

IT Acceptable Use Policy

(ISP01)

DOCUMENT CONTROL	3
1 POLICY STATEMENT	4
2 INTRODUCTION	4
3 USER AUTHORISATION.....	4
4 COMPLIANCE WITH LEGAL OBLIGATIONS.....	4
5 INTERNET ACCESS	5
6 USING EXTERNAL WEB 2.0 SERVICES.....	5
7 SOCIAL NETWORKING SITES.....	5
8 GOOD EMAIL PRACTICE AND 'ETIQUETTS'.....	5
9 RVC SOFTWARE AND ONLINE RESOURCES.....	6
10 REMOTE ACCESS	6
11 MONITORING AND LOGGING.....	6
12 USE OF COLLEGE IT RESOURCES FROM HoR ON CAMPUSES.....	6
13 BREACHES OF THIS POLICY.....	7
14 RECOMMENDED READING.....	7
15 SUMMARY OF CONTACTS.....	8
ANNEXE: SERVICE DEFINATION FOR AN ACCOMMODATION CONNECTION.....	9

Document Control

Policy Version:-	3.0
Policy Review Interval:-	Annually by Information Security Group from the date of

	authorisation
Author:-	Director of LISD
Authorised By:- ISG Members:-	Information Security Group Director of Estates (Chairperson) Head of IT Infrastructure Services Director of Library and Information Services Division IT and Development Manager
Authorisation Date:-	December 2014

1 Policy Statement

The purpose of this Policy is to describe the obligations placed on students and staff of The Royal Veterinary College when using IT services. 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). Students and staff who connect their own IT equipment to the College’s network are particularly reminded that such use requires compliance to this policy.

Any queries arising from this Policy or its implementation raised directly with the [Director of the Library & Information Services Division](#) or the [Head of IT Infrastructure Services](#).

2 Introduction

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. IT staff will be positive and aim to solve any hardware or software problems with the minimum of fuss or delay.

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 respect these conditions of use as repeated breaches could result in financial penalties or loss of service.

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 either of our Customer Services Managers who are [Sally Burton](#) (Hawkshead) and [Gwyn Jervis](#) (Camden).

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 either of the Customer Services Managers or the [Head of IT Infrastructure Services](#). Passwords should be routinely changed (every 90 days is recommended) 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 Legal Obligations

There is a substantial amount of legislation relevant to the use of RVC IT services, including the Computer Misuse Act, the Copyright Act, the Data Protection Act, the Protection of Children Act, the Obscene Publications Act, the Sex Discrimination Act and the Race Relations Act. Users may refer to the *Introduction to Information Technology Law* which is available from the library.

IT services must not be used for:

- the creation, collection, storage, downloading or displaying of any 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 in breach of licence conditions; such as films, music, journal papers etc which are covered by the terms of the Copyright Act
- the use of torrent sites
- the use of proxy server services such as the TOR network

There are also a number of more general conditions of use pertaining to RVC IT services:

- use of IT services must not interfere with any others' use of these facilities and service
- must not use personally owned equipment to store or transmit personal data or otherwise sensitive data owned by the College
- use only of authorised computers and/or data
- no use, copying or amendment any data or program belonging to other users without their express and specific permission

- No use of College IT services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person
- no taking or using photographs of RVC clients and/or their animals without permission
- no use of the College's IT services to conduct any form of commercial activity without express permission
- no use of the College's IT services to disseminate mass (unsolicited) mailings
- no installation, use of or distribution of unlicensed
- Use of IT services for commercial work may be governed by software licence constraints and users should verify that the intended use is permissible under the terms of those licences by contacting the [IT & Development Manager](#)
- No AV or other IT equipment in any teaching room should be unplugged or moved or otherwise interfered with

5 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.

6 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.

7 Good Email Practice and 'Etiquette'

- Sending an email from your College account is similar to sending a letter on an RVC letterhead so do not say anything that might discredit or bring embarrassment to the College.
- Don't pretend you are someone else when sending mail.
- Don't send frivolous, abusive or defamatory messages which have the potential to offend or distract the recipient from carrying out useful work (and may contravene the law).
- 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.

RVC has a duty of care to staff/students and if abusive material/emails are received from an RVC or external account, these can be reported to the Director of Library and Information Services or LISD IT & Development Manager.

8 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](#).

9 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 either of the LISD Helpdesks 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.

10 Monitoring and Logging

The volume of internet and network traffic and the internet sites visited may be monitored and 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 LISD by contacting the [IT Helpdesk](#). You should record any instances where you have accessed inappropriate sites by accident e.g. perhaps through mistyping an address.

11 Use of the College IT Services from Residential Accommodation on Campus

This service, provides network connections from College accommodation. This provides access to facilities and services on the college network, plus access to the internet and some other services.

Non-RVC owned accommodation is not directly connected to the RVC computer network and whilst internet connections may be available, these will be operated by a third party who may charge additional fees – please check with the operators of these facilities for further details.

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 (10baseT or 100baseTX) 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 fileshares 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 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.

12 Breaches of This Policy

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

13 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](#)

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 Library and Information Service 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 switches or bridges, or the use of NAT-based routing devices, DHCP DNS Web services is expressly forbidden.