



RCN GROUP DATA PROTECTION POLICY

Version 3.0

Document control summary

Title	Data Protection Policy
Status	Approved
Version No.	3.0
Date of Approval	
Author(s)	Huw Bevan – IT Operations Manager Idris Evans – Information Security and Compliance Manager
Approved by	ET & Partnership Forum RCNi Executive team & RCNi Partnership forum
Circulated to	All staff
Next Review Date	September 2019

VERSION CONTROL SUMMARY

Version	Date	Summary
1.0	September 2012	Approved by ET and Partnership Forum. The Policy sets out to inform staff of their responsibilities under the Data Protection Act.
2.0	September 2015	Minor changes - staff names and job titles
3.0	April 2018	Change to take into account GDPR and new Data Protection Bill Make this policy a group policy as opposed to RCN specific Approved by ET, Partnership forum and RCNi exec team

CONTENTS

Section		Page
1	Introduction	4
2	Aims and Objectives	4
3	Definitions	4
4	Policy statement	5
5	Roles and responsibilities	8
6	Monitoring and Reporting	11
7	Breach of this policy	11
8	Impact Assessment Statement	11
9	Policy Review	11

1. Introduction

- 1.1 The lawful and correct treatment of personal and sensitive data is an integral part of the RCN Group's functions. Compliance with data protection legislation is vital for maintaining confidence between ourselves, and our members, clients and staff.
- 1.2 This is an RCN Group policy and applies to all staff, contractors and any other individual or company representing the RCN, RCNi and RCN Foundation.
- 1.3 This policy will be reviewed every three years or as required by legislative or good practice recommendations.

2. Aims and Objectives

- 2.1 This policy outlines how the RCN Group will meet its legal obligations concerning confidentiality and information security standards. It is based on relevant legislation, professional standards and guidance including:
 - General Data Protection Regulation 2018
 - Data Protection Act 2018
 - Computer Misuse Act 1990
 - Common law Duty of Confidentiality.

3. Definitions

- 3.1 Personal information/data relates to a living individual who can be identified from the information and includes:
 - factual information – e.g. name, address, or online identifier
 - expressions of opinion about the individual
 - indication of the intentions of the Data Processor (the RCN)
 - any other person in relation to the individual concerned.
- 3.2 Sensitive personal data (special categories of personal data) can only be processed in limited circumstances and is further defined to include a data subject's:
 - racial or ethnic origin
 - political opinions
 - religious beliefs or other beliefs of a similar nature
 - membership of a trade union

- physical or mental health or condition
- sexual life
- genetic or biometric data
- criminal record, including the commission or alleged commission of any offence and any proceedings/sentence for an offence.

3.3 A record can be in computerised and/or manual form and includes:

- hand written notes
- letters to and from the RCN Group
- electronic records
- print outs
- photographs
- video and audio recordings.

As such this policy extends, but is not limited, to:

- corporate and administrative records
- employee records
- financial records
- call recordings
- membership records including Case Management
- any personal information held in accordance with the organisation's Data Protection registration with the Information Commissioner's Office
- all records relating to an individual.

4. **Policy Statement**

This policy provides guidance in relation to the protection, sharing and disclosure of personal data including member, customer and staff information. It applies to all staff and departments within the RCN Group.

The RCN Group fully endorses and abides by the six principles of the GDPR which require personal data to be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

4. Accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
 5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
 6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- 4.1** As the Data Controller we (the RCN group) are responsible for, and must be able to, demonstrate compliance with the above. To do this the RCN Group will, through appropriate management, and strict application of criteria and controls:
- (a) Observe fully the above conditions regarding the collection and use of information.
 - (b) Meet our legal obligations to specify the purposes for which information is used.
 - (c) Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs.
 - (d) Ensure the quality of information used.
 - (e) Apply strict checks to determine the length of time information is held.
 - (f) Ensure that the rights of people about whom information is held can be fully exercised under the GDPR.
 - (g) Ensure that staff are appropriately trained, understand their responsibilities for complying with legislation and good practice and know where to obtain further advice and information about handling personal data.
 - (h) Appoint a designated Data Protection Officer for the organisation and, as required, ensure their details are registered with the Information Commissioner's Office.
 - (i) Ensure that queries about the handling of personal information are promptly and courteously dealt with.
 - (j) Regularly review, audit and evaluate the way personal information is handled and managed.

4.2 Rights of the Data Subject

The GDPR provides the following rights for individuals:

1) The right to be informed

This encompasses the RCN Group’s obligation to provide “fair processing information” (typically through a privacy notice) and emphasises the need for transparency over how we use personal data

2) The right of access

Under GDPR, any living person, who is the subject of personal information held and processed by the RCN Group, has a right to apply for access to that information. This is known as a subject access request.

Information must be provided without delay and, at the latest, within one month of receipt of the request. This period can be extended by a further two months where requests are complex or numerous. Where this is the case, the subject must be informed of the delay within one month and provided with an explanation of why the extension is needed.

3) The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Any third parties to whom the data has been disclosed, must also be informed of the rectification where possible. The individuals must also be informed that their information has been shared.

These requests must be responded to within one month. This can be extended by two months where the request for rectification is complex.

4) The right to erasure

The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

5) The right to restrict processing

Individuals have a right to ‘block’ or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it.

6) The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7) The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on “grounds relating to his or her particular situation”.

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defense of legal claims.

You must inform individuals of their right to object “at the point of first communication” and in your privacy notice. This must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information”.

8) Rights in relation to automated decision making and profiling.

The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

4.3 Exemptions

- If the release of personal data would reveal information, which related to and identified another person (third party) for example, where a relative has provided certain information, this information will be withheld unless consent from the individual is obtained.
- If the release of personal data is likely to cause serious harm to the data subject’s physical or mental health or of any other person.

5. Roles and Responsibility

The RCN Group has a duty to ensure that the requirements of the General Data Protection Regulation and the Data Protection Act 2018 are upheld.

5.1 Responsibility of Chief Executive & General Secretary

The RCN's Chief Executive & General Secretary has overall responsibility for Data Protection within the RCN Group.

5.2 Data Protection Officer

The RCN Group has appointed the RCN IT Operations Manager to the role of Data Protection Officer.

Responsibilities include:

- a) to inform and advise the controller or processor, and employees who carry out processing, of their obligations pursuant to the GDPR Regulation and to other Union or Member State data protection provisions
- b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
- c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to [Article 35](#) of the GDPR
- d) to cooperate with the supervisory authority
- e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in [Article 36](#) of the GDPR, and to consult, where appropriate, with regard to any other matter.

The Data Protection Officer shall have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

5.3 Data Owners

Directors and Seniors Managers are responsible for information held manually and electronically within their Directorate areas.

As Data Owners their responsibilities include:

- informing the Data Protection Officer of any changes in the processing of personal data
- identifying and justifying how sets of data are used
- identifying all personal data for which they are responsible
- agreeing who can have access to the data
- ensuring that Privacy Notices are issued and kept up to date
- ensuring that Data Processing Agreements are in place with third party data processors and kept up to date.

5.4 All staff and members with access to personal data

The RCN Group will take all necessary steps to ensure that everyone managing and processing personal data understands their legal and contractual responsibilities.

Individuals are responsible for maintaining confidentiality and adhering to data protection legislation in line with this responsibility.

Individuals include:

- all staff within the RCN Group, including but not limited to trainees, agency workers or consultants
- members with access to personal data including council members, accredited representatives and forum chairs.

Further responsibilities include:

- All staff and accredited representatives with cases are required to pass the GDPR training every 2 years.
- observing all guidance and codes of conduct in relation to obtaining, using and disclosing personal data
- observing all information sharing protocols in relation to the disclosure of information
- obtaining and processing personal information only for specified purposes
- only accessing personal information that is specifically required to carry out their work
- recording information correctly in both manual and electronic records
- ensuring any personal information held is kept secure
- ensuring that personal data is not disclosed in any form to any unauthorised third party
- ensuring sensitive personal information is sent securely
- notifying the Data Owner and contacting the Data Protection Officer (data.protection@rcn.org.uk) whenever new software is being considered, or a significant change to a current application or system is being proposed and the system holds personal data. The DPO will assess whether a Data Privacy Impact Assessment is required.
- contacting the DPO immediately on receipt of a subject access request so that RCN Group process can be followed
- notifying the DPO or the data owner (who will notify the DPO) immediately of any data breaches (tel 02920 546400 or email data.protection@rcn.org.uk) as well as your line manager. Please see the RCN Group guidance for reporting data breaches.

6 Monitoring and Reporting

- Diversity and equality outcomes are measured, monitored and evaluated as standard business practice. The Data Protection Officer will monitor activity and outcomes of the Data Protection Policy for fairness and consistency; and assess the effectiveness of its application.
- Information to assess the effectiveness of the Policy will be collected from sources such as the Learning Management System.
- As part of the HR Performance Reports, the Executive Team and Partnership Forum will be provided with (appropriately anonymised) information from the HR monitoring process on a quarterly basis.

7 Breach of this policy

Failure to adhere to this policy could result in staff being personally liable and/ or may also result in action under the relevant supporting performance / capability Policy .

8. Impact Assessment Statement

This policy has undergone an equalities impact assessment and has been determined to have no unjustifiable negative impact on a specific equality group or groups.

9. Policy Review

It is the responsibility of the Director of Organisational Capability & Change to monitor and review this policy, and ensure that any changes are presented to the RCN and RCNi Executive Teams for approval, and negotiating changes with the respective recognised trade unions.