Northeastern University
London

Acceptable Use Policy for Students (IT)

Introduction

1. The purpose of this Policy is to clarify the ways in which Northeastern University London (the University) information technology devices and systems may be used by students.

2. This Policy applies to student use of the University wireless network, University computers and systems including Google Apps. Any other device or system at the University, and devices and systems owned or operated by the University, is subject to this Policy.

3. This Policy supports the University's compliance with the Government backed Cyber Essentials Certification. This Policy supports IT Infrastructure best practices, the University's data security policies, and guidelines and regulations of relevant regulatory bodies.

4. This Policy should be read in conjunction with the following:

    4.1. Bring Your Own Device Policy

    4.2. Bullying, Harassment, and Sexual Misconduct Policy

    4.3. Data Protection Policy

    4.4. Disciplinary Procedure for Students

    4.5. Information Security Policy

    4.6. Internal Communications Policy

    4.7. Lost Property Policy

    4.8. Prevent Policy

    4.9. Safeguarding Policy

Best Practices

5. Having only one electronic copy of coursework is not advisable. 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 (see Extenuating Circumstances Policy). It is therefore advisable to use at least one, and preferably both, of the following methods to back up work: a) an online service such as Google Drive or Dropbox; and b) an external hard drive. The latter should be stored in a separate secure location.

6. The University does not accept any liability for lost or stolen equipment in or outside of the University (see Lost Property Policy).

7. Unnecessary printing is strongly discouraged for environmental and cost reasons. Any printing facilities in the University are made available on a

pay-per-use basis via PaperCut. Lecture notes and similar student handouts will normally be located on Canvas.

Terms of Use for University Systems and Devices

8. Students must have a working personal device (e.g., laptop, tablet, mobile phone) with wireless capability. The University is unable to provide technical support.
9. Students may connect to the Internet on the University’s premises, free of charge, using the University’s student wireless network. Availability of the network is not guaranteed and certain bandwidth-heavy applications such as video and Skype may be restricted.
10. Students are not permitted to connect a rooted or jailbroken mobile device to the University’s network.
11. Students must not attempt to access or connect to the University’s wired networks or its other wireless networks.
12. Students must not attempt to connect any other device, other than their personal one (as noted in paragraph 8), to the University network.
13. Students must ensure their personal device that they will use to connect to the University network and cloud services (Google) is up to date with the latest operating system version for the model, otherwise they risk having it blocked from network access. Devices that are no longer supported by the manufacturer and no longer receive official system updates present a security risk and should not be used to access the University network and resources.
14. Students must ensure the device they use to access the University's wireless network and platforms has an anti-malware/anti-virus software installed and that the software is set to update daily, scan files and web pages automatically upon access, and prevent malicious connections on the Internet.
15. Students are strongly recommended to install all released updates and firmware for the devices you are using to connect to the University’s network and data within 14 days of their release.
16. Students must ensure all applications on personal devices are installed through the device’s official application store.
17. Students 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.

18. The University, 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:

    18.1. Computer Misuse Act 1990

    18.2. General Data Protection Regulation 2018

    18.3. Human Rights Act 1998

    18.4. Regulation of Investigatory Powers Act 2000

    18.5. Terrorism Act 2006

    18.6. Counter Terrorism and Security Act 2015

    18.7. Counter-Terrorism and Border Security Act 2019

19. Students must not interfere with University computers, including installing or removing hardware or software, changing device settings, or using/attaching an external storage drive (flash drive, HDD, etc)

20. In the event that power supply is needed, students may only use official branded cables and chargers. Students must also ensure these are safe to use and in good working condition, e.g., cables not frayed, pins not bent.

The Internet

21. This section relates to your use of the Internet when connected to the University's wireless network.

22. Whether conducting themselves in the classroom or through online platforms, students must be mindful of and comply with the expectations set out in the University's policies and procedures. This includes, but is not limited to, Bullying, Harassment and Sexual Misconduct Policy; Disciplinary Procedure for Students; Prevent Policy; and Safeguarding Policy.

23. Students must not:

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

    23.2. Use the Internet for fraud or software piracy.

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

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

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

Google Apps

24. The University provides students with a University email address. Students must not send email purporting to be on behalf of the University.

25. Students must ensure their University email account is enrolled in Multi-Factor Authentication (2FA).

26. Students are advised to turn the notifications on for their University emails or check University emails twice per day.

27. Students must communicate with University staff by way of University email accounts.

28. Students must not send abusive email messages from their University email account.

29. Students must not use their University email account to distribute spam.

30. Students should remember that undertakings given by email are legally binding.

31. The University has no offline noticeboards, printed timetables, etc. Students should check online news, calendars, timetables and announcements daily.

32. Communications via University platforms should be in compliance with the Internal Communications Policy.

Security

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

34. Students must use a password for University accounts. The University may impose controls on passwords, but even if the University recommends frequently changing passwords to make them hard to guess, passwords must:

    34.1. Be at least eight characters long.

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

35. Students must:

    35.1. Change their password several times a year and not recycle old passwords.

    35.2. Keep their password secure.

    35.3. Not give their password to anybody else.

35.4. Change their password immediately if they believe that somebody else may know it.

35.5. Not use or attempt to obtain or use any password other than their own.

36. If a student suspects that one of their account passwords has been compromised or leaked, students should inform IT as soon as possible so it can be changed to prevent fraudulent use.

37. Students must not use or install any hardware or software designed to enable ‘hacking’ or to spread viruses on University computers. This also includes using or installing such hardware or software on a student’s own device(s).

38. Students must regularly check their device to ensure it is free from viruses etc. before bringing it into the University.

39. The University recommends against using wireless systems – including the University’s – for banking, buying things with a credit card, and similar private use.

Legal Requirements

40. Students must ensure that all software installed on their personal devices has a valid licence.

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

Enforcement, Monitoring and Privacy

42. University computers, any device connected to the University’s networks, and services such as the University Google Apps account may be subject to monitoring and filtering. Use of such devices, networks and services is subject to agreement to such monitoring and filtering. This falls in line with the University’s Prevent Policy and commitment to the University’s statutory duty.

43. If an alleged breach of this Policy is brought to the University’s attention, the allegation will be investigated. If appropriate, the University may take

reasonable steps to prevent further abuse. The investigation may involve inspecting student files or email messages.

44. The University 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 the Disciplinary Procedure for Students.

45. Students may use University email for personal correspondence and the University Internet connection for personal purposes, but the University expects students to exercise good judgment. University emails are not completely private under the GDPR.

Version History

Title: Acceptable Use Policy for Students (IT) **Approved by: Academic Board** **Location: Academic Handbook/ Policies and Procedures/ General/ Operations**				
Version Number	**Date Approved**	**Date Published**	**Owner**	**Proposed Next Review Date**
23.9.0	February 2023	March 2023	Director of Resourcing and Operations	May 2024
Version numbering system revised March 2023				
8.0	October 2020	October 2020	HROM	May 2022
7.0	September 2019	September 2019	HROM	May 2022
6.1	May 2018	May 2018	Facilities Manager	May 2020
Referenced documents	Extenuating Circumstances Policy, Disciplinary Procedure for Students; Support to Study Policy; Complaints Procedure for Students; Bring Your Own Device Policy; Internal Communications 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; Cyber Essentials: Requirements for IT Infrastructure.			