Bringing Your Own Device Policy

Policy Purpose

This policy defines the requirements to be complied with when using your own equipment for business purposes.

We recognise that many of our staff prefer to use their own personal mobile devices (such as laptops, tablets, smartphones and handheld computers), for business purposes, and that there can be benefits for both the College and staff, including increased flexibility in our working practices, in permitting such use. However, the use of personal mobile devices for business purposes gives rise to increased risk in terms of the security of our IT resources and communications systems, the protection of confidential-proprietary information and reputation, and compliance with legal obligations.

The purpose of this policy is to protect our systems and College data, and to prevent data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

No one is required to use their personal mobile device for business purposes. However, if they do so it must be in accordance with this policy.

Scope

This policy covers all employees, Associate Faculty, external consultants and contractors who use a personal mobile device including any accompanying software or hardware (referred to as a **device** in this policy) for business purposes. It applies to use of the device both during and outside office hours and whether or not use of the device takes place at your normal place of work.

This policy also applies to all devices used to access our IT resources and communications systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) desktops, smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers.

NOTE: Printouts of policy documents must be compared with the master copy on the Intranet to determine whether they are up to date.

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the document owner.

General

When you access our systems you may be able to access data about the College and its subsidiary companies, customers, clients, distributors, suppliers and other business connections, including information which is confidential, proprietary or private (collectively referred to as company data in this policy).

When you access our systems using a device, we are exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to our systems or company data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of company data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.

Appropriate Use and Compliance

You are expected to comply with all related internal policies and external regulations that the College is required to comply with. These include:

- Information Security Guidelines & Password Standards
- IT Policy
- Data Protection Policy
- Employee Handbook

The College of Health's internal policies are available on the intranet.

You should never access or use our systems or company data through a device in a way that breaches any of our other policies.

For example, you must not use a device to:

- Breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy;
- Defame or criticise us or our affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;
- Breach our Data Protection Policy;
- Breach any other laws or ethical standards (for example, by breaching copyright or licensing restrictions by unlawfully downloading software on to a device).

Connecting devices to our systems

Connectivity of all devices is centrally managed by IT Support, who must approve a device before it can be connected to our systems.

Devices that have not been provided by the College of Health and authorised for secure access must not be connected directly to the College. Access is provided for devices through the internet, and internet access is provided on College of Health sites through the appropriate wireless services. Do not attempt to connect non-College of Health devices via any wired connection.

We reserve the right to refuse or remove permission for your device to connect with our systems. IT will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, us, our staff, our business connections, our systems, or our College data at risk or that may otherwise breach this policy.

Security

You must at all times:

- Use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device.
- Secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device.
- Protect the device with a pin number or password and keep that pin number or password secure at all times.
- Not download or transfer any company data to the device, for example via e-mail attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device.

We reserve the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the College data on it for legitimate business purposes, which include (without limitation) enabling us to:

- Inspect the device for use of unauthorised applications or software;
- Inspect any College data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect College data;
- Investigate or resolve any security incident or unauthorised use of our systems;
- Conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal.

Monitoring

The contents of our systems and College data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as **content** in this policy) during the course of business or on our behalf is our property, regardless of who owns the device.

We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. 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 device, whether or not the device is in your possession.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore you should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential.

Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, in order to:

- Prevent misuse of the device and protect company data;
- Ensure compliance with our rules, standards of conduct and policies inforce from time to time (including this policy);
- Monitor performance at work; and
- Ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

Personal Data

We shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless absolutely necessary. If such access or copying occurs inadvertently, we shall delete any and all such personal data as soon as it comes to our attention. This limitation does not apply to personal data which is also College data (including personal e-mails sent or received using our e-mail system). For this reason, you are encouraged not to use work e-mail for personal purposes.

Technical Support

We do not provide technical support for devices. If you use a device for business purposes you are responsible for any repairs, maintenance or replacement costs and services.

Support will be provided by the IT Support for users attempting to gain access to an available College service.

Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist staff in connecting to our systems.

Breach

Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal. Disciplinary action may be taken whether the breach is committed during or outside office hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

Contact

If you have any questions regarding this policy or have questions about using your device for business purposes which are not addressed in this policy, please contact the Chief Operating Officer.

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
18/06/24	Chief Executive Officer	Christina Cunliffe

1.2. Amendment History

Date	Version	Author	Description
18/06/24	5.0	Matt Green	Minor changes

NOTE: Printouts of policy documents must be compared with the master copy on the Intranet to determine whether they are up to date.

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the document owner.