New College of the Humanities

Acceptable Use Policy for Students (IT)

INTRODUCTION

1. Your use of the College wireless network, College computers and systems including Google Apps, and your use of any other device or system at the College or owned or operated by the College is subject to this Policy.
2. The College aims to manage its resources efficiently and to foresee and prevent avoidable, expensive problems; the College expects you to cooperate with these aims and to use good judgment.

BASICS

3. You must have a working personal device (e.g. laptop, tablet, mobile phone) with wireless capability. The College is unable to provide technical support. Having only one electronic copy of your notes and assignments is extremely risky. Hardware and software can easily fail, and the consequences of lost work can be considerable. The loss of data is not accepted as an extenuating circumstance for summative written assignments.[1] It is therefore strongly urged that you use at least one, and preferably both, of the following methods to back up your work: a) an online service such as Google Drive or Dropbox; and b) an external hard drive. Do not carry the latter about with your laptop, and at home store it securely (so that it would be unlikely to be discovered in case of a break-in).
4. The College does not accept any liability for lost or stolen equipment in or outside of the College.
5. The online College timetabling is done via CELCAT which should be accessed daily to account for any changes.
6. Unnecessary printing is strongly discouraged for environmental and cost reasons. Any printing facilities in the College are made available on a pay- per-use basis via PaperCut. Lecture notes and similar student handouts will normally be located on Canvas.

[1] Extenuating Circumstances Policy

GENERAL

7. You may, if you wish, connect to the Internet on the College's premises, free of charge, using the College's student wireless network. Availability of the network is not guaranteed and certain bandwidth-heavy applications such as video and Skype may be restricted.
8. You must not attempt to access or connect to the College's wired networks or its other wireless networks.
9. You must not attempt to connect any other device, other than your personal one (as noted in paragraph 3), to the College network.
10. You must not access, distribute, publicise or make available unsuitable, offensive or terrorist-related material. Pornographic or abusive images are strictly prohibited. This includes using webcams, cameras or video cameras for recording unsuitable or offensive images.
11. The College, its staff and its students must act and comply within a manner that falls within the UK and European Union respective legislations. This includes, but not limited, to the following:
    - Computer Misuse Act 1990
    - General Data Protection Regulation 2018
    - Human Rights Act 1998
    - Regulation of Investigatory Powers Act 2000
    - Terrorism Act 2006
    - Counter Terrorism and Security Act 2015
    - Counter-Terrorism and Border Security Act 2019
12. You must not interfere with College computers, including installing or removing hardware or software or changing their settings.
13. In the event that power supply is needed, you may only use official branded cables and chargers. You must also ensure these are safe to use and in good working condition, e.g. cables not frayed, pins not bent.
14. If you make online comments concerning the College or people at the College, e.g. on websites, Twitter or Facebook, you must use good judgment and avoid unduly bringing the College or other people into disrepute. This is also inclusive of cyber bullying.[2] [3]
15. For the academic year 2020-21, students are required to use personal devices during classes as directed by faculty. This is to support the

[2] Bullying and Harassment Policy

[3] Student Code of Conduct and Disciplinary Procedures

hybrid teaching and learning model in response to COVID-19.

THE INTERNET

16. This section relates to your use of the Internet when connected to the Colleges wireless network.

17. You must not:

    17.1. Attempt to access illegal, extremist or terrorist material on the Internet.

    17.2. Use the Internet for fraud or software piracy.

    17.3. Use point to point or peer to peer file sharing software, such as Kazaa, Limewire, etc.

    17.4. Download pirated software, games, films, music or similar materials.

    17.5. Attempt to bypass Internet filtering by use of third-party proxies or otherwise.

GOOGLE APPS

18. The College provides you with a College email address. You must not send email purporting to be on behalf of the College.

19. Students are advised to turn the notifications on for their College emails or check your College emails twice a day.

20. When you send an email to College staff you must do so from your College email account. Staff will normally only send emails to your College email account.

21. You must not send abusive email messages from your College email account.

22. You must not use your College email account to distribute spam.

23. Please remember that undertakings that you give by email are legally binding.

24. The College has no offline noticeboards, printed timetables, etc. You should check online news, calendars, timetables and announcements daily.

SECURITY

25. You must not attempt to bypass security or to gain unauthorised access to files, equipment or any other resources. This is gross misconduct. Disciplinary action may include expulsion.

26. You must use a password for your College accounts. The College may impose controls on passwords, but even if the College recommends you frequently change passwords to make them hard to guess,

passwords must:

26.1. Be at least eight characters long.

26.2. Include at least one each of numbers, uppercase letters, lowercase letters and punctuation marks.

27. You must:

27.1. Change your password several times a year and not recycle old passwords.

27.2. Keep your password secure

27.3. Not give your password to anybody else.

27.4. Change your password immediately if you believe that somebody else may know it.

27.5. Not use or attempt to obtain or use any password other than your own.

28. You must not use or install any hardware or software designed to enable 'hacking' or to spread viruses on College computers. This also includes using or installing such hardware or software on your own devices.

29. You must regularly check your device to ensure it is free from viruses etc. before bringing it into the College.

30. The College recommends against using wireless systems – including the College's – for banking, buying things with your credit card, and similar private use.

LEGAL REQUIREMENTS

31. You must ensure that all software installed on your devices has a valid licence.

32. You must comply with the law, including copyright and the General Data Protection Regulation (GDPR). The College complies with the GDPR. All College networks, systems and apps – including Google Mail, Instant Messenger, Google Apps, etc. – your communications using these College systems remain the property of the College and may be subject to Subject Access Requests (SAR) under the provisions of the GDPR.

ENFORCEMENT, MONITORING AND PRIVACY

33. College computers, any device connected to the College's networks, and services such as your Google Apps account may be subject to monitoring and filtering. Your use of such devices, networks and services is subject to your agreement to such monitoring and filtering.

33.1. This falls in line with our Prevent Policy and commitment to our statutory duty.

34. If an alleged breach of this Policy is brought to the College's attention, the allegation will be investigated. If appropriate, the College may take reasonable steps to prevent further abuse. The investigation may involve inspecting your files or email messages.

35. The College may treat failure to comply with this Policy as misconduct, leading to disciplinary action and sanctions appropriate to the seriousness of the breach. For further details, please see review the Student Code of Conduct and Disciplinary Procedures.

36. You may use College email for personal correspondence and the College Internet connection for personal purposes, but we expect you to use good judgment. College email are not completely private under the GDPR.

Title: Acceptable Use Policy for Students (IT) **Approved by: Academic Board**					
Version number	Date approved	Date published	Owner	Location	Proposed next review date
8.0	October 2020	October 2020	HROM	Academic Handbook/ policies and procedures/ general	May 2022
7.0	September 2019	September 2019	HROM	Academic Handbook/ policies and procedures/ general	May 2022
6.1	May 2018	May 2018	Facilities Manager	Academic Handbook/ policies and procedures/ general	May 2020
Referenced documents	Undergraduate Extenuating Circumstances Policy, Postgraduate Extenuating Circumstance Policy, Student Code of Conduct and Disciplinary Procedures; Student Disability Policy; Student Complaints Policy				
External Reference Point(s)	UK Quality Code Theme: Enabling Student Achievement; General Data Protection Regulation; Computer Misuse Act 1990; Human Rights Act 1998; Regulation of Investigatory Powers Act 2000; Terrorism Act 2006; Counter Terrorism and Security Act 2015; Counter-Terrorism and Border Security Act 2019				