Richmond
American University
London

IT ACCEPTABLE USE POLICY

Introduction

1. The University view IT systems as essential tools for our employees, students, contractors, partners and agents (collectively known as Users). However, the use of those tools can expose users and the University to technical, commercial and legal risks if they are not used appropriately.

2. This policy sets out how the IT facilities provided by the University should be used, both by authorised users and by visitors.

3. The aim of this policy is to ensure that everyone using IT facilities is aware of their responsibilities and uses these facilities appropriately and within all relevant laws.

4. The use of the network is monitored for performance, and for the detection and prevention of misuse.

Scope

5. This policy applies to all individuals who use University IT systems, services or devices, including visitors.

6. This policy applies to all information, in whatever form, relating to University business activities, and to all information handled by the University relating to other organisations with whom it deals.

7. This policy also covers all IT and information communications facilities and devices owned or operated by the University or on its behalf.

Roles and Responsibilities

8. The University provides IT systems, services and devices for use in teaching, learning and administrative support functions within the University. While it is accepted that a certain amount of personal use will be made of University systems, this should be kept to a minimum, must not impact the quality or integrity of those systems, for yourself or for others, and must at all times remain within the rules set out in this policy.

Network Access and User Accounts

9. Access to the University IT systems is controlled by usernames and passwords. All usernames and passwords are uniquely assigned to named individuals, who are accountable for their activity on the University IT systems.

10. Individuals must:

10.1 Change your password, or request a new one from the IT Department, if you suspect your current password has become known by others.

10.2 Inform the IT Department immediately if for any reason you suspect a third party has access to University's data and/or systems.

11. Individuals must not:

11.1 Allow anyone else to use their credentials on any University IT system.

11.2 Leave their user accounts logged in at an unattended and unlocked computer.

11.3 Use someone else's username and password to access University IT systems.

11.4 Leave their password unprotected (for example by writing it down).

11.5 Attempt to access data that they are not authorised to use or access.

11.6 Exceed the limits of their authorisation or specific business need to interrogate University systems or data.

11.7 Store University data on any non-authorised equipment.

11.8 Give or transfer University data or software to any person or organisation outside the University without the authority of the University.

Internet and E-Mail Use

12. E-Mails and other means of electronic communication are essential to University operations. As a key business tool, such use should be limited to the University's objectives, working practices and goals.

13. The University will not tolerate the use of the internet and E-Mail system for unofficial or inappropriate purposes, including:

13.1 Using the internet or email for the purposes of harassment or abuse.

13.2 Using profanity, obscenities, or derogatory remarks in communications.

13.3 Accessing, downloading, sending or receiving any data (including images), which the University considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material, except where this is for academic research or courseware.

13.4 Using University email credentials to sign up for personal accounts.

13.5 Using the University's internet or email to make personal gains or conduct a personal business.

13.6 Using the University's internet or email to gamble.

13.7 Using University systems in a way that could affect their reliability, capacity or effectiveness, for example distributing chain letters or spam email, or using services which require excessive network bandwidth.

13.8 Publishing any defamatory information about the University online.

13.9 Publishing any internal or confidential information externally.

13.10 Sending unprotected sensitive or confidential information externally.

13.11 Forwarding University email to personal non-University email accounts.

13.12 Making official commitments on behalf of the University unless authorised to do so.

14. The University regularly backs up all E-Mails and information stored on its systems, and reserves the right to monitor and inspect usage of its electronic systems at any time without notice; this includes file data and any electronic communication sent or received by you using the University‘s systems. Such monitoring is intended to ensure this Policy is being adhered to and is effective, as well as ensuring that those using University systems are acting lawfully.

Social Media and Online Publishing

15. Guiding principles for using Social Media, either for personal use or for representing the University online, are published in the Social Media Policy

Legal Obligations

16. This Policy gives guidance on the most important legal issues which may arise from use of University‘s E-Mail system and internet access. Breaking the law could lead to one or more of the following consequences;

16.1 Civil and/or criminal liability for yourself and the University;
16.2 Disciplinary action against you including your dismissal;
16.3 Termination of any service contracts.

Breach of Copyright

17. Materials which you may encounter on the internet or receive by E-Mail are likely to be protected by copyright. Copyright applies to all written materials, software, music recordings, graphics and artwork and video clips. The Copyright Policy contains details of the obligations surrounding the use of copyright material.

18. Never download any software, music recordings or other materials that you know to be fakes or “pirate copies”.

Unwanted Contracts

19. An exchange of E-Mail messages can lead to a contract being formed. You therefore must adhere to the University‘s established policies and procedures about purchasing and contracting.

20. Never commit the University to any obligations without ensuring that you have the authority to do so. If you have any concern, please contact the Finance department.

21. You should also ensure that the person with whom you wish to enter into a contract is adequately identified. Any contract entered into via E-Mail must contain the following statement: “Any contract formed by this E-Mail will be governed and construed in

accordance with the laws of England and the parties submit to the non-exclusive jurisdiction of the English Courts".

22. Mark all E-Mails relating to contractual negotiations "Subject to Contract".

23. Beware of any attempt your recipient may make to amend or change the Terms and Conditions of the Contract.

Defamation

24. If you send an E-Mail, whether internally or externally, or post any information on the internet, containing any remark which may adversely affect the reputation of any third party, you will be exposing both yourself and the University to legal action for defamation.

25. You therefore should not send or circulate any materials which could be considered defamatory.

Unauthorised Access

26. In order to reduce the risk of unauthorised access or loss of information, the following practices should apply:

    26.1 Internal and confidential information must be protected using security features, for example: privacy screens, secure print on printers.
    26.2 Computers must be logged off or protected with a screen locking mechanism controlled by a password when unattended.
    26.3 Internal and confidential information must not be left on printers or photocopiers.
    26.4 All business-related printed matter must be disposed of using confidential waste bins or shredders.

Remote Access and Remote Working

27. It is accepted that laptops and mobile devices will be taken off-site. In addition to conditions explicitly defined in the Remote Working Policy, the following controls must be applied:

    27.1 Equipment and media taken off-site must not be left unattended in public places or visible in a car.
    27.2 Laptops must be carried as hand luggage when travelling.
    27.3 Information must be protected against loss or compromise when working remotely (for example at home or in public places).
    27.4 Particular care must be taken with the use of mobile devices such as laptops and smartphones. They must be protected at least by a password or a PIN and encryption.

Software and Licensing

28. All software on University computers must be approved by the IT Department. Users must not use any other software on University computers. Authorised software must be used in accordance with the software supplier's licensing agreements.

29. Only the University's IT Department may install software (whether paid or free, licensed or demo/trial) onto University computers.

30. All IT procurement (including software) must be managed by the IT Department (see the IT Procurement Policy.)

31. Some software licences include provision for installation on multiple devices, for example a University computer and a personal laptop. Users should check with the IT Department before installing University software onto a personal device.

    31.1 If installation on a personal device is acceptable under the software's licence agreement, the arrangement automatically ends when the user leaves the University. It is your responsibility to uninstall any University-owned software from personal devices as soon as your entitlement ceases.

    31.2 If no such provision exists, using University software licences on personal devices constitutes software piracy, and is a criminal offence.

Viruses, Malware and Cyber Security

32. Viruses and malware, including ransomware, pose a significant risk to the University's IT estate and its data. It is the responsibility of every User to remain vigilant to the potential risks, and to consult the IT Department if in any doubt. In particular, individuals must not:

    32.1 Remove or disable anti-virus software from University devices.

    32.2 Attempt to remove any virus, malware or suspected infection without consultation with the IT Department.

    32.3 Download any software, documents or media from untrusted sources or unofficial websites.

    32.4 Open or download unsolicited E-Mail attachments, or non-text attachments (e.g. software, or executable files)

33. E-Mail attachments and software downloaded from the internet, may contain computer viruses or other harmful content. You should consult the IT Department if you are in any doubt as to the authenticity of a message or attachment.

34. You must not open, download or copy any software from the Internet, before it has been checked for viruses or other harmful content.

35. Any User who knowingly distributes a computer virus or any harmful code using the University‘s IT systems will be subject to disciplinary action, which may lead to dismissal or service contract termination clauses, and potentially to criminal proceedings.

36. All Users have a responsibility to report any security incident, actual or suspected, or any threat or vulnerability of which they become aware, without delay to the IT Department.

Use of Devices

37. As an Associate of the University, you may be issued with IT equipment, for example, a computer, laptop, telephone or other device. You are responsible for the security of these items whilst they are issued to you, and it is your responsibility to ensure their immediate return in good working order to University upon termination of employment or service contract.

38. In the event of any University equipment being lost, damaged or stolen, as a direct result of your negligence, the University reserves the right to recover part or all of the cost of the repair or replacement from you.

39. If you are requested to do so, you must return all IT equipment immediately. Failure to do so may result in the appropriate value of such IT equipment being withheld from your salary or other sums otherwise owed to you until the IT equipment is returned to the University in good working order.

40. The University allows the use of privately-owned computers and other devices to process University data, both on campus and remotely. The University reserves the right to revoke this privilege on an individual basis if users do not abide by the BYOD Policy.

Data Protection and Information Ownership

41. Loss of a device containing University data must be reported to the Data Protection Officer on dpo@richmond.ac.uk, who will manage the data loss.

42. Data should be stored and edited online, if available and the downloading of data locally should be avoided whenever possible. Where data is downloaded locally this should only be stored as long as is necessary and should be deleted when no longer required.

Unacceptable Use or Activity

43. Users are expected to conduct themselves at all times in an appropriate manner. In particular, it is forbidden to:

    43.1 Perform any unauthorised changes to University IT systems, network or information;

    43.2 Connect any unauthorised device to the University network or IT systems without explicit approval of the IT Department;

43.3 Engage in any acts of hacking, including attempting to access another user's account or any form of sabotage, for example causing a denial of service (DoS) attack;

43.4 Attempt to use administrator privileges to access any University system;

43.5 Operate any system for "mining," generating or trading crypto-currency;

43.6 Generate adverse publicity or tarnish the University's name;

43.7 Disclose confidential information about the University;

43.8 Any other activity which could bring the University into disrepute.

Obligations on Leaving the University

44. All University data and equipment, for example laptops, mobile devices or other removable media, must be returned to the University at termination of contract.

45. All University data or intellectual property developed or gained during the period of employment/service remains the property of the University and must not be retained beyond termination or reused for any other purpose.

46. All University data or licensed software must be removed from personally owned devices.

Breaches of Policy

47. Breaches of this policy will be handled in accordance with the University's standard disciplinary procedures.

48. A severe breach of this policy could result in dismissal or termination of contract, and in extreme cases could lead to legal or criminal proceedings.

49. Incompetence, misconduct and/or performance issues will be addressed through standard HR policies.

Supporting Policies and Legislation

50. As well as the terms laid out in this document, the following policies are also in force. This policy expects compliance with all other related policies and legislation:

50.1 Access Control Policy

50.2 Bring Your Own Device (BYOD) Policy

50.3 Data Retention Policy

50.4 Information Security Policy

50.5 Remote Working Policy

50.6 Social Media Policy

50.7 Whistleblowing Policy

VERSION MANAGEMENT

Responsible Department: IT			
Approving Body: University Board (on recommendation of Operations Committee)			
Version no.	**Key Changes**	**Date of Approval**	**Date of Effect**
1.0	Initial Version	24 July 2025	September 2025
		Restricted Access? ***Tick as appropriate*: Yes X No ☐**	