RVC DATA PROTECTION POLICY

POLICY and PROCEDURES

Responsibility of	**Data Protection Officer**
Review Date	**July 2019**
Approved by	**CEC**
Author	**D.Hardyman-Rice**

CONTENTS **PAGE**

1) Policy Statement

The Royal Veterinary College holds and processes information about employees, students, clients, suppliers and other *Data Subjects* for various academic, administrative and commercial purposes. The College is committed to protecting the rights and freedoms of all our *Data Subjects* and to processing their data securely in accordance with our legal obligations.

The RVC will process data in accordance with the six Data Protection Principles, having established and documented a lawful basis for data processing together with an additional condition when processing any *Special Category Data*.

The RVC will not process data in ways that have an unjustifiably adverse effect on the *Data Subjects* and only handle data fairly and in ways that *Data Subjects* would reasonably expect.

The RVC will implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is undertaken in accordance with its legal obligations.

The RVC recognizes that data subjects have specific rights relating to the collection and use of their personal data and will ensure that it complies with these individual rights.

The RVC will ensure that it remains in compliance with current UK Data Protection law.

In the event that there is conflict between this Policy and the requirements of legal compliance, then the legal requirements of the current UK Data Protection law will prevail.

Any questions relating to this Data Protection Policy or to its use / implementation should, in the first place be addressed to the *Data Protection Officer*, C/o RVC Secretariat, Hawkshead Campus.

2) Key definitions

General Data Protection Regulation (GDPR)	European Regulation that governs the processing of Personal Data. GDPR is effective from 25May18 and is enshrined in UK legislation.
Data Controller	For the purpose of this Policy, RVC is the Data Controller. A natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data as determined by law.
Data Processing	Any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as (but not limited to) collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the Data Controller.
Data Protection Officer (DPO)	The DPO acts as a contact point for Data Subjects and the Supervisory Authority (viz.: the ICO).
Data Protection Impact Assessments (DPIA)	This is an impact assessment undertaken in conjunction with the DPO in cases where the type of Personal Data processing carries a high risk of infringing the rights, freedom and interests of an individual(s).
Data Subject	Please see under Personal Data
Departmental Data Officer	The person nominated to support and advise a Dept. / Area or Section head on data compliance and good practice and to assist the work of the DPO.
Filing System	Any structured set of Personal Data, which is accessible according to specific criteria whether centralized, decentralised or dispersed on a functional or geographical basis, whether held in hard copy or electronically.
Personal Data	This is any information relating to an identified or identifiable natural person (the Data Subject).
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and/or deliberate causes.
Privacy Notice	Information provided to a Data Subject to advise that their data is being collected / processed. This is provided in a concise, transparent, easily accessible form, using clear and plain language. Data Subjects must be advised that their data is being collected and / or processed.
Special Category Data	The type of data that could create more significant risks to a Data Subject's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. Such data includes religious beliefs; ethnicity; political opinions – more details can be found in §20.
Supervisory Authority / Regulator	For RVC this is the Information Commissioner's Office (ICO), which is the Government-authorized body that ensures that processing of personal data complies with current UK Data Protection law.

For ease of reference, terms shown in this Policy in *Italic Script* refer to definitions shown above

3) Six Data Protection Principles

When *Personal Data* is processed, it must be processed in accordance with the six Data Protection Principles as defined under law, requiring that *Personal Data* shall be:

1st. processed fairly, for a legal purpose and undertaken in a way that is open and transparent regarding the reason for its collection and regarding how the data will be used.

2nd. collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those stated purposes;
[For information regarding the further processing of *Personal Data*, please see §17 below]

3rd. adequate (not excessive), relevant and limited to what is necessary in relation to the purposes for which the data are processed;

4th. accurate and, where necessary, kept up to date;

5th. kept in a form that permits identification of *Data Subjects* for no longer than is necessary for the stated purposes for processing the data;
[For further information regarding the retention / storage of data, please see §18 below]

6th. processed in a manner that ensures appropriate security of the *Personal Data*, including protection against unauthorized or unlawful processing.

4) Data Controller

Under the current UK Data Protection law, the Royal Veterinary College is identified as a *Data Controller* and, as such, is responsible for ensuring that the College is in compliance with the six Data Protection Principles for processing personal data (See §3 above). The RVC is also considered a 'Public Authority' under UK Data Protection Law and must therefore also act in accordance with the particular requirements relating to this status.

5) Supervisory Authority

The processing of any *Personal Data* at the Royal Veterinary College (the *Data Controller*), is supervised / regulated by the **Information Commissioner's Office** (ICO).

The ICO is an independent public body that through its sponsoring department within the UK Government, is the appointed *Supervisory Authority / Regulator* that ensures that in processing *personal data*, organizations in the UK including the RVC, comply with the requirements of the current UK Data Protection law.

In order to continue to process data lawfully, the RVC will maintain appropriate registration with the *Supervisory Authority*.

6) Accountability & Transparency

As a *Data Controller*, the RVC is governed by the provision for accountability under current UK Data Protection law. It will provide evidence through its documented records of compliance if so requested by the *Supervisory Authority*. Such evidence will reflect the lawful basis (bases) for processing data, show that due consideration has been given to the lawful basis applicable to each *data processing* purpose and that decisions on *data processing* are justified.

Under delegated authority from the College Executive Committee, the responsibility for monitoring compliance with the GDPR / current UK Data Protection law, our data protection policy, awareness-raising, training, and audits will rest with the *Data Protection Officer* (DPO).

The College Executive Committee will ensure that:

- it involves the *DPO*, in a timely manner, in all issues relating to the protection of *Personal Data*
- the *DPO* is sufficiently well resourced to be able to perform their tasks
- it does not penalize the *DPO* for performing their duties
- it ensures that any other tasks or duties assigned to the *DPO* do not result in a conflict of interests with their role as a *DPO*.

7) Data Protection Officer (DPO)

As a Public Authority, the College has a duty to appoint and support a *Data Protection Officer* (*DPO*). This person reports directly to the College Executive Committee. The requirements of the role and how it be supported are as specified by UK data Protection Law. In accordance with legislation the *DPO's* responsibility will include but not be limited to:

- maintaining appropriate registration with the *Supervisory Authority* (ICO)
- ensuring that the College fulfils its responsibilities as a *Data Controller*
- act as a contact point for *Data Subjects* and the *Supervisory Authority*
- inform and advise on the College's data protection obligations as specified by the current UK Data Protection law
- putting into place comprehensive but proportionate governance measures (policies / procedures)
- maintain robust breach detection, investigation and internal reporting procedures
- keeping a record of Departmental Data Officers in each relevant and accountable area
- monitoring internal compliance and directing *Departmental Data Officers* as required
- establishing the lawful basis (bases) for the processing of data
- ensuring that with regard to the processing of children's data that appropriate systems and processes are in place in order to address the particular protections appropriate for children
- provide advice regarding *Data Protection Impact Assessments* (*DPIA*)

The *DPO* post-holder will be as is, from time to time, recommended by the RVC Executive and approved by RVC Council.

8) Implementation of the RVC Data Protection Policy

The *College Executive Committee* has overall responsibility for the implementation of this Policy with the advice and operational support of the DPO. *Departmental Data Officers* will be identified in each relevant and accountable area and will be responsible for advising on and supporting Heads of Department in the implementation of this Policy and associated *data processing* at departmental / sectional / faculty level. *Departmental Data Officers* and Heads of Department will be supported in their roles by the *DPO*.

9) Data Processing

Any person (staff, student or contractor) at whatever level in the RVC, who is undertaking the processing of *Personal Data* on behalf of the College, must act in accordance with this Policy.

Departmental Data Officers will be responsible for helping Heads of Department to ensure that the processing of *Personal Data* in their respective areas is undertaken in accordance with this Policy.

Any person involved in processing personal data may seek advice and support from their areas *Departmental Data Officer* and / or the *DPO*.

Any person involved in the processing of *Personal Data* must note that any infringements or any breaches of the provisions of the current UK Data Protection law may result in substantial fines levied against the RVC. [Please refer to §10 DPIA and §24 Personal Data Breaches], may well cause reputational damage and result in negative impacts on our Charitable objects.

Deliberate and significant breaches of this policy may result in disciplinary action being taken and/ or criminal charges brought by the Police, depending on the nature and severity of the breach.

In order to comply with the 1st principle of data processing [See §3 above], anyone processing *Personal Data* has a duty to provide specific information to *Data Subjects* when asking for their personal information or when acquiring their personal information for processing and a duty to facilitate the exercise of the rights of *Data Subject* (See §22 below).

10) Data Protection Impact Assessment (DPIA)

DPIA is a process that guides the identification and minimization of data protection risks.

For any processing that is likely to result in a high risk to / higher severity of any impact on the rights, interest or freedom of a *Data Subject,* the staff member responsible must undertake a DIPA and submit it to the DPO for approval before processing is performed.

The *DIPA* must:

- describe the nature, scope, context and purposes of processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to the *Data Subject(s)*
- identify any additional measure to mitigate those risks.

Responsible staff should follow any advice and guidance issued by the *DPO* and also may seek local support from their *Departmental Data Officer*.

11) Record Keeping of Personal Data at the RVC

At the first point of communication (whether verbal, written or electronic) and in a concise, transparent, easily accessible form, using clear and plain language, *Data Subjects* must be provided with privacy information, advising them that their data is being collected and / or processed. This can be achieved in a number of ways, the most common being a *Privacy Notice* (See §13)

Appropriate records must be kept of all *data processing* activity. This can be either in written or electronic form but must be available upon either internal request or at the request of the *Supervisory Authority*, in order to demonstrate compliance with the current UK Data Protection law. Records must be:

- accurate and, where necessary, kept up to date
- kept in a form that permits identification of *Data Subjects* for no longer than is necessary for the stated purposes for processing the data
- protected against unauthorized or unlawful processing.

12) Security

All *Personal Data* must be processed in a manner that ensures its security. This must include protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. Appropriate technical and organizational security measures must be employed.

13) Privacy Notices

The term *Privacy Notice* describes all the privacy information that the *Data Controller* makes available or provides to a *Data Subject* when it collects / processes data about them. A *Privacy Notice* must include:

- details of the legal basis for processing
- the purpose for the processing
- special condition(s) associated with any Special Category Data
- the contact details of the *Data Protection Officer*
- the rights of the *Data Subject* including the Right to Object [See Appendix 1(7)]
- details of any automated decisions / profiling
- details of retention of the data

14) Use of Third Party Data Controllers / Processors

Data Subjects must be advised, at the earliest opportunity, if their data is going to be collected by / shared with or processed by any third party *Data Processors* or *Data Controllers*.

Staff responsible for processing personal data must ensure that appropriate controls, assurances and safeguards are in place in order to protect the interests of our Data Subjects or of the Data Subjects of other Data Controllers when undertaking work as a Data Processor on their behalf.

15) Lawful Basis for Processing Data

Under the 1st Principle for Data Protection, there are 6 (six) types of lawful processing as specified in the current UK Data Protection law. In accordance with this 1st Principle, *anyone processing personal data at the College* has a duty to establish, justify and document the lawful basis (bases) for processing all forms of data. In doing so they may need to consider a variety of lawful bases for processing data, depending on how the data is intended to be used. Before any processing of personal data takes place, advice should be sought from the ICO's resources, from the relevant *Departmental Data Officer and* if required through consultation with the *DPO*, before documenting which one of the six lawful bases is appropriate. The six lawful bases are:

1) Consent
   Processing can be justified if the *Data Subject* has given their recent, clear, explicit and defined consent for their data to be processed for one or more specified purpose.
   Consent needs to take the form of a clear affirmative action by the *Data Subject* such as by ticking a box to be included on a mailing list. NB leaving a pre-completed box ticked is not an affirmative action.

2) Contract

Processing can be justified if it is necessary because of a contract that the *Data Subject* has entered into with the RVC or because the RVC has been asked to do something (e.g. to provide a cost estimate) before the *Data Subject* enters into a contractual arrangement.

For example, if someone is paying the RVC to provide a service, then the RVC will be fully justified in processing the *personal data* for that purpose.

3) Legal Obligation

Processing can be justified in order to comply with a common law or statutory obligation. It should be noted however, that this does not apply to contractual obligations.

4) Vital Interests

Processing can be justified based on vital interests if it is necessary to process *personal data* in order to protect the *data subject's* life. Such processing must be necessary – if a person's vital interests can be protected in another less intrusive way, this lawful basis will not apply.

5) Public Task (Function)

Processing can be justified based on Public Task, when *personal data* needs to be processed in the exercise of public functions and powers that have a clear basis in law or in order to perform a specific task in the public interest that is set out in law. The RVC is likely to rely on the Public Task basis for many of its activities as a Public Authority.

6) Legitimate Interests

Public Authorities can only rely on legitimate interests if they are processing *personal data* for a legitimate reason **other than** performing their tasks as a Public Authority. If the requirement for *data processing* is distinct from its responsibilities as a Public Authority (e.g. client information processed during veterinary clinical activities or for alumni relations, fundraising etc.), then the RVC may consider whether Consent or Legitimate Interests is the appropriate basis for the particular circumstances.

Processing can be justified based on Legitimate Interests, when the processing of *personal data* is undertaken in ways that a *data subject* would reasonably expect and which has a minimal impact on privacy or where there is a compelling justification for the processing.

If choosing this as the lawful basis for processing data, it is to be inherently understood that there is extra responsibility on anyone processing the data to consider and protect the freedom, rights and interests of D*ata Subjects* and the legitimate interests of the *Data Subject* may override the legitimate interests of the RVC.

In order to demonstrate compliance with the current UK Data Protection law, any Legitimate Interest assessments must be fully documented including the final decision.

16) Change of Lawful Basis for Processing Data

If it is subsequently established that the chosen lawful basis is not appropriate, the lawful basis cannot be automatically switched. There should be a genuine change in circumstances or there is a new and unanticipated purpose, which means there is a good reason to review the lawful basis and make a change. Any such changes must be discussed and agreed with the *DPO* and the *Data Subject* must be informed accordingly, with any change being fully documented.

17) Further Processing of Personal Data

Where further processing of *Personal Data* is considered for a purpose other than that for which the data was originally collected, the *Data Subject* must be provided with information on that other purpose and with any other relevant information before such further processing takes place. Any changes to the purpose for the processing must be documented by the person processing the data.

18) Retention of Personal Data

No specific minimum or maximum retention period is specified by law but retention of *Personal Data* must comply with the 5th Data Protection Principle (§3 above). In practice this means that anyone who is responsible for processing *Personal Data* will need to:

- review the length of time that they keep *Personal Data*
- consider the purpose or purposes for which they hold the information in deciding whether (and for how long) to retain it
- securely delete information that is no longer needed for this purpose or these purposes
- update, archive or securely delete information if it goes out of date.

The law does not define 'delete' or 'deletion' but recognizes that the implied meaning of 'destruction' differs for paper records and electronic records. The deletion of *Personal Data* is an important issue and anyone responsible for the deletion of *Personal Data* should refer to the ICO guidance available through the following link:
https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf
Any uncertainty relating to the storage or deletion of *Personal Data* must be raised with the *DPO*.

19) Processing Children's Personal Data

Children need particular protection when their data is being collected and processed, since they may be less aware of the risks involved. For this reason and prior to the processing of any children's *Personal Data*, the person responsible for processing the data must carry out a *DPIA*.(§10 above)

20) Processing Special Category Data

In addition to establishing the appropriate lawful basis (or bases) for each data processing activity, if the data being processed includes *Special Category Data*, then a specific condition for processing such data must also be identified. Even when a *Data Subject* has given consent to the processing of their personal data in general, explicit consent must be obtained from them before any of their *Special Category Data* is processed.

This category of data could create more significant risks to a *Data Subject's* fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

Such data includes (but is not limited to):

- race
- ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetics
- biometric data used to identify an individual
- health
- sex life
- sexual orientation

The choice of lawful basis for data processing does not dictate which special category condition is applicable.

The choice of the specific condition for processing *Special Category Data* must be made in consultation with the *DPO* and, in order demonstrate compliance, all decisions must be fully documented.

The requirements for processing *Special Category Data* are shown in Appendix 2.

21) Criminal Offence Data

Personal Data relating to criminal convictions and offences or related security matters must only be processed by anyone responsible for processing data when they are acting in an official capacity or under specific legal authorization. Advice should be sought from *Departmental Data Officers* and/ or the *DPO* before processing any such data within their area and all decisions must be fully documented.

22) Rights of Data Subjects (Individuals)

The RVC recognizes that *Data Subjects* are afforded certain rights under the current UK Data Protection law. It should be noted that not all these rights are absolute.

Data Subjects must be informed of their right to object at the first point of communication, as well as in any relevant *Privacy Notice*. They retain the right to lodge a complaint with the *Supervisory Authority* at any point.

The *Departmental Data Officer* must ensure that, for all data processing in their area, there is compliance with the statutory duty to facilitate the exercise of these *Data Subject* rights. These rights are described in Appendix 1.

23) Subject Access Request (SAR)

In order to exercise their rights, *Data Subjects* can make a Subject Data Access Request (SAR) to the RVC. These requests can be made verbally or in writing.

Upon receipt of an SAR, the *Departmental Data Officer* within the relevant area of the College must be advised immediately, who will notify the *DPO* accordingly. In consultation with the *DPO*, an appropriate response must be made to the request within **1 month**.

24) Personal Data Breaches

A *Personal Data Breach* is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, *Personal Data*. This includes breaches that are the result of either accidental and/or deliberate causes.

Any breach of *Personal Data* must be taken very seriously and must be immediately reported to the *DPO*, to the area's *Departmental Data Officer* and the Head of Dept./Section Area.

The *DPO* will be ultimately responsible for managing the breach investigation and resolution and should receive full and timely co-operation from staff, students and contractors in support of these activities.

Certain types of *Personal Data Breaches* must, where feasible, be reported to the *Supervisory Authority* **within 72 hours** of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individual's rights and freedoms, the *Data Subject(s)* concerned must also be advised without due delay.

The *DPO* will facilitate the decision-making process about whether or not notification needs to be given to the *Supervisory Authority* and/or the affected *Data Subject(s)*.

APPENDIX 1 - Rights of Individuals

1) Right to be informed
   Data Subjects have the right to be informed about the collection and use of their *Personal Data*.

2) Right of Access
   In order to be aware of and to verify the lawfulness of the *data processing*, *Data Subjects* have the right to
   - obtain confirmation that their data is being processed
   - access their personal data
   - supplementary information about the *data processing* (usually provided in *Privacy Notices*)
   - any information about where their data came from if not collected from them directly.

3) Right of Rectification
   Data Subjects have the right to have inaccurate *Personal Data* rectified / completed if incomplete.

4) Right of Erasure (Right to be Forgotten)
   This right for the erasure of *Personal Data* only applies in certain circumstances, which include:
   - the data is no longer necessary for the purpose under which it was originally collected or processed
   - if relying on Consent as the lawful basis for processing the data and the *Data Subject* withdraws consent
   - if relying on Legitimate Interests as the lawful basis for processing the data and an overriding legitimate interest no longer exists
   - the data is being processed for direct marketing purposes and the *Data Subject* objects to this processing
   - data has been processed unlawfully (in breach of the 1st Data Protection Principle)
   - data must be erased in order to comply with a legal obligation
   - data collected from children particularly when the processing is based upon the Consent of a child.

5) Right to Restrict Processing
   Data Subjects can limit the way that an organization uses their data arising, for example, from concerns about the content of the information held or about the way that their data has been processed. Restriction usually applies for a certain period of time.

6) Right to Data Portability
   Data Subjects have the right to obtain and reuse their *personal data* for their own purposes enabling them to move, copy or transfer *personal data* across different services in a safe and secure manner without hindrance to its usability.

7) Right to Object
   Data Subjects have the right to object if processing is based on Legitimate Interests or Public Task or if data is being used for direct marketing (including profiling) or being processed for scientific/historical research and statistics.

8) Rights in relation to Automated Decision Making and Profiling
   Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects the *Data Subject*.

APPENDIX 2 - Requirements for Special Category Data

- The *Data Subject* has given explicit consent to the processing of the data
- It is necessary for carrying out obligations and exercising specific rights in the field of employment, social security and social protection law
- It is necessary to protect a *Data Subject's* vital interests when the *Data Subject* is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the *Data Subjects*
- The *Data Subject* has made the data public
- It is necessary for legal claims or proceedings
- It is for reasons of substantial public interest
- It is necessary for the purposes of preventative or occupational medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision or management of health or social care or treatment. In such cases it must be carried out on the basis of legislation or under contract with a health professional and is subject to safeguards as specified by the current UK Data Protection law
- It is necessary for reason of public health
- It is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.