Royal Veterinary College
University of London

IT Acceptable Use Policy

Version 6.1 (September 2024)

Contents

Document Control

Policy Version:	4.0
Policy Review Interval:	Annually by IT Strategy Group/IT Security group from the date of authorisation
Author:	Deputy Chief Operating Officer and Assistant Director of Infrastructure Services
Authorised By: **ISG Group Members:**	IT Strategy Group Group Chair: Director of Estates Head of IT Infrastructure Services Director LISD IT & Development Manager
Authorisation Date:	16th December 2015
Policy Version:	5.0
Revised by:	Acting Assistant Director of IS
Amendments:	Introduction amended Unified Communications and related sub-sections added
Re-authorised By:	IT Strategy Group
Authorisation Date:	1st August 2016
Policy Version:	5.1
Date of review:	November 2016
Revised by:	IT Governance
Amendments:	Formatting and document control updates, Contents page corrected Hyperlinks to other policies updated, No changes to policy content
Policy Version:	5.1.1
Date of review:	February 2017
Revised by:	CIO, IT Governance
Amendments:	Cross reference the Aug16 Telephony/UC amendments to new ITPOL005 No changes to policy content
Re-authorised By:	CIO
Policy Version:	5.2, 5.3
Date of review:	February 2018
Event:	Annual Review
Amendments:	CIO 'comments & mark-ups' accepted, IoT reference, Chair amendments
Re-authorised By:	Information Security Group (ISecG)
Re-authorisation Date:	July 2018
Policy Version:	5.4
Date of review:	February 2020
Event:	Annual Review
Amendments:	Microsoft Teams referenced, email usage advice updated
Re-authorised By:	Information Security Group
Re-authorisation Date:	June 2020

Policy Version:	6.0.2
Date of review:	July 2023
Amendments:	References to contacting IT Helpdesk updated, email storage reference removed and multi-factor authentication references added, software usage updated document sharing platforms and personal network equipment mis-use clarified Monitoring and logging section replaced with clarification of extent and justifications
Reviewed By:	IT Resources Manager, Infrastructure Operations Director, Director of IT, Head of IT Governance
Re-authorised By:	InfoSecG
Re-authorisation Date:	August 2023
Policy Version:	6.1
Date of Review:	September 2024
Amendments:	6.1 Annual policy review meeting DM/ES/SJ College reworded to RVC
Revised by :	Deputy COO, Director IT, IT Governance
Re-authorised by:	Information Security Group/Deputy COO
Re-authorisation Date:	November 2024

1. Policy Statement

The purpose of this Policy is to describe the obligations placed on all users of IT services of the RVC. For the purposes of this policy the term "*IT services*" refers to any IT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the Internet).

Any queries arising from this Policy or its implementation raised directly with the IT Helpdesk **by logging a call via the Service Desk Portal, or emailing the IT Helpdesk (helpdesk@rvc.ac.uk).**

2. Introduction

Any individual using the IT services has, by default, accepted this Policy and is obliged by it. Your use of IT Service may be suspended or terminated for violation of this Policy.

Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is evaluated that you have breached the policy and its requirements.

Students are directed to this policy during their registration each year and are required to acknowledge their agreed adherence to and compliance with the policy.

Staff are advised of this policy during their induction and of the RVC's requirement for them to adhere and comply with the policy.

The RVC is committed to providing the best possible IT services to all users and will, at all times, endeavor to ensure that RVC IT equipment is accessible, operates efficiently and runs suitable software.

As a user of RVC IT equipment and services, you have certain obligations which we are obliged to make clear as part of our agreement with the Joint Academic Network (Janet), the provider of our internet connection. These are outlined below and it is important that all students and staff adhere to these conditions of use as repeated breaches could result in financial penalties or loss of service to the institution or its members.

Governance: Don't break the law, do abide by RVC's regulations and policies, and do observe the regulations of any third parties whose facilities you access.

Identity: Don't allow anyone else to use your IT credentials, don't disguise your online identity and don't attempt to obtain or use anyone else's.

Infrastructure: Don't put the institution's IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.

Information: Safeguard personal data, respect other people's information and don't abuse copyright material. Remember that mobile devices may not be a secure way to handle information.

Behaviour: Don't waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world.

In general, use of RVC IT services should be for your study or research or as part of your work. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of use below or deny access for academic purposes for others.

3. User Authorisation

Access to all systems and services is controlled by a central IT account and password with multi-factor authentication configured. Students are allocated their User ID and initial password automatically as part of their registration with the RVC. Managers/supervisors of new staff are able to apply for an IT account by completing an account request form available from the Helpdesks or via the intranet which must If you have any problems getting your account set up or in using your account, you can log a call via the Service Desk Portal, or email the IT Helpdesk (helpdesk@rvc.ac.uk).

No member of IT staff will ever ask you to supply your password details either in person or by telephone or email. You should therefore assume that any request for you to do so may be a phishing attempt. This is when your account details are sought by third parties for fraudulent purposes. You should never disclose your password to anyone else and should report requests to do so to the IT Helpdesk either via the Service Desk Portal, or email (helpdesk@rvc.ac.uk). Passwords should be changed immediately if the user believes or suspects that their account has been compromised and the IT Helpdesk contacted for further advice and assistance. "Complex" passwords using a combination of upper and lower case and characters and digits should be used, 8 characters or more.

4. Compliance with Statutory *Prevent* Obligations

The RVC respects the important role universities play in the upholding the right to free speech, the RVC is also committed to its statutory obligation to challenge extremist views and ideologies whether expounded by its staff or students. This obligation is outlined in the HM Government *Prevent* Duty Guidance, 2015.

Accordingly, Library and IT facilities and equipment must not be used for any activity with the purpose of drawing people into terrorism and/or the furtherance of terrorist activity including, but not limited to:

- popularising extremist views or support for terrorism
- the sharing of extremist ideas which may be used to legitimise terrorism
- creation of an atmosphere conducive to terrorism

5. Compliance with Other Legal Obligations

There is a substantial amount of other legislation applying to the use of RVC IT services, including (but not limited to) all current UK Data Protection laws, the Computer Misuse Act, the Copyright, Designs and Patent Act, the Protection of Children Act, the Obscene Publications Act, the Sex Discrimination Act and the Race Relations Act – see section 15. for further details.

Therefore, as well as the *Prevent* related activities described under Section 4, the RVC's network infrastructure and associated IT services MUST NOT be used for:

- the creation, collection, storage, downloading or displaying of illegal offensive, obscene, indecent or menacing images, data or material capable of being resolved into such
- the downloading, copying and/or re-sale of copyrighted material such as films, music, journal papers etc. in breach of the owner's license terms and the Copyright, Designs and Patent Act
- processing personal data in a manner that does not comply with the RVC's Data Protection Policy and all current UK Data Protection legislation
- conducting activity that will harass, defame, defraud, intimidate, impersonate or otherwise abuse another person

Other conditions pertaining to the acceptable use of RVC IT infrastructure and services are:

- IT activity must not interfere with any others' legitimate use of these facilities and services
- personally owned equipment must not be used to store or transmit personal data or otherwise sensitive data owned by the RVC
- no taking or using of photographs and video of RVC clients and/or their animals without consent is permitted
- no installation, use of or distribution of unlicensed software is permitted
- no use, copying or amendment of any data or program belonging to third parties is permitted without their express consent
- all software must be used in accordance with the licensing terms of that product.
- all requests for new software to be installed or procured should be submitted via the appropriate form found on the Service Desk Portal
- no use of the RVC's IT services to disseminate unauthorised mass mailings is permitted
- no IT or associated AV equipment installed within RVC facilities should be removed, rewired or otherwise tampered with by unauthorised parties
- no use of 'torrent' applications and download sites is permitted, presenting an unacceptable risk to the institution in terms of license breaching content and malware contained
- no configuration and operation of proxy server services associated with the 'dark web' is permitted
- no use of the RVC's IT infrastructure and services to conduct commercial activity without express permission is permitted

6. Internet Access

All RVC networks connect to the Internet via Janet. All hosts on the campuses have potential access to the Internet and must be registered with IT Infrastructure Services so that they can be allocated correct network addresses and host names. Non-registered hosts will be denied access to the Internet.

All BYOD (Bring Your Own Device) and IoT (Internet of Things) equipment connecting to the RVC network must be pre-configured to work securely, or IT Helpdesk consulted for further assistance before connection is made.

7. Unified Communications

This guidance intends to make clear what constitutes legitimate use of telephones, email, instant messaging, email and the Internet and applies to all staff and students, whether using the RVC IT or personal computers/devices.

7.1. Voice and Video Calling (Telephony)

The RVC telephone platform is based on Microsoft Teams, which can be used similarly to a traditional phone system, but additionally, users are able to make video and text messaging communication using computers, smartphones and tablets. Users must only use their RVC accounts for Teams, rather than personal credentials.

Further information relating to RVC UC and telephony system usage is available in the document 'ITPOL005 Telephony & Unified Communications Acceptable Use Policy', key guidelines of these services being:

Staff

- In making use of RVC landline and mobile telephones all users are expected to act responsibly, keeping usage and costs to a minimum.
- Information must never be given out over the phone unless it is absolutely clear who it is being given to and that they are entitled to and are ready and able to accept it.
- Care must be taken to ensure that conversations involving confidential and/or personal information cannot be overheard.
- The RVC's telephones are provided primarily for business use in order to assist staff in carrying out official RVC business. RVC landline and mobile phones must not be used for any secondary business purpose unless approved as part of a formal RVC scheme.
- It is accepted that there are occasions when making personal calls at work cannot be avoided. However, it should be remembered that calls are logged and abuse of a telephone system or mobile telephone may violate this policy.
- Such monitoring of telephone use will comply with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and current UK Data Protection legislation. It will be used to establish facts, confirm legitimate business use and compliance with this Policy, monitor standards of service and training, maintain effective operation of systems and identify unauthorised use. Call logs are kept for a period of one year.
- Where the RVC has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the RVC reserves the right to record calls.

Students

- Microsoft Teams is also available for students, however, students are only able to make calls to other students and staff.

7.2. Instant Messaging

Microsoft Teams Instant Messaging (IM) facilities provides an optional, usually informal, method of communication. Use of third party messaging platforms such as WhatsApp to circulate or share RVC business information is not permitted.

- IM should be handled in the same way as other Social Media channels – you should avoid writing anything that would be considered defamatory, offensive or breaches privacy. See Social Media Policy.
- Be aware that anything that you write in an IM relating to the RVC business, can be saved by any parties in the conversation.
- IM conversations that are saved in your Outlook folder will be subject to disclosure under Freedom of Information or RVC's Data Protection Policy.
- If IM is used to provide advice to students the member of staff should handle this in the same manner as other guidance meetings: i.e. take notes, and provide a summary by email.

Students: When contacting the RVC staff, please continue to use well-known communications channels as these enable staff to manage workloads effectively.

- Email and office hours for academic staff
- Email, web-forms and phone for student services (IT Helpdesk etc.)

7.3. E-mail

Staff and students should treat email as any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.

The RVC has a duty of care to staff/students and if abusive material is received from an RVC or external account, these can be reported to the IT Helpdesk by logging a call via the Service Desk Portal, or emailing the IT Helpdesk (helpdesk@rvc.ac.uk).

Key rules of using the RVC email systems are:

- Do not pretend you are someone else when sending email.
- Do not use personal accounts to send or receive RVC related email.
- Always ensure that email usage is appropriate, timely and accurate.
- Any use of an RVC account which is deemed defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure.
- Where the RVC has reasonable grounds to suspect misuse of RVC e-mail in either scale of use, content or nature of messages, it reserves the right to audit the account concerned.
- The RVC also reserves the right to access an employee's RVC e-mail account in their unexpected or prolonged absence (e.g. – due to sickness) in order to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted by HR or the line manager before this is done, in order to provide him/her with prior knowledge.
- Be aware that the various legislation/policies of the RVC relating to written communication apply equally to email messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information and wrongful discrimination.

- Content subject to UK data protection legislation or otherwise sensitive in terms of commercial or research activity should not be included in or attached to standard unencrypted emails, please refer to IT policies on Information Handling (ITPOL002) and Encryption (ITPOL003) for further information.
- Only use email signatures that are consistent with the current advice issued by RVC External Relations and also follow the Social Media guidance issued by the RVC.
- Abide by any departmental advice issued on appropriate Subject lines, message content etc which apply to the local operational circumstances, especially where communications with external parties are involved.
- Always consider other channels of communications such as the RVC Intranet, Learn and signage systems before proposing 'mass emails' as often the content will not be applicable to many of the recipients within distribution lists used.
- If an organisation wide email is agreed for broadcast, the recipients/distribution group names should be included in the (hidden) *Bcc*: field rather than the *To*: field, for both security and avoidance of accidental replies to all.
- When creating or requesting new group/team/distribution list names for communication and collaboration purposes, ensure that a similar designation does not already exist or will appear at all misleading or unprofessional. Ensure that ownership of such groups is delegated to a new owner when a member of staff leaves the RVC.
- Remember the use of the RVC IT facilities and networks is restricted to bona fide purposes only, i.e. teaching, study, research, administration or related activities. When using these systems, you must abide by the Acceptable Use Policy.

7.4. Document Sharing Platforms

Documents must be shared via the RVC's OneDrive, Teams and SharePoint platforms (UK based), rather than via external third party platforms such as DropBox where local legislation may differ.

7.5. Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information in relation to RVC activities. However, it is legitimate for users of IT services to make use of the Internet in its various forms in the same way as email above so long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene. Inappropriate use of the Internet may be treated as misconduct under the appropriate disciplinary procedure. The RVC reserves the right to audit the use of the Internet from particular computers or accounts where it suspects misuse of the facility.

8. Personally Owned Devices

Personally owned devices must not be used to store or share RVC business information. Where it is necessary for staff to use personally owned devices for RVC work purposes, these must have up to date anti-virus and anti-malware software. Advice and guidance is available from IT Helpdesk by logging a call via the Service Desk Portal, or emailing the IT Helpdesk (helpdesk@rvc.ac.uk).

9. Using Social Media

Users of services external to the RVC such as Facebook/Twitter are expected to abide by the RVC's Social Media Policy. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. New RVC social media accounts must be cleared with External Relations before being created.

10. RVC Software and Online Resources

Computer Programs on IT equipment are protected by the law pertaining to copyright. Users must not copy software or other data without the explicit consent of the copyright owner. Similarly, online library resources including datasets, textbooks and e-journals are protected by copyright law and by license agreements. Users must not pass RVC login details to other users or people outside of the RVC. If in doubt, users should check with the RVC Copyright Officer by emailing the IT Helpdesk.

11. Remote Access

Remote access to the RVC network is possible for staff and students via the secure portal at https://rdweb.rvc.ac.uk/RDWeb/webclient/ and for staff only, via the Virtual Private Network (VPN).

Remote access from external networks or across the Internet must be made via secure methods only. Multi-factor authentication verification of credentials are required:

(see https://www.rvc.ac.uk/lisd/office-365-account/multi-factor-authentication for further details).

Further information and guidance is also available from the ISD IT Helpdesk by logging a call via the Service Desk Portal, or emailing the IT Helpdesk (helpdesk@rvc.ac.uk). Connections via the RDWeb portal or VPN are considered direct connections to the campus network. As such, using the VPN service, or generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy. All connection attempts are logged.

12. Monitoring and Logging

The RVC's IT Services log information relating to the use of its IT facilities with associated monitoring (usually automated) of the data gathered, primarily for the purposes of user authentication, network security and the detection of cyber attacks or evidence of unauthorised access (hacks) and data loss prevention (breaches).

Legitimate use of information gathered from logging and monitoring of the use of RVC IT facilities therefore includes:

• Network and data security purposes, preventing, detecting, investigating and resolving unauthorised access to or use of RVC IT systems and data.

• The effective and efficient operation, capacity and development of IT facilities and services

• Necessary compliance with Section 29 of the Counter-Terrorism Act 2015 (Prevent)

• Identification of significant risks to the well-being of members of the RVC or its visitors

• Any other lawful purpose as may arise or be imposed upon the RVC by UK legislation requirements such as requests for information from government or law enforcement agencies.

• Investigation of serious misconduct alleged of staff and student members of the RVC

• Detection and prevention of infringement of all IT security policies including this Acceptable Use Policy

In summary: Monitoring is only carried out in accordance with UK law (see section 15) including Data Protection Act 2018 and the Investigatory Powers (Interception by Businesses, etc. for Monitoring and Record-keeping Purposes) Regulations 2018, as necessary and justifiable for business purposes. No unauthorised member of the RVC (staff or student) is allowed to or attempt to monitor the use of IT facilities and services by others without explicit authority.

If you become aware that there has been unauthorised access to your computer, you must bring it to the attention of ISD by contacting the ISD IT Helpdesk by logging a call via the Service Desk Portal, or emailing the IT Helpdesk (helpdesk@rvc.ac.uk).

13. Residential Accommodation on Campuses

The RVC provides wireless and wired network connectivity in all the halls of residences.

The RVC reserves the right to permit or block network services for the purposes of security, bandwidth and traffic management, legal reasons or to protect the RVC and its reputation.

Personal equipment connected to the RVC domain and network from halls of residence must comply with certain standards (100/1000baseTX, 802.11n/ac) and the only protocol family supported by IT Infrastructure Services is TCP/IP.

Users connected to the RVC domain from halls of residence must not:

- Run Peer to Peer applications that distribute copyright material.
- Attempt DDNS dynamic Name Server Updates.
- Set up network file shares that are writable without a password.
- Re-distribute access to others, nor any RVC resource made available to them.
- Configure any device attached to the domain with any IP address not specifically allocated to them.
- Connect any form of Wireless Access point to the domain, nor configure any computer with wireless capability such that the domain can be accessed wirelessly.
- Download or distribute copyright material in breach of any licence conditions.

Neither are they permitted to run:

- DHCP servers
- DNS Servers
- Routing Protocols (such as OSPF, RIP etc)
- Network Discovery Protocols
- Internet Connection Sharing
- Port Scanners
- Web services

Virus/malware risk management is an important priority and any personal computer not adequately protected under this provision will have its access to the domain disabled - until it is quarantined, inoculated and made safe. RVC employs technologies which proactively scan for malware/P2P applications activity.

14. Breaches of This Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity and may result in disciplinary action. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

15. Recommended Reading

This policy encourages all users to familiarise themselves with the requirements, conditions and responsibilities of other related internal and external policy and legislative material that will inform their use of the RVC's IT services. These related sources are:

- RVC IT Policies
- JANET Acceptable Use Policy
- JANET Regulations Summary
- RVC's Data Protection Policy
- Obscene Publications Act 1959 **www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents** and Obscene Publications Act 1964 **www.legislation.gov.uk/ukpga/1964/74**
- Protection of Children Act 1978 **www.legislation.gov.uk/ukpga/1978/37/contents**
- Police and Criminal Evidence Act 1984 **www.legislation.gov.uk/ukpga/1984/60/contents**
- Copyright, Designs and Patents Act 1988 **www.legislation.gov.uk/ukpga/1988/48/contents**
- Criminal Justice and Immigration Act 2008 **www.legislation.gov.uk/ukpga/2008/4/contents**
- Computer Misuse Act 1990 **www.legislation.gov.uk/ukpga/1990/18/contents**
- Human Rights Act 1998 **www.legislation.gov.uk/ukpga/1998/42/contents**
- Data Protection Act 1998 **www.legislation.gov.uk/ukpga/1998/29/contents**
- Regulation of Investigatory Powers Act 2000 **www.legislation.gov.uk/ukpga/2000/23/contents**
- Prevention of Terrorism Act 2005 **www.legislation.gov.uk/ukpga/2005/2/contents**
- Terrorism Act 2006 **www.legislation.gov.uk/ukpga/2006/11/contents**
- Police and Justice Act 2006 **www.legislation.gov.uk/ukpga/2006/48/contents**
- Freedom of Information Act 2000 **www.legislation.gov.uk/ukpga/2000/36/contents**
- Freedom of Information (Scotland) Act 2002 **www.legislation.gov.uk/asp/2002/13/contents**
- Equality Act 2010 **www.legislation.gov.uk/ukpga/2010/15/contents**
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) **www.legislation.gov. uk/uksi/2003/2426/contents/made**
- Defamation Act 1996 **www.legislation.gov.uk/ukpga/1996/31/contents** and Defamation Act 2013 **www. legislation.gov.uk/ukpga/2013/26/contents**

Annexe: Service Definition for a RVC Halls of Residence Connection

1- Introduction

This document describes the service provided to students who connect to the RVC campus network via either a wireless connection or an access data socket provided in a halls of residence bedroom.

2- Purpose of Service

The connection service provides students with the means to connect their own computing equipment (typically a workstation or laptop) to the RVC data network, in order to access computing services, resources and facilities in RVC and on the Internet. The service is intended to emulate that typically provided to the home environment by an ISP using broadband or similar communications technology. By this means, it enables students to extend the electronic learning environment into their term time residence.

3- Service Description Details

Access to external networked services is essentially uncontrolled – in effect, what you might expect to be able to do from a home broadband connection, you can expect to be able to do from a halls of residence bedroom. There is however some control on outbound access in that certain specific destination "ports" are blocked where these are known to be associated with malpractice or malware.

If an external service is not working and resident would like it to be available then details of this external service should be provided to the IT Helpdesk by logging a call via the Service Desk Portal, or emailing the IT Helpdesk (helpdesk@rvc.ac.uk) for consideration, though the RVC reserves the right to permit or block services for the purposes of security, bandwidth and traffic management, legal reasons or to protect the RVC and its reputation.

4- Service Availability and Quality Expectations.

The service is generally available for 24 hours a day, 7 days a week. Any planned systems and network upgrades are announced on Intranet pages or emailed to all students/users. All major IT upgrades are agreed with senior RVC management and advance notice is given. Every effort is made to minimise the number of downtimes to the service.

5- Service Conditions

All residents must at all times comply with the RVC and Janet Acceptable Use Policy (AUP), to minimise wastage through misuse of computational and communications resources, and to protect both the integrity of the underlying IT infrastructure and the good name of RVC.

IT Infrastructure Services reserves the right to actively scan for vulnerabilities or infections on connected systems and monitor the usage. This is in order to guarantee the integrity of the network service and user compliance with this service. In any case of misuse, RVC reserves the right to suspend students' use of the Halls of Residence connection and associated services if they contravene these regulations in any way.

The use of personal wireless-based access points, routers or bridges, or the use of NAT-based routing devices and DHCP DNS Web services configured on the back of the RVC network is expressly forbidden.