RVC Royal
Veterinary
College
University of London

IT Encryption Policy

Version 3.2.1 (August 2018)

Contents

Document Control

Initial Implementation	
Policy Version:	1.0.
Policy Review Interval:	Annually by Information Security Group from the date of authorisation
Author:	Director of LISD
Authorised By:	Information Security Group
ISecG Group Members:	Vice Principal Operations (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:	2.0
Date of review:	October 2015
Amendments:	None
Policy Version:	3.0, 3.1
Date of review:	October 2016
Amendments:	Data Protection Officer link amended from S Jackson to M Grigson Reference to AC20 Data Quality and Management Policy Encryption standards specified Mandatory encryption of all RVC purchased portable computers specified Provision of encrypted portable storage devices via IT Purchasing Advice on data types requiring encryption Email and encryption
Revised by:	IT Governance
Re-authorised By:	Information Security Group
Re-authorisation Date:	17th January 2017
Policy Version:	3.2.1
Date of review:	February 2018, August 2018 Chair approved following member circulation
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
Amendments:	LISD references amended to ISD following restructure, review date amended
Re-authorisation Date:	August 2018

1. Introduction

This IT Encryption Policy sets out the principles and expectations of how and when information should be encrypted and the use of encryption for RVC owned portable devices and storage. This advice should be used in conjunction with the 'AC20 RVC Data Quality and Management Policy' that applies, describing the responsibilities of staff in handling, maintaining and securing accurate and reliable data at the RVC.

2. Definition

Encryption is the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

3. When to use encryption

Encryption must always be used to protect strictly confidential information transmitted over data networks to protect against risks of interception. This includes when accessing network services which require authentication (for example, usernames and passwords) or when otherwise sending or accessing strictly confidential information (for example, in emails).
Where confidential data is stored on or accessed from mobile devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders) the devices themselves must be encrypted (using "full disk" encryption), irrespective of ownership.

Where strictly confidential data is stored in public, cloud based storage facilities the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data. Where data is subject to an agreement with an external organisation, the data should be handled (stored, transmitted or processed) in accordance with the organisation's specified encryption requirements.

3.1 Email and encryption

In relation to email, any personal or commercially sensitive data should only be sent via the College email system when absolutely necessary and where that is true, the data must be sent in an encrypted form. The recommended method would be to attach the data as an encrypted file to one email then sending the recipient details of how to decrypt in a separate email in order to reduce the chances of interception or any accidental or malicious distribution of the sensitive data. Utilities such as the 7-Zip application installed as a standard package on RVC PCs offer an easy method to encrypt files before transmission.

4. Key management

In most cases, encryption keys will be in the form of a password or passphrase. Losing or forgetting the encryption key will render encrypted information unusable so it is critical that encryption keys are effectively managed. When devices are encrypted by IT Helpdesk staff, ISD will take responsibility for the secure management of the keys. In all other cases, it will be the individual member's responsibility to manage the keys. It is advisable to make secure backups of your keys and to consider storing copies with trusted third parties.

5. Encryption standards

There are many different encryption standards available. Only those which have been subject to substantial public review and which have proven to be effective should be used. Specific guidance is available from the IT Helpdesk and/or the Data Protection Officer.

All new laptops, tablets and portable storage devices purchased through IT Purchasing will be supplied with encryption pre-installed and enabled. Any memory stick or USB storage device may have encryption applied through an appropriate software tool. The encryption standards used for securing RVC purchased devices are:

BitLocker	AES-XTS standard, built into Microsoft Windows
FileVault2	AES-XTS standard, built into Mac OSX

Advanced Encryption Standard (**AES**), also known as **Rijndael** (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES uses a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES keys for RVC devices will be securely stored on servers for future support purposes and will be routinely backed up to prevent loss.

Note, the project group developing the popular TrueCrypt freeware encryption utility was suspended in May 2014 so that application is no longer recommended.

6. UK law

Failure to comply with this policy may result in prosecution of the College or an individual member of the College in relation to data breaches, identity theft, fraud or distress resulting in fines up to the limit of £500,000 and/or damage to the College's reputation and relationship with stakeholders or professional associates.

Export regulations relating to cryptography (encryption) are complex, but so long as the encryption software used to encrypt a device or file is considered to be a "mass market" product it is unlikely that you will encounter any problems leaving or re-entering the UK. That said, you may be required to decrypt any devices or files by UK authorities on leaving, entering or re-entering the country. If you are requested to decrypt your files or devices you are advised to do so.
Section 49 of the Regulation of Investigatory Powers Act (RIPA) includes a provision whereby certain "public authorities" (including, but not limited to law enforcement agencies) can require the decryption of devices or files. Failure to comply with such a lawful request is a criminal offence in the UK.

7. Travelling abroad

In addition to what has been written above about export regulations, you should also be aware that government agencies in any country may require you to decrypt your devices or files on entry or exit from the country. If you are travelling abroad with encrypted confidential data this means that there is a risk that the data may have to be disclosed and you should consider the consequences of this. Wherever possible, do not take confidential data with you when you travel (keep the data at the University and access it using the University's secure, remote access facilities).

Particular attention should be paid to the possible inadvertent export of data subject to the Data Protection Act to countries outside of the EEA (or the few other countries deemed to have adequate levels of protection) when travelling.

8. RVC mobile devices and portable storage media

All new laptops, tablets and portable storage devices purchased through IT Purchasing will be supplied with encryption pre-installed and enabled. Windows laptops purchased through IT Purchasing will feature the necessary TMP (Trusted Platform Module) that makes the encryption process straightforward and any memory sticks purchased through IT Purchasing will be have the necessary encryption capability included.

NB. As with other IT and data security guidelines, encryption and data quality and management policies apply to all operating systems and versions in use – Windows, Apple Macintosh, Android and Linux. If in doubt contact the IT Helpdesk for further advice.

Unencrypted laptops and portable media (potentially those purchased before October 2016) that are used for College business and holding College data should be logged with the IT Helpdesk (helpdesk@rvc.ac.uk) for an encryption process to be applied, or users should restrict them from off-site use.

8.1 Smartphones

College supplied smartphones offer built-in encryption via a passcode that should be enabled and used at all times. The use of smartphones for storing College data is not recommended, if it is absolutely necessary to use these devices for activities involving College data, cloud solutions (Microsoft OneDrive) would be advised over storing on the smartphone's internal storage.

9. Data requiring encrypting

The need for data encryption applies to data that may be regarded as confidential or sensitive where loss (through data corruption or theft) would result in financial or reputational damage to the College or result in a breach of the Data Protection Act under which the individual or institution may be prosecuted.

All RVC staff are responsible for their safeguarding of College data under the Data Protection Act and regular training is mandatory in order to be informed of appropriate measures for handling data correctly.

Examples of circumstances where staff should be especially careful in their actions includes;

- Using public wi-fi access points or third party computers that are not guaranteed to possess adequate security levels
- Transporting laptops, tablets or storage media where theft or loss is more likely to occur than when working on campus
- Storing of documents, spreadsheets, images on mobile devices or equipment at home, including synchronisation with cloud services
- Sending and reading e-mails and email attachments – unencrypted attachments may be intercepted, or unintentionally mishandled by the recipient

Data that should receive consideration under the Data Protection Act includes:

- Data sets relating to living, identifiable individuals, including, students, staff, alumni, research participants.
- Any information relating to living, identifiable individuals which might potentially be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary related information, staff performance, grading, promotion or personal and family lives.
- Information relating to current students' or alumni programmes of study, grades, records or their personal lives.
- Data relating to living, identifiable individuals' health, disability, ethnicity, sexual health, political or religious affiliations, trade union membership or criminal offences/convictions.
- Any Financial related data held in Agresso.
- Any identifiable client details from Hospital Patient Records Systems
- Any information that has been provided to the College in confidence.
- Data relating to the medical records of any living, identifiable individual.
- Business related data that would be likely to disadvantage the College in its funding, commercial or policy negotiations.
- Meeting papers or data relating to proposed changes College strategies, policies or procedures, before the changes are agreed and announced.

- Security arrangements for high profile or vulnerable visitors, students and events whilst the confidentiality of arrangements are still relevant.
- Any data or information that would attract legal professional privilege.
- Information relating to identifiable research participants, other than information that is already in the public domain.

Where data is not confidential or commercially sensitive with little impact if lost or stolen then there can be greater freedom in its storage and transmission but as good practice, users are encouraged to exercise caution and carry out reasonable precautions at all times by considering:

- Does the data need to be carried on portable devices or transmitted to third parties.
- Does the data need additional controls before proceeding ie coming under the Data Protection Act.
- What actions could be taken to reduce the associated risk, for example anonymizing records or reducing the amount of data included.
- Will data held on portable media be used in conjunction with public wi-fi or public computers where there is a greater risk of malware or hacking.

9.1 Research data

It should be noted that there are extra considerations surrounding research data as this may be subject to additional restrictions under the terms of their awards and governance within the ISO standards that apply. For further information, contact the Research Office and/or ISD Research Data Manager.