Royal Veterinary College
University of London

Information Security Policy

Version 5.1.1 (August 2018)

Contents

DOCUMENT CONTROL..... 3

1 INTRODUCTION..... 4

2 WHAT MUST I KNOW? 4

3 HOW DO THE KEY PRINCIPLES RELATE TO ME?..... 5

Document Control

Policy Version:	1.0
Policy Review Interval:	Annually by Information Security Group from the date of authorisation
Author:	Director of LISD
Authorised By: **ISG Group Members:**	Information Security Group Director of Estates (Chairperson) Head of IT Infrastructure Services Director of Library and Information Services Division LISD IT and Development Manager
Authorisation Date:	December 2014
	Review & amendments
Policy Version:	3.0, 3.1, 4.0
Date of review:	December 2015
Amendments:	Minor updates
Policy Version:	5.0
Date of review:	December 2016
Amendments:	References to other policy numbers updated 'University' amended to 'College' Formatting design changed to be consistent with other policies
Revised by:	IT Governance
Re-authorised By:	Information Security Group
Policy Version:	5.1, 5.1.1
Date of review:	January 2018, August 2018
Amendments:	5.1: References to ITPOL005 updated (now including Unified Comms), UK Data Protection legislation, 5.1.1: ISecG member review, syntax changes
Re-authorised By: **ISG Group Members:**	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:	August 2018

1. Background

Information is one of the College's most important assets and each member of College has a responsibility to keep this information secure and to make sure it is only used appropriately and for its intended purpose. This information includes personal and research data and business and clinical information. If members of the College do not always take due care over the management of information it can be lost, leaked or stolen via phishing and other scams.

With these risks in mind, the College has adopted an Information Security Policy which underpins the College's approach to information management, allows it to meet its statutory obligations and provides assurances that it is doing all it can to keep its information secure. The Policy describes the expectations that the College places on its staff in maintaining information security and seeks to avoid instances of lost or misplaced information which can lead to reputational damage to the College as well as the levying of financial penalties by the Information Commissioner.

The majority of organisations know the dangers of information security breaches and some have suffered intellectual theft, serious reputational damage and in some cases fines for negligent management of data. We all have a requirement to work within the guidelines of the policy and by doing this you can help ensure the safety of your own data and that of others.

In simple terms, the most common causes of data loss or leakage can be avoided by:

- Making sure that only those who need access to data have that access.
- Not storing information where it can be accidentally exposed or lost, e.g. unencrypted USB drives and laptops.
- Making sure that if data has to be transported it is done so securely using encrypted devices or channels.

The Information Security Policy is an umbrella document for the following related policies which detail the College's approach to information security:

- IT Acceptable Use Policy (ITPOL001)
- Information Handling Policy (ITPOL002)
- Encryption policy (ITPOL003)
- Outsourcing and Third Party Compliance Policy (ITPOL004)
- Telephony & Unified Communications Policy (ITPOL005)
- Printing Acceptable Use Policy (ITPOL006)
- Incident Response Policy (ITPOL007)
- Data Storage – Backup, Restore, Retention and Cloud Policy (ITPOL008)
- Confidential Disclosure Agreement (ITPOL009)
- BYOD Policy (ITPOL10)
- Computer Account Management (ITPOL011)

2. What must I know?

- All College staff must undertake the mandatory Information Security training provided by HR Dept.
- All members of the College must understand the IT Acceptable Use Policy (ITPOL001)
- All members of the College must process information in accordance with the RVC Data Protection Policy and current UK Data Protection legislation that applies, processing any personal data with particular care.

- Researchers must comply with RVC Research Data Management Policies and Research Office procedures applying to their activities and related data processing and data retention.
- Anyone considering using third parties for the processing or storage of University information should read the Outsourcing and Third Party Compliance Policy (ITPOL004).
- Users of the College's Managed Print Service should be familiar with the Printing Acceptable Use Policy (ITPOL006)

It is not expected that all staff will become experts in information security, but staff must become familiar with the principles expressed in the related policies. Further information is contained in the table below of information security do's and don'ts.

3. How do the key principles relate to me?

The above underpinning principles of the Information Security Policy are best presented as a checklist of do's and don'ts:

Do	Don't
• Seek advice from the IT Helpdesk if you are unclear about any aspect of information security.	• Disclose your password to anyone.
• Report any loss or suspected loss of data.	• Use a personal email account for conducting University business.
• Change your password if you have any suspicion that it may have been compromised.	• Undermine or seek to undermine the security of computer systems.
• Ensure that personally owned equipment which has been used to store or process College data is disposed of securely.	• Make copies of restricted College information without permission.
• Encrypt your mobile devices and make sure that restricted information is always encrypted before it's sent to others. See ITPOL003 IT Encryption Policy.	• Provide access to College information or systems to those who are not entitled to access.
• Password protect your personally owned devices. See Information Handling Policy.	• Use your College password as the password for any other service.
• Keep all of the software on your personally owned devices up to date.	• Connect personally owned storage or mobile devices to College owned equipment if you are a member of staff or a research postgraduate.
• Comply with the law and University policies. Contact the Copyright Officer, FOI Officer and Data Protection Officer for assistance if required.	• Send unauthorised bulk email (spam).
• Be mindful of the risks of using open (unsecured) wifi hotspots or computers in internet cafes, public libraries etc.	• Leave your computers unlocked when left unattended.
• Do assume that Information Security is relevant to you.	• Leave hard copies of confidential unattended or unsecured.
• Use encrypted file attachments on emails where transmission is absolutely necessary.	• Send personal or sensitive data via non-encrypted email.

Do	Don't
• Ensure College data is saved on RVC network drives before any other storage location or service is used as a backup or share.	• Use third party cloud storage solutions that have not been authorised for College activities.