Royal Veterinary College
University of London

BYOD Policy

(Bring Your Own Device)

Version 1.2 (August 2018)

Contents

Document Control

Policy Version:	1.0
Policy Review Interval:	Annually by the Information Security Group (ISecG) from the date of authorisation
Author:	IT Governance
Authorised By: **ISecG Members:**	Information Security Group Deputy Director, Infrastructure (Chair) Deputy COO and Director of Infrastructure Chief Information Officer Head of Governance, Planning and Compliance Head of IT Governance & ISD Service Strategy
Authorisation Date:	13th January 2017
Review & amendments	
Policy Version:	1.1
Date of review:	February 2018
Amendments:	Updated to reflect ISD restructure, GDPR added to DPA compliance
Authorised By:	-
Authorisation Date:	-
Review & amendments	
Policy Version:	1.2
Date of review:	June 2018
Amendments:	UK Data Protection legislation referenced, August 2018 Chair approved following member circulation
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
Authorisation Date:	August 2018

1 Policy Statement

The purpose of this document is to identify required and recommended IT practices around the use at the Royal Veterinary College of non-College owned IT equipment such as laptops, tablets and smartphones in the practice commonly referred to as BYOD – bring your own device and latterly as BYOE – bring your own everything (as further categories of devices have become able to access the Internet and College networks).

In order to maintain infrastructure security and minimise any potential loss or corruption of College data, BYOD devices are also subject to the IT security and data handling policies in place to mitigate risks posed to the institution and allow its legal and operational obligations to be met. In particular, the College must remain in control of any personal data for which it is responsible regardless of the ownership of any devices used in conjunction with such data. It is a user's responsibility to maintain the security of their personal equipment if used for College related activities, where necessary measures to ensure the appropriate management and controls of devices will distributed via the College network through system polices or management applications such as Microsoft InTune.

The network infrastructure and IT resources created for Internet access and the storage of data are provided for purposes of legitimate College and academic activities, users of personal IT equipment should be aware that the IT Acceptable Use and its associated policies still apply to use within the institution and for remote access.

2 Scope

This policy applies to the following:

- all users of the College IT infrastructure and services
- access to and storage of College data using personally owned equipment (i.e. BYOD)
- additional responsibilities and recommendations for RVC staff accessing College data
- using BYOD equipment on RVC premises
- using BYOD equipment for remote access to College IT services

3 BYOD requirements

3.1 Password/PIN protection

All BYOD equipment must be password or PIN number protected (or use equivalent biometric facilities to personalise log ins).

3.2 Anti-virus measures

All BYOD equipment must be configured with a fully functioning and updating anti-virus package, if necessary these can be obtained via links from the ISD webpages. This requirement applies to all classes of device and operating systems.

3.3 Sensitive data storage

Users should not store or access personal, confidential or commercially sensitive College data on unencrypted personal storage devices or where other users would have easy access to the data due to shared access or common data drives.
All data processing should comply with the current UK Data Protection legislation and associated RVC IT policies. Staff needing to access such data for their roles should approach IT Purchasing with a business case supported by their department for a suitable College device to be provided.

3.4 Notification
Where a loss of personal equipment that has been used for BYOD and holding or potentially holding RVC data occurs, the loss should be reported to the IT Helpdesk for assessment any institutional risk. If necessary the loss will be escalated to the College Data Protection Officer. If a loss of College data on the personal device is definite and significant the loss should be reported immediately to helpdesk@rvc.ac.uk and data@rvc.ac.uk rather than any delay made whilst loss of the physical device is investigated.

3.5 Domestic networks
Users should ensure that their domestic IT (broadband) networks are configured securely before accessing RVC IT systems remotely or processing College data.

3.6 Public 'wifi hotspots'
Users should not access RVC IT systems or process College data whilst connected to public wifi hotspots where the security measures in place are unconfirmed, they are almost certainly insecure if 'open'.

3.7 Third party cloud storage
Users should not upload any College data to unauthorised third party cloud locations that they or the College do not specifically authorise and verify the security of, first consult ISD's IT Helpdesk on Microsoft OneDrive provision.

3.8 General security
Remote and off premises mobile users of all devices should ensure all reasonable measures have been taken to ensure both the physical and logical security of their 'IT' for their own safety and that of College data. Such measures would include the use of up to date applications and operating system software, use of both firewall and anti-virus software and ensuring that data remains backed up on the College servers.

3.9 Equipment disposal
Users must be aware once a device has been used in conjunction with College data, that all College data should be removed and/or deleted prior to the device's disposal and/or selling on.

4 Preventative measures

In order to secure all access and ensure that BYOD equipment complies with the College IT security standards, devices accessing certain IT systems such as wifi networks, portals and VPN services may be scanned for details of their OS and antivirus configuration and where necessary additional applications or fixes automatically applied to make the device secure on the network.

Staff using personal devices for work activities should regularly assess any personal data processing aspects and rather than place themselves or College in a position that is not compliant with current UK Data Protection legislation approach the ISD IT Helpdesk for advice or IT Purchasing with a brief business case for more suitable College equipment to be provided to them.