Royal Veterinary College
University of London

Outsourcing and Third Party Access Policy

Version 4.0.2 (August 2018)

Document Control

Initial Implementation	
Policy Version:	1.0, 2.0
Policy Review Interval:	Annually by Information Security Group (ISecG) from the date of authorisation
Author:	Director of LISD
Authorised By: **ISecG 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,
Date of review:	December 2015
Amendments:	None
Policy Version:	4.0
Date of review:	November 2016
Amendments:	Formatting changes, document control standardisation Reference to IT Security sub policies ITPOL001 to ITPOL006
Revised by:	IT Governance
Re-authorised By:	Information Security Group
Re-authorisation Date:	17th January 2017
Policy Version:	4.0.2
Date of review:	February 2018, August 2018, Chair approved after member circulation
Amendments:	ISG amended to ISecG, date of review amended
Re-authorised By:	Information Security Group
Re-authorisation Date:	August 2018

Contents

1. Introduction

The Outsourcing and Third Party Access Policy sets out the conditions that are required to maintain the security of the Royal Veterinary College's information and IT systems when third parties (External Organisations), other than the College's own staff or students are involved in their operation. These generally are when:

- third parties (for example contractors/engineers/consultants) are involved in the design, development or operation of information IT systems for the College. There may be many reasons for this to happen, including writing and installing bespoke software, third party hardware/software maintenance or operation of systems, to full outsourcing of an IT facility

- access to the College's information systems is granted from remote locations where computer and network facilities may not be under the control of the College.

- users who are not members of the College are given access to information or IT systems.

This access can involve a risk to the College's information, which should be assessed before the third party access is granted. Such access must be subject to appropriate conditions and controls to ensure the risk can be managed. Other occasions may arise where third parties require access to information systems. This policy will also apply in these situations.

2. Policy Statements

All third parties who are given access to the College's information systems, whether suppliers, customers or otherwise, must agree to follow the College's Information Security Policy.

The College will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the College will require external suppliers of services to sign a confidentiality agreement to protect its information assets.

Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the College's Information Security Policy and its sub policies (ITPOL001 to ITPOL006).

All contracts with external suppliers for the supply of services to the College must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

Any facilities management, outsourcing or similar company with which this College may do business must be able to demonstrate compliance with the College's Information Security Policy and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.