Data Protection Policy (DP-Pol-090)

Document Title	Data Protection Policy
Document Number	DP-Pol-090
Version	2.0
Department	Quality Assurance and Corporate Risk
Owner/Responsible for Implementation	Manager, Quality Assurance and Corporate Risk
Approving Body	Executive Board
Effective date:	June 2019
Next Review date:	June 2022
Related Documents	DP-Pol-089 – Records Management Policy ISMS-Pol-101 – Information Security Policy ED-Pol-88 – Programme Information & Data Management Policy DP-Pol-133 – Data Breach Management Policy and Procedure DP-SOP-81 – Subject Access Procedure DP-T-82 – Subject Access Request Assessment Form

1. Purpose

RCPI is committed to compliance with the General Data Protection Regulation. This means ensuring that the appropriate and commercially reasonable technical and organisational measures are implemented.

The purpose of this document is to provide a point of reference and guidance on decisions about activities that could in any way impact on an individuals' right to privacy.

2. Scope

This policy applies to all staff (including but not limited to full-time, part-time and temporary staff) employed by RCPI who process personal data during the course of their employment for academic, research, administrative and/or other purposes.

It is the responsibility of staff to oversee the activities and work of external providers, for example specialised contractors or business consultants, with whom they are engaged to ensure that they are fully aware of the RCPI Data Protection Policy.

This policy also applies to all clinician and lay members of RCPI boards and committees who may, in the course of their engagement with RCPI, attain access personal data which is under the controllership of RCPI. Equally, it applies to all Trainees, Members and Fellows.

This policy applies to personal data processed by RCPI in paper and electronic format and is not restricted by location or form of access.

3. Permitted Legal Basis for the Use Personal Data.

RCPI uses or processes, in various different ways, the personal data of individuals in order to carry out its functions and fulfil its obligations.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' (GDPR Art.4)

RCPI, as a data controller, ensures that there is an appropriate legal basis for the processing of all personal data. The lawful purposes as set out in the GDPR are as follows:

- the individual has **consented** to processing. Consent is valid only where the consent is:
  - specific, informed and freely given
  - given as clear affirmative action (pre-ticked/ opt-out consent is not valid)
  - documented and retained
  - easy to withdraw by the data subject
- processing is required to fulfil a **contract**
- processing is necessary for the **legitimate interests** of RCPI and does not interfere with the rights and freedoms of individuals. If legitimate interest is to be used as a as a legal basis for processing personal data, you must contact the DPO to perform a 'Legitimate Interests Assessment'.
- processing is necessary for compliance with a **legal obligation**
- processing is necessary to protect an individual's vital interests. It is unlikely that RCPI would have occasion to rely on this legal basis.
- processing is necessary for the performance of a task carried out in the public interest. It is unlikely that RCPI would have occasion to rely on this legal basis.

4. Commitment to Principles of the General Data Protection Regulation

RCPI undertakes to carry out its business with due regard for the following principles which are set out in the General Data Protection Regulation.

2.1 Transparency

Transparency demands that data processing be undertaken in a transparent manner and that data subjects are provided with information in relation to processing of their personal data. This includes the identity of the controller (i.e. RCPI), the contact details of the DPO for RCPI, the duration of the personal data storage as well as reference to the existence of the data subject's various rights. It also includes the legal basis for the collection of the personal data, as described in Section 3 of this document.

2.2 Purpose Limitation

Purpose Limitation is the principle that personal data is only processed for the particular purpose for which it was collected.

2.3 Data Minimisation

Data Minimisation demands that collection of personal data are limited to what is adequate, necessary and relevant to the purposes for which it was collected.

2.4 **Accuracy**

The principle of Accuracy requires that personal data must be accurate and kept up to date and every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified.

2.5 **Storage Limitation**

Under the principle of Storage Limitation personal data is not to be kept in an identifiable form for any longer than the purposes for which it was collected (subject to certain limited exceptions).

2.6 **Integrity and Confidentiality**

The principle of Integrity and Confidentiality requires that technical and organisational security measures be put in place to ensure that personal data is protected from various forms of data breaches.

2.7 **Accountability**

The seventh key principle is Accountability, which requires that data controllers are able to demonstrate compliance with each of their obligations under the GDPR.

5. Commitment to the Rights of Individuals under the GDPR

RCPI undertakes to carry out its business with due regard for the rights of individuals as set out in the General Data Protection Regulation.

3.1 **Right of Access**

The right of data subjects to obtain details concerning the processing of their personal data and to have access to a copy of any personal data that is processed.

3.2 **Data Portability**

This is a new data subject right under the GDPR whereby data subjects may request controllers to provide them with the personal data that they have provided to the controller, including the right to have their personal data transferred to another controller (where technically feasible to do so). However, this right is subject to certain exceptions.

3.3 **Right of Erasure / Right to be Forgotten**

Data subjects have the right to have their personal data erased without undue delay where certain conditions are met. However, this is not an absolute right and, for example, is not available where controllers are required by law to retain certain personal data or where it undermines the right to freedom of expression.

3.4 **Right of Rectification**

In line with the Accuracy principle, data subjects have the right to have any inaccurate personal data rectified without undue delay.

3.5 **Right to Object**

Data subjects have a right to object to the processing, including profiling, of their personal data where such processing is based on legitimate interests of the controller (or a third party). Such objections may arise where personal data is processed or profiled for advertising purposes based on the legitimate interests of the controller (or a third party). In such a case, the controller must cease processing the data unless it can show that it has a compelling legitimate interest to continue such processing. The right to object is in essence a form of opt-out in relation to data processing for advertising/marketing purposes. The right to object also arises where personal data is processed based on public interest grounds.

6. Technical measures in place to protect the individuals' right to privacy

Refer to RCPI's Information Security Policy (ISMS-Pol-101)

7. Organisational measures in place to protect the individuals' right to privacy

RCPI has established the following structures to ensure compliance with the General Data Protection Regulations.

- Data Inventory
- Policies and procedures
- Data Protection Impact Assessments
- Vendor Management
- Data Protection Audit Schedule
- Training and Communications
- Periodic reporting to the Executive Board of the organisation

8. Definitions

Personal data: Any information relating to an identified or identifiable person who can be identified, directly or indirectly, by reference to an identifier such as name, image, identification number, location data or online identifier.

Data processing: Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special category data: Data revealing an individual's racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, data relating to trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health and data concerning an individual's sex life or sexual orientation.

Data controller: An entity which determines the purposes and means of the processing of personal data e.g. RCPI is a data controller in relation to personal data relating to its staff, learners, trainers, members and fellows.

Data processor: An entity which processes personal data on behalf of the controller.

9. References

General Data Protection Regulation

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Useful Website for Navigating the General Data Protection Regulation

http://www.privacy-regulation.eu/en/

Data Protection Act 2018

https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf

Data Protection Commissioners Website

https://dataprotection.ie/docs/Home/4.htm

Data Protection Resources

http://gdprandyou.ie/resources/