POLICY
IT Acceptable Use Policy

Owner:

Chief Operating Officer

THE COLLEGE
OF HEALTH

IN MANU VIS MEDENDI

Document Control

Reference: COH-HR-136
Status: Issued
Classification: Confidential
Issue No.: 2.0
Issue Date: 12/5/21
Page: 1 of 4

IT Acceptable Use Policy

Introduction

It is the responsibility of all users of the College's IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

Purpose

This Acceptable Use Policy is intended to provide an Acceptable Use framework for such use of the College's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

Scope

This policy applies to all Users of the College's IT provision including staff, students, visitors, contractors and others of the College's facilities. The College seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the College. The College also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people from being drawn into terrorism.

Unacceptable Use

The College's IT provision and Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

- Any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material; This includes pornography, hate speech, violence and promotion of terrorism;

- Unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;

- Unsolicited "nuisance" emails;

NOTE: Printouts of policy documents must be compared to 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.   P a g e | 1

- Material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the College or a third party;

- Material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;

- Material with the intent to defraud or which is likely to deceive a third party;

- Material which advocates or promotes any unlawful act;

- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or

- Material that brings the College into disrepute.

The College's IT provision & Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

- Intentionally wasting staff effort or other College resources;

- Corrupting, altering or destroying another User's data without their consent;

- Disrupting the work of other Users or the correct functioning of the College's IT Network; or denying access to the College Network and its services to other users.

- Pursuance of commercial activities

Where the College IT Provision or Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College Network.

Users shall not:

- Introduce data-interception, password-detecting or similar software or devices to the College's Network;

- Seek to gain unauthorised access to restricted areas of the College's Network;

- Access or try to access data where the user knows or ought to know that they should have no access;

- Carry out any hacking activities; or

NOTE: Printouts of policy documents must be compared to 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.   P a g e | 2

- Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User the College may in its sole discretion:

a) restrict or terminate a User's right to use the College IT Provision & Network;

b) Withdraw or remove any material uploaded by that User in contravention of this Policy; or

c) Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the User is also a member of the College (either staff or student), the College may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Policies & Regulations.

Definitions

College IT Provision & Network – all computing, telecommunication, and networking facilities provided by the College, with particular reference to all computing devices, either personal or College-owned, connected to systems and services supplied.

NOTE: Printouts of policy documents must be compared to 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.   P a g e | 3

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
12/05/21	Chief Operating Officer	Matt Green

1.2. Amendment History

Date	Version	Author	Description

136. CoH IT Acceptable Use Policy V1 MTG 120521

NOTE: Printouts of policy documents must be compared to 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.   P a g e | 4