Royal Veterinary College
University of London

Information Handling Policy

Version 3.1.3 (August 2018)

Contents

Document Control

Policy Version:	1.0
Policy Review Interval:	Annually by the Information Security Group from the date of authorisation
Author:	Director of LISD
Authorised By:- **ISecG Members:-**	Information Security Group (ISecG) Director of Estates and Campus Services (Chairperson) Director of Library and Information Services Division LISD IT and Development Manager Head of IT Infrastructure Services
Authorisation Date:	December 2014
Review & amendments	
Policy Version:	2.0
Date of review:	December 2015
Amendments:	None
Policy Version:	3.0
Date of review:	November 2016
Amendments:	Formatting changes, document numbering standardisation Cross references to related the new 'AC20 Data Quality and Management Policy' and other existing polices added Specification of example data needing consideration
Revised by:	IT Governance
Re-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
Review Date:	July 2018
Policy Version:	3.1.3
Amendments:	Update policy relating to UK Data Protection legislation amendments (GDPR)
Revised by:	IT Governance
Re-authorised By: **ISecG 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. Introduction

This Information Handling Policy is a sub-policy of the Information Security Policy and sets out the requirements relating to the handling of the College's information. Information must be managed correctly in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur. This policy operates in conjunction with other information and data related policies to ensure suitable governance of the College's assets:

- RVC Data Protection Policy
- All current UK Data Protection legislation.
- ITPOL001 Acceptable Use Policy covering the appropriate use of the College's IT systems.
- ITPOL003 IT Encryption Policy covering requirements for data security on devices and storage media.
- AC20 Data Quality and Management Policy provides further guidance on the requirements for College data to be accurate, valid, complete, relevant, timely and reliable.

2. Inventory and ownership of information assets

An inventory of the College's main information assets will be developed by the Business Intelligence Group and reviewed on a regular basis. Organisational units will have nominated owners who will be assigned responsibility for identifying departmental or organisational units' assets so that appropriate security measures may be put in place to protect the information/data.

3. Security classification

Each information asset category will be assigned a security classification by the asset owner which reflects the sensitivity of the asset according to the following classification scheme:

- Public – available to any member of the public without restriction.
- Open – available to any authenticated member of the College.
- Confidential – available only to specified members, with appropriate authorisation.
- Strictly Confidential – available to only a very small number of members, with appropriate authorisation.
- Secret – the most restricted category. It is not anticipated that many College assets will be assigned this classification.

Any information which is dis-closable under the Freedom of Information Act 2000 will be classified as public. Any data which is classified as sensitive personal data under the Data Protection Act 1998 (or its successor legislation) will be classified as strictly confidential. Any information which is not explicitly classified will be classified as open, by default.

4. Access to information

Members of the College will be granted access to the information they need in order to fulfil their roles within the College. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

5. Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely. Confidential paper waste must be disposed of securely and in accordance with College information security procedures to comply with UK/EU legislation (contact the Facilities team of the Infrastructure Services Directorate for more details).

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the College, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the College until it is disposed of securely.

6. Removal of information

College data which is subject to the Data Protection Act or which has a classification of confidential or above should be stored using College facilities or with third parties subject to a formal, written legal contract with the College. In cases where it is necessary to otherwise remove data from the College, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Strictly confidential data in electronic form must be strongly encrypted prior to removal. Secret data must never be removed except with the explicit written permission of the data owner.

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
- 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.

7. Personal data and current UK Data Protection legislation

The key concepts and principles current UK Data Protection legislation requires that where personal data is concerned, RVC data controllers and data handlers must consider and process personal data with an understanding of:

7.1. Data protection principles

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

7.2. Accountability and governance

- The RVC must be able to demonstrate compliance with the current UK Data Protection legislation:
- We will establish a clear governance structure with roles and responsibilities.
- We will keep a detailed record of all data processing operations - this will be achieved via the annual survey
- The documentation of data protection policies and procedures.
- Data protection impact assessments (DPIAs) for high-risk processing operations.
- Implementing appropriate measures to secure personal data.
- Staff training and awareness.
- Where necessary, appoint a data protection officer.

7.3. Data protection by design and by default

- There is a requirement for us to build effective data protection practices and safeguards from the very beginning of all processing:
- Data protection must be considered at the design stage of any new process, system or technology.
- A Data Privacy Impact Assessment is an integral part of privacy by design.
- The default collection mode must be to gather only the personal data that is necessary for a specific purpose.

7.4. Lawful processing

We must identify and document the lawful basis for any processing of personal data. The lawful bases are:

- Direct consent from the individual;
- The necessity to perform a contract;
- Protecting the vital interests of the individual;
- The legal obligations of the organisation;
- Necessity for the public interest; and
- The legitimate interests of the organisation.

7.5. Valid consent

There are now stricter rules for obtaining consent:

- Consent must be freely given, specific, informed and unambiguous.
- A request for consent must be intelligible and in clear, plain language.
- Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
- Consent can be withdrawn at any time.
- Consent for online services from a child under 13 is only valid with parental authorisation.
- Organisations must be able to evidence consent.

7.6. Privacy rights of individuals

Individuals' rights are enhanced and extended in a number of important areas:

- The right of access to personal data through subject access requests.
- The right to correct inaccurate personal data.
- The right in certain cases to have personal data erased.
- The right to object.
- The right to move personal data from one service provider to another (data portability).

7.7. Transparency and privacy notices

Organisations must be clear and transparent about how personal data is going to be processed, by whom and why.

- Privacy notices must be provided in a concise, transparent and easily accessible form, using clear and plain language.

7.8. Data transfers outside the EU (please seek advice from data@rvc.ac.uk)

The transfer of personal data outside the EU is only allowed:

- Where the EU has designated a country as providing an adequate level of data protection;
- Through model contracts or binding corporate rules; or
- By complying with an approved certification mechanism, e.g. EU-US Privacy Shield.

7.9. Data security and breach reporting

Personal data needs to be secured against unauthorised processing and against accidental loss, destruction or damage.

- Data breaches must be reported to the Information Commissioners Office within 72 hours of discovery, so you must report them to data@rvc.ac.uk as soon as they are discovered.
- Individuals impacted should be told where there exists a high risk to their rights and freedoms, e.g. identity theft, personal safety. This will be done with the assistance and advice of the Secretariat after you have informed them of the breach.

8. Using personally owned devices

Data subject to current UK Data Protection legislation must never be stored on personally owned devices. Data classified as sensitive must neither be stored on nor processed using personally owned devices.

Personally owned devices must not be used for the storage or processing of any other information classified as strictly confidential or above without the explicit written permission of the data owner. Appropriate security measures must be taken when using personally owned devices to process or store any College data.

9. Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. Staff offices should be locked when empty.

10. Backups

Information owners must ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis. Information which is entrusted to the care of IT Infrastructure Services will meet these requirements.

11. Exchanges of information

Whenever personal data or other confidential information is transmitted to or exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as strictly confidential may only be exchanged electronically both within the College and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the College must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

12. Reporting losses

All members of the College have a duty to report the loss, suspected loss or unauthorised disclosure of any College information or data asset to the College's Data Protection Officer.

Particular care needs to be taken when information assets are in transit on laptops, tablets or media such as memory sticks and external hard drives. College supplied mobile devices must always be fully encrypted by IT Helpdesk staff as described in the current ITPOL003 IT Encryption Policy. Details of the loss or theft of RVC hardware must be reported immediately to the IT Helpdesk (helpdesk@rvc.ac.uk), as well as advising the College's Data Protection Officer (data@rvc.ac.uk) of any personal information held on that device (to enable compliance with any requirement to declare data breaches to the ICO within 72 hours of them occurring).

13. Further information

RVC Data Protection Policy (May 2018)

RVC Data Protection Policy (May 2018).pdf