RCN Group Data Protection Policy

Who does this policy apply to? This policy applies to all personal data the RCN Group processes regardless of where the personal data is stored (i.e. which devices) and regardless of the data subject. All staff and others processing personal data on the Group's behalf are required to read this policy
Purpose and description of the document This policy outlines the RCN Group's responsibilities under Data Protection Legislation
Document name RCN Group Data Protection Policy
Author/s Huw Bevan – Associate Director of Group Technology, Operations, Security & Data Idris Evans – Information Governance Manager
Cross Reference RCN Group IT Policy RCN Group Confidentiality Policy
Status and version Approved – final v4.2
Policy owner Huw Bevan, Associate Director of Group Technology, Operations, Security & Data
Circulated to: RCNi Board, RCN Foundation Board, RCN Group Audit Committee RCN Executive Team, RCNi Executive Team, RCN Foundation SLT
Datepolicyapprovedandby whom: RCN Council: 28 February 2023 RCNi Board: 30 November 2022 RCNF Board: 31 January 2023 Group Audit Committee: 27 October 2022
Date of implementation: 1 March 2023
Date of next review: 31 March 2026
Department responsible for Review: Transformation, Innovation and Digital

CONTENTS

1 Introduction

1.1 The RCN Group obtains, uses, stores and processes personal data relating to potential/current/former staff and RCN members, RCNi customers, beneficiaries and supporters of RCN Foundation funding, RCN Foundation Donors, contractors, website users and contacts. These parties are collectively referred to in this policy as data subjects. When processing personal data, the Group is obliged to fulfil data subjects' reasonable expectations of privacy by complying with the General Data Protection Regulation (GDPR) and other relevant data protection legislation such as the UK Data Protection Act (2018), which govern the lawful and correct treatment of the above personal and sensitive data.

Personal data is defined as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, financial, cultural or social identity of that natural person'

The handling of such data is an integral part of the RCN Group's functions, a vital element of which is compliance with the above legislation. This ensures the Group acts properly and lawfully and maintains the confidence of all data subjects. The Group takes its responsibilities very seriously with regard to the requirements of the GDPR and the Data Protection Act. This policy sets out how the Group manages those responsibilities.

In GDPR terminology, and in context of this policy the RCN Group is the Data Controller.

2 Scope

2.1 This policy applies to all personal data the RCN Group processes regardless of where the personal data is stored (i.e. which devices) and regardless of the data subject. All staff and others processing personal data on the Group's behalf are required to read this policy. A failure to comply with this policy may result in disciplinary action.

2.2 All senior managers and Senior Regional officers are responsible for ensuring that all staff and members within their area of responsibility comply with this policy. Appropriate practices, processes, controls and training must be followed to ensure that compliance.

Types of personal data

2.3 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 Group)

2.4 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

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

- handwritten notes
- letters to and from the RCN Group
- electronic records
- printouts
- photographs
- video and audio recordings

2.6 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

3 GDPR Principles

3.1 The handling of personal data, as described above, is governed by the six principles of the GDPR. The RCN Group requires all data handlers to abide by these principles at all times.

The principles require personal data to be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

  - 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

  - Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed

  - 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

  - 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

  - 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 The RCN Group's Data Protection Responsibilities and the Rights of Data Subjects

RCN Group Responsibilities

4.1 As the Data Controller the RCN Group is responsible for, and must be able to demonstrate, compliance with the above principles. To do this the RCN Group will, through appropriate management and strict application of criteria andcontrols:

(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 isused.
(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 isheld.
(f) Ensure that the rights of people about whom information is held can be fully exercised under the UK GDPR.
(g) Ensure that staff and members 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.

Third-party data processors

4.2 Where external organisations are used to process personal data on behalf of the RCN Group, responsibility for the security and appropriate use of that data remains with the Group.

Where a third-party data processor is to be used:

(a) a Data Protection Impact Assessment (DPIA) must be undertaken before the activity starts. Contact dataprotection@rcn.org.uk to arrange this
(b) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data
(c) reasonable steps must be taken to ensure that such security measures are inplace
(d) a written contract establishing what personal data will be processed and for what purpose must be set out
(e) a data processing agreement, available from the Information Governance team, must be signed by both parties

For further guidance about the use of third-party data processors please contact the Data Protection Officer.

Rights of Data Subjects

4.3 The UK 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 UK 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.

Dependent on the scope of the request for access, automated searches will be undertaken by the Data Protection Officer, Information Governance Manager or Information Governance Officer in line with the request.

(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 UK 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 forpurposes ofscientific/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 defence 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 UK 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-makingprocess.

4.4 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 Responsibilities

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

5.1 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 Associate Director of Group Technology, Operations, Security and Data to the role of Data Protection Officer.

Responsibilities include:

a) to inform and advise the controller or processor, and individuals who carry out processing, of their obligations pursuant to the UK 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 all users 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 UK 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 the UK GDPR, and to consult, where appropriate, with regard to any othermatter.

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.
- ensuring that, where needed, that Data Protection Impact Assessments (DPIAs) are undertaken

5.4 All staff and members with access to personal data on behalf of the RCN Group

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, committee and board members, accredited representatives, and other RCN activists
- Any members representing the RCN

Further responsibilities include:

- All individuals listed above are required to pass the UK 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 ofinformation
- 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: 029 2054 6400 or email: data.protection@rcn.org.uk) as well as your line manager. Please see the RCN Group guidance for reporting data breaches. (See also section 7 below).

Record Keeping

5.5 In line with GDPR requirements the Group must keep full and accurate records of all data processing activities. Where necessary this must include records of data subjects' consents, i.e. where consent is the legal basis of processing and does not fall under 'legitimate interest' or contractual necessity.

5.6 For record-keeping regarding data breaches, see section 7 below

Third parties

5.7 The RCN shares some member information with carefully selected third parties, who carry out trade union related data processing activities on the RCN's behalf. For more information, see the RCN Group Privacy Statement.

6 Monitoring and Reporting

6.1 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.

6.2 Information to assess the effectiveness of the policy will be collected from sources such as the Learning Management System.

6.3 As part of the People & OD Performance Reports, the Executive Team and Partnership Forum will be provided with (appropriately anonymised) information on training completion from the HR monitoring process on a quarterly basis.

7 Breach of this policy

7.1 The RCN Group has procedures in place to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

7.2 Records of personal data breaches must be kept, clearly stating:

- the facts surrounding the breach
- the effects of the breach
- the remedial action taken

7.3 If you know or suspect that a personal data breach has occurred, you should immediately contact the Data Protection Officer and follow the instructions in the personal data breach procedure. You must retain all evidence relating to personal data breaches in particular to enable the Group to maintain a record of such breaches, as required by the GDPR.

7.4 Failure to adhere to this policy could result in individuals being personally liable and/or may also result in action under the relevant disciplinary policy.

8 Impact Assessment Statement

8.1 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

9.1 It is the responsibility of the Associate Director of Group Technology to monitor and review this policy and ensure that any changes are presented to the RCN and RCNi Executive Teams and RCN Foundation for approval and negotiating changes with the respective recognised trade unions.

Title	RCN Group Data Protection Policy
Status	Draft
Version No.	4.2
Date of Approval	
Author(s)	Huw Bevan – Associate Director of Group Technology, Operations, Security & Data Idris Evans – Information Governance Manager
Approved by	ET & Partnership Forum RCNi Executive team & RCNi Partnership Forum, Group Audit Committee RCNi Board, RCNF Board and RCN Council
Circulated to	All staff and members
Review cycle and next review date	3 years 31 March 2026