Royal Veterinary College
University of London

IT Acceptable Use Policy

Version 5.3 (July 2018)

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
Review & amendments	
Policy Version:	5.0
Date of review:	August 2015
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) Deputy Director, Infrastructure Services [Chair] Head of Governance, Planning and Compliance Chief Information Officer Head of IT Governance & ISD Service Strategy Head of Students Records and Finance Business Analyst (Clinical Services) Assistant Director of Finance (Financial Services) Research Support Officer (Systems) Senior Payroll & Pensions Co-ordinator
Re-authorisation Date:	July 2018

1. Policy Statement

The purpose of this Policy is to describe the obligations placed on all users of IT services of the College. 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 helpdesk@rvc.ac.uk

2. Introduction

Any individual using the IT services is believed to have 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 College'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.

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. Students are allocated their User ID and initial password automatically as part of their registration with the College. 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 be authorised by a line manager/supervisor. If you have any problems getting your account set up or in using your account you can 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 hand over your password to anyone else and should report requests to do so to the IT Helpdesk (helpdesk@rvc.ac.uk) Passwords should be regularly changed and should be changed immediately if the user believes or suspects that their account has been compromised. "Hard" passwords using a combination of upper and lower case and characters and digits should be used.

4. Compliance with Statutory *Prevent* Obligations

The College respects the important role universities play in the upholding the right to free speech, but 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.

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 College
- 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
- no use of the College's IT infrastructure and services to conduct commercial activity without express permission is permitted
- software licencing for authorised commercial activity must be verified by consulting with the IT Helpdesk (helpdesk@rvc.ac.uk)
- no use of the College'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

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 College 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 College IT or personal computers/devices.

7.1. Voice and Video Calling (Telephony)

The College telephone platform is based on Microsoft Skype for Business, which works similarly to a traditional phone system, additionally users are able to make voice and video calls using computers, smartphones and tablets.

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 College 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 the information 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 College's telephones are provided primarily for business use in order to assist staff in carrying out official College business. College landline and mobile phones must not be used for any secondary business purpose unless approved as part of a formal College 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 College 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 College reserves the right to record calls.

Students

- The Skype for Business system is also available for students, however, students are ONLY able to make Skype for Business voice and video calls to other students and staff.

7.2. Instant Messaging

Skype for Business Instant Messaging (IM) provides an optional, usually informal, method of communication.

- 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 College 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 College 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 like 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 helpdesk@rvc.ac.uk.

Key rules of use are:

- Do not pretend you are someone else when sending email.
- Any other use of e-mail for either personal or College purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure.
- Where the College has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.
- The College also reserves the right to access an employee's RVC e-mail account in her/his unexpected or prolonged absence (eg – due to sickness) in order to allow it 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 College 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.
- Remember the use of the College 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. Use of the Internet

The primary reason for the provision of Internet access is for the easy retrieval of information in relation to College 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 as 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 College reserves the right to audit the use of the Internet from particular computers or accounts where it suspects misuse of the facility.

8. Using External Web 2.0 Services and Social Media

Users of services external to the College such as Facebook/Twitter are expected to abide by the College'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.

9. 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 login details other users or people outside of the RVC. If in doubt, users should check with the RVC Copyright Officer by emailing foi@rvc.ac.uk.

10. Remote Access

Remote access to the College network is possible for staff and students via the secure portal at https://portal.rvc.ac.uk 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. Further information and guidance is available from the ISD IT Helpdesk or by emailing helpdesk@rvc.ac.uk. Connections via the 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.

11. Monitoring and Logging

The volume of internet and network traffic and the internet sites visited may be monitored, logged and kept for an appropriate amount of time, though the specific content of any transactions will not be monitored unless there is a suspicion of improper use. Logs are taken for reasons of security, diagnostic and account/audit reasons and we are obliged to monitor to fulfill our responsibilities with regard to UK law and the Janet Code of Practice. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines. Such records and information are sometimes required - under law - by external agencies and authorities. The RVC will comply with such requests when formally submitted.

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 helpdesk@rvc.ac.uk. You should record any instances where you have accessed inappropriate sites by accident e.g. perhaps through mistyping an address.

12. Residential Accommodation on Campuses

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

The College reserves the right to permit or block network services for the purposes of security, bandwidth and traffic management, legal reasons or to protect the College 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 College 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 college 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. College employs technologies which proactively scan for malware/P2P applications activity.

13. 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.

14. 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:

- JANET Acceptable Use Policy
- JANET Regulations Summary
- RVC's Data Protection Policy

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 College data network, in order to access computing services, resources and facilities in College 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 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 College 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 College 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 College.

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 wireless-based access points, routers or bridges, or the use of NAT-based routing devices, DHCP DNS Web services is expressly forbidden.