equipment or on the internet or email systems.

The College of Health provides a file storage system that is routinely backed up. All confidential and essential information should be stored on these drives. Every user will have a home drive where they can store their own College of Health data. Anything stored on a computer's C or D drive, my documents or desktop is not backed up. Be very careful when using memory sticks as they can easily be lost. Only use these for sharing important information if no other suitable option is available, ensure they remain secure and delete the content when no longer required reducing any risk if a data breach in the case of loss.

Any USB device from outside the College of Health that is required to be connected to any devices must be scanned for viruses first. All College machines should do this automatically but staff should contact their Line Manager for guidance if they do not think this is the case.

General Unauthorised Use

Within the terms of this policy, the following is defined as inappropriate communication which includes any form of communication which is against the best interests of the College of Health, or which could bring the College of Health into disrepute or subject the College of Health to any legal liability.

Staff must not interfere with the work of others or the system itself. The facilities must be used in a responsible manner. In particular, staff must not:

- Create, transmit or cause to be transmitted material which is designed, or likely to cause annoyance, inconvenience, needless anxiety or offence, and must not create, transmit or cause to be transmitted offensive, obscene or indecent material;
- Create, transmit or cause to be transmitted any material about any individual, organisation or product without having taken reasonable steps to verify its accuracy;
- Create, transmit or cause to be transmitted any knowingly defamatory material, including opinions expressed about any individual, organisation or product;
- Create, transmit or cause to be transmitted material whereby the copyright of another person is knowingly infringed;
- Upload, download or open any files unless virus scanned;
- Upload or transmit any virus, worm, Trojan horse or any other similar form of program or coding whether executable or otherwise;
- Play computer games, either networked or otherwise,
- Use/access gambling sites/chat rooms;
- Create, transmit or cause to be transmitted any material that is unlawful;
- Create, transmit or cause to be transmitted any material which is vulgar, obscene or contains sexually or racially explicit language or material;

- Gain deliberate unauthorised access to facilities or services accessible via local or national networks or the world wide web;
- Transmit by e-mail any confidential information of the College of Health including information relating to any customers, suppliers or staff of the College of Health, other than in the normal course of their duties;
- Send any message internally or externally which is abusive, humiliating, hostile or intimidating;
- Gain unauthorised access to, or violate the privacy of, other people's files, corrupt or destroy other people's data or disrupt the work of other people;
- Disclose passwords to third parties without the consent of the College of Health;
- Send any message purporting to be from someone else;
- Transmit or cause to be transmitted any repetitive e-mails to bulk recipients (spamming) save in the course of their duties.

Inappropriate communication includes all of the above, but the list is not exhaustive. The use of the system for any inappropriate communication will be dealt with through the disciplinary procedure and may lead to dismissal.

General Authorised Use

The e-mail system is available for communication on matters directly concerned with the business of the College of Health. Whilst using the internet or e-mail staff must:

- Observe this policy at all times and note the disciplinary consequences of non-compliance, which in the case of a gross breach or repeated breach of the policy may lead to dismissal;
- Ensure that the College of Health's standard e-mail sign-off and disclaimer is used for all external e-mail;
- Produce and write e-mail with the care normally given to any form of written communication;
- Appreciate that e-mail is relatively insecure and consider security needs and confidentiality requirements before any transmission;
- Not knowingly disclose any unique password to any unauthorised person and make all reasonable efforts to ensure that the confidentiality of any such password is maintained.

If staff are in any doubt about sending confidential material, they should consider sending the information in another form. E-mail messages can be used as evidence in court proceedings. It is possible to enter into a legally binding contract using e-mail. Offers or contracts transmitted using e-mail are as legally binding on the College of Health as those sent on paper. While negotiating the terms of any contract, staff must take care to ensure that they do not create a legally binding contract unless they have the proper authorisation and all terms have been approved.

Copyright and Licensing

Staff have a responsibility to ensure that copyright and licensing laws are not breached when composing or forwarding e-mails and e-mail attachments. Staff must not knowingly copy any licenced software or copyright media from the internet or any other source, send, receive or copy copyright or commercially sensitive or any information in breach of the General Data Protection Regulations (GDPR) via the internet or any other source. Staff must not knowingly perform any action which could interfere with the integrity or normal operation of any internet site.

All software on College of Health equipment must be appropriately licenced.

Explicit and Illegal Material

Staff accept the risk that inbound e-mails may contain explicit or offensive material that is beyond the control of the employer. Staff must not compose, view, download, print or send any material which is embarrassing, sexually explicit, obscene or involves violence or inappropriate humour.

Viewing sexually explicit content or the downloading and/or circulation of pornography or other offensive, illegal, terrorism or obscene material or using the Internet for gambling or illegal activities constitutes gross misconduct and may result in termination of employment. "Rogue" websites exist that appear harmless but instead direct the user automatically to another website that may contain inappropriate material. If this occurs, staff should contact their Line Manager immediately.

Personal Use of Social Media

Staff are prohibited from using social media for personal use during working hours or by means of the College of Health computers, networks, mobile phones and other College of Health equipment without permission.

When logging on to and using social networking, blogs and vlogs at any time for businesses purposes, staff must not:

- Conduct themselves in a way that is detrimental to the College of Health or brings the College of Health into disrepute
- Use their work e-mail address when registering on such sites unless they have written authorisation from the Directors.
- Make comments that may damage working relationships between staff and clients of the College of Health
- Include any information about the College of Health's staff, contractors, suppliers or clients (staff may still be liable even if staff, contractors, suppliers or clients are not expressly named as long as the College of Health reasonably believes they are identifiable)
- Make any derogatory, offensive or discriminatory comments about the College of Health, its staff, contractors, suppliers or clients (a staff member may still be liable even if the College of Health, its staff, contractors, suppliers or clients are not expressly named in the websites or blogs as long as the College of Health reasonably believes they are identifiable)
- Make any comments about the College of Health's staff that could constitute unlawful discrimination, harassment or bullying
- Disclose any trade secrets or confidential information belonging to the College of Health or any information which could be used by one or more of the College of Health's competitors.
- Use online chat rooms using College of Health equipment or during working hours.

Any staff member who contravene these rules, whether inside or outside the workplace, may face disciplinary action under the College of Health's disciplinary procedure - including termination of employment.

Online Gaming

Staff are not permitted to play online games using College of Health equipment or during working hours.

Social Media, Email and Internet Monitoring

The College of Health reserves the right to monitor staff internal and external e-mails and use of the Internet, both during routine audits of the IT environment and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring include:

- Establishing the existence of facts;
- Ascertaining compliance with regulatory or self-regulatory practices or procedures;
- Ascertaining or demonstrating standards which ought to be achieved by persons using the system (e.g. quality control);
- Preventing and detecting crime;
- Investigating or detecting unauthorised use of the system, as set out in this policy;
- Ensuring the effective operation of the system;
- Checking that communications are relevant to the business of the College of Health.

If staff are absent from work, their mailbox will be checked to ensure that the College of Health responds promptly to students, patients, stakeholders and other contacts and that communications are relevant to the business of the College of Health.

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private.

When monitoring e-mails, the College of Health will, except in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where circumstances warrant it, the College of Health may open e-mails and access the content. In this case, the College of Health will avoid, if possible, opening e-mails clearly marked as private or personal.

The College of Health reserves the right to restrict, deny or remove e-mail or Internet access to or from any staff member and where using email or internet is an integral part of the staff member's job, the College of Health will assess whether or not the staff member is capable of performing their job going forward. Action following the removal of email or internet access for work purposes may include termination of employment.

The College of Health reserves the right to monitor, intercept and review, without further notice, activities using the IT resources and communications systems, including but not limited to social media postings and activities, to ensure that the rules are being complied with and for legitimate business purposes and staff consent to such monitoring by their use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

In the event of an employee ceasing employment, under this policy the College reserves the right where there is clear justifiable business reason, to access your email account.

Business Use of Social Media

Blogs and social media offer exciting and innovative ways for the College of Health to thrive. Participating in them can be a good way to expand and elevate our business presence.

If duties require staff to speak on behalf of the organisation in a social media environment, they must still seek approval for such communication from their Line Manager, who may require them to undergo training before they do so and impose certain requirements and restrictions with regard to their activities. The guidelines below apply whether staff are using social media as part of the College of Health's strategic marketing, public relations, corporate communications or recruiting activities, or as an unofficial "ambassador" on behalf of the College of Health.

If staff are contacted for comments about the organisation for publication anywhere, including in any social media outlet, they should direct the enquiry to a Director and must not respond without written approval.

If staff are authorised to use social media for business purposes this is subject to the following requirements:-

Staff will:

- Speak knowledgeably;
- Be engaging and interactive;
- Add value with their contribution;
- Not be argumentative;
- Be respectful;
- Comply with our policies;
- Protect our customers, suppliers, business associates and investors;
- Not comment on our business performance or plans (this may include ignoring rumours and saying 'no comment' if asked a direct question);
- Respect and comply with the terms of the sites that they visit;
- Act quickly to correct any mistakes.

Failure to follow these guidelines, particularly in a way that could expose us to liability, will be subject to appropriate disciplinary procedures, and may in extremely serious cases result in termination of employment.

Using College of Health Devices For Personal Use

Staff are permitted to use their College of Health devices for reasonable personal use so that is not disruptive in any way to themselves or any other staff member. Any information stored on College of Health devices including photos, music, files, downloads, emails, texts etc is College of Health property and staff should ensure that any personal items are stored on a personal device. Personal items may be ordered via the internet outside of normal working hours.

Reading and Storing Electronic Messages

In the event a staff member receives an electronic mail (eg email, WhatsApp, sms) message that contains confidential information the staff member must not disclose or use that confidential information. Misuse of the College of Health messaging systems will be considered to be misconduct and will be dealt using the College of Health's disciplinary procedure.

Viruses and Attachments

If a staff member receives an attachment or program which they consider to be suspicious, they should 'delete' promptly and inform their Line Manager. Staff should beware of incoming e-mails from an unknown source and always check that the actual email is genuine and not a forged email address (spoofing) e.g. someone pretending to be from Apple. Staff should not open e-mail attachments unless they know who they are from and are expecting them.

All incoming and outgoing external e-mails are checked for computer viruses and, if a virus is found, the message will be blocked. E-mails may also be checked for other criteria, for example, having an attached image file or containing offensive or inappropriate material. The College of Health reserves the right to block and then read these messages to ascertain whether they are business-related.

Files obtained from sources outside the College of Health may contain dangerous computer viruses that may damage the College of Health 's computer network, these files may include:

- Disks brought from home
- Files downloaded from the Internet
- Newsgroups
- Bulletin boards, or other online services
- Files attached to e-mail
- Files provided by customers or vendors
- USB flash drives and memory sticks

Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non College of Health sources without first scanning the material with approved virus checking software. If a user suspects that a virus has been introduced into the College of Health's computer network, they should notify the IT department immediately.

Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and when connected to the network users have a responsibility to conserve these resources. As such, users must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to:

- Sending mass mailings or chain letters
- Spending excessive amounts of time on the Internet
- Playing games
- Engaging in online chat groups

- Uploading or downloading large files (for example over 250mb)
- Accessing streaming audio and/or video files, or
- Otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet

Data Protection

The College of Health will comply with the provisions of the General Data Protection Regulations and abide by our Data Protection Policies.

Retention and Purging

Deletion of old e-mails is to be managed by each staff member, keeping in mind data storage levels, archival records, contractual evidence and legal discovery issues. If further information is needed regarding the length of time certain information must be kept by the College of Health, employess must contact their Line Manager.

1. Document Controls

1.1. Document Approvals

Named person(s) below indicates that this document has been reviewed and approved by the appropriate people. This document is subject to formal change control procedure.

Date	Role/Position	Name
01/12/20	Chief Operating Officer	Matt Green
13/06/24	Chief Executive Officer	Professor Christina Cunliffe

1.2. Amendment History

Date	Version	Author	Description
13/06/24	7.0	Matt Green	Minor changes