# RCN GROUP CONFIDENTIALITY POLICY

| |
|---|
| **Whodoesthispolicyapplyto?**<br>This applies equally to all<br>• permanent staff<br>• temporary staff<br>• agency staff<br>• any RCN member holding a governance position (Council, committee and board members, accredited Reps and all other RCN activists) or undertaking any activity related to their duties as a member of the RCN such as Accredited Stewards and members carrying out branch-related duties<br>• volunteers<br>• secondees<br>• any other person authorised to use RCN Group systems, such as students or trainees, those on temporary placements, off-payroll workers, contractors' staff, and computer supplier employees.<br>• anyone in the above roles carrying out the activities described regardless of location including remote working<br>• |
| **Purpose and description of the document**<br>The aims of this policy are to:<br><br>• set out the RCN Group's commitment to the protection of personal and corporate information<br>• identify arrangements for the management of sensitive information<br>• provide clarity on individual responsibilities<br>• provide guidance on how the RCN Group ensures the protection of confidential data from theft and misuse |
| **Document name**<br>RCN Group Confidentiality Policy |
| **Author/s**<br>Huw Bevan – Associate Director of Group Technology, Operations, Security & Data<br>Idris Evans – Information Governance Manager |
| **Cross Reference** RCN Group IT Policy<br>RCN Group Data Protection Policy |

| |
|---|
| **Status and version**<br>Approved –final v2.2 |
| **Policy owner**<br>Huw Bevan – Associate Director of Group Technology, Operations, Security & Data |
| **Circulated to :**<br>RCNi Board, RCN Foundation Board, RCN Group Audit Committee<br>RCN Executive Team, RCNi Executive Team, RCN Foundation SLT |
| **Date policy approved and by whom:**<br><br>RCN Council – 28 February 2023<br>RCNi Board – 3 November 2022<br>RCNF Board – 31 January 2023<br>Group Audit Committee – 27 October 2022 |
| **Date of implementation:** 1 March 2023 |
| **Date of next review:** March 2026 |
| **Department responsible for Review:**<br><br>Transformation, Innovation and Digital |

# CONTENTS

## 1 Introduction

1.1 Members, staff and any other service users have a right to expect that any personal information given by them to the RCN Group will be regarded as confidential and kept in accordance with the law. Service users have the legitimate expectation that everyone handling data on behalf of the RCN Group will respect their privacy and act appropriately.

1.2 This means personal information will only be used for the purpose intended and not for any other purpose without authorisation, and will not be disclosed elsewhere unless, wherever possible, the person has given their explicit consent. The only exceptions to this would be in cases where there is a legal obligation to disclose or where there is evidence that disclosing the information is necessary.

1.3 The purpose of this policy is to establish a clear and agreed understanding of what confidentiality means within the Group, to encourage uniformity in practice and ensure that staff, members and other service users know what they can expect from the RCN Group.

1.4 Note: the term service user refers to all individuals and organisations who may share confidential information with the RCN Group.

1.5 Confidentiality does not solely relate to personal information but also to the RCN Group's corporate information.

## 2 Policy Aims

2.1 The aims of this policy are to:

- set out the RCN Group's commitment to the protection of personal and corporate information
- identify arrangements for the management of sensitive information
- provide clarity on individual responsibilities
- provide guidance on how the RCN Group ensures the protection of confidential data from theft and misuse

## 3 Scope

3.1 The confidentiality requirements covered by this policy apply to:

- RCN Group staff
- RCN Council, RCNi Board, RCN Foundation Board and committee members across the Group
- Country and regional board members
- RCN activists and accredited representatives
- RCN members when acting on behalf of RCN
- Third party organisations acting on the RCN's behalf

## 4 Responsibilities

4.1 The RCN Group will ensure it meets its legal responsibilities regarding confidentiality in relation to all current and future legislation, which guarantees a right of privacy.

*RCN Executive Team (ET)*

4.2 ET has overall responsibility for ensuring that the confidentiality policy is put into practice. In particular the ET will ensure that:

- line managers are aware of their responsibilities to their staff and other individuals
- arrangements are in place to monitor and implement this policy

ET will review the operation of this confidentiality policy every two years.

*Information Governance Manager*

4.3 The Information Governance Manager is responsible for the overall management and development of confidentiality practices and services across the RCN Group, ensuring that services are of a high standard in order to comply with appropriate legislation and standards for the Group.

*Senior managers*

4.4 Senior managers are responsible for ensuring that all directorate staff are aware of the relevant approved policies.

*Staff and members*

4.5 All staff and members, whether permanent, temporary or contracted, including students, contractors and volunteers must ensure they comply with the requirements of this policy, including any procedures and guidelines which may be issued relating to confidentiality.

4.6 All staff and members have a responsibility to act professionally in order to meet the confidentiality standards outlined in this policy. This is a legal and professional obligation, which is also set out in employment contracts.

*Group Data Protection Officer*

4.7 It is the responsibility of the Group Data Protection Officer to ensure compliance with legal requirements regarding the registering of information held by the Group on individuals, and the intended purpose of that information.

## 5 General Principles

5.1 Personal information belongs to the individual or organisation entrusting it to the RCN Group. This information remains personal and in the control of the giver. Once received by the RCN Group it may not be used for any purpose other than that for which it was given; nor may it be passed on to any individual or organisation outside the Group without the explicit permission of the giver.

5.2 Commercial and operational information of each entity belongs to those respective entities of the RCN Group. This information remains in the control of the RCN and may not be passed on to any individual or organisation outside the RCN without the explicit permission of an appropriate manager.

5.3 Service users must only access information that is appropriate to their role and responsibilities. If they discover that they have access that they should not have this should be highlighted to their line manager and to the IT Service Desk (02920546400)

5.4 Many Group staff will, by virtue of their role, have access to confidential information about other staff and/or RCN members. This information must always be handled with the utmost confidentiality. Unauthorised disclosure of personal information may be a disciplinary matter (see the relevant RCN & RCNF/RCNi Disciplinary Policy).

5.5 Staff must keep financial data such as bank details secure using appropriate security protocols. Credit card information should never be stored in Group systems. For additional guidance please contact the Information Governance Manager.

5.6 When individuals are attending meetings virtually, or taking part in telephone or video calls, they should take special consideration of their location and use a headset or find a suitably private meeting room if there is a risk of sensitive or confidential information being overheard.

## 6 Operational Practice

6.1 Each staff member and individual user of any RCN Group services has the right to see any personal information that the RCN keeps on them in paper or computer files and to request that information is changed where it is inaccurate.

6.2 Only those involved in the direct provision of services to staff, members or service users should access that individual's personal and/or confidential information.

6.3 The RCN Group maintains an appropriate level of security, in accordance with Data Protection regulations, that adequately protects information held in the systems. Confidential paper files must be kept in a locked area and computer-based files must be stored securely in locations that provide access only to those who need it. Specific access permissions should apply where necessary.

6.4 Where sensitive or personal information is to be sent by email staff should consider using the appropriate Sensitivity Label (see guidance on the Intranet )

6.5 The use of information for reports, monitoring and funding applications must avoid any specific detail about individuals that might lead to their identification unless they have given written permission for it to be so used.

6.6 Constructive liaison with other organisations is sometimes essential if individuals and groups are to be offered an effective service by the RCN Group. However, users of Group services must have given their permission before any information that is held by the RCN about them can be passed on to a third party where that information specifically identifies them or might lead to their identification.

6.7 Information held by the RCN Group will not be used or supplied for the purpose of direct commercial marketing without the consent of the member. In the case of directories or similar publications, the Group will seek consent from organisations or individuals before releasing their details into the public domain.

6.8 If confidential work needs to be stored in shared folders, Team sites or channels, you must ensure that only those who are authorised have access to it. Personal folders should not be shared.

6.9 All access to computers is password protected. Users should not disclose passwords or security details to others. Disclosure of this information may result in disciplinary action.

6.10 No sensitive information should be sent via email without following the RCN Group's Data Protection Policy.

## 7 Exceptions

7.1 The RCN acknowledges that, on rare occasions, it may be necessary to break the basic rules of confidentiality. There are only three exceptional areas for a service user with capacity where disclosure may be made without consent. These are where:

- statute law requires it
- there is a court order necessitating it
- disclosure may be necessary in the public interest where a failure to disclose information may expose the individual, or others, to risk of death or serious harm

7.2 In such cases, staff should discuss the matter with the appropriate ET member. Decisions that are made, and the reasons for them, must be properly recorded. Members should initially raise the matter with the relevant Senior Regional Officer, who will escalate the issue as necessary.

7.3 When confidential information is divulged without consent, except where it might result in more harm to other people, the individual concerned should be informed and given an explanation of all resulting actions taken.

## 8 Sharing information within the RCN Group

8.1 In order to give the best possible service to users of RCN Group services, it is sometimes necessary to share information with other colleagues within the Group.

8.2 Similarly, it is important that in meetings staff and members should feel able to talk freely. Information given to staff or members acting on behalf of the RCN Group is, in these circumstances, considered to be given to the Group as an organisation rather than to the individual staff member or volunteer. However, it should be absolutely clear to all attending such meetings that they are bound by the RCN's rules of confidentiality and that confidential matters must not be discussed outside the RCN.

8.3 Meeting papers that contain confidential information should be clearly marked 'Confidential'. Where appropriate all such papers should be collected at the end of the meeting by the meeting organiser, and securely destroyed.

8.4 Casual or social discussion about members or other service users is strictly prohibited.

## 9 Impact Assessment

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

## 10 Policy Review

10.1 It is the responsibility of the Information Governance Manager to monitor and review this policy and to present any necessary changes, after negotiation with the Partnership Forum, to the Executive Team.

| | |
|---|---|
| Title | RCN Group Confidentiality Policy |
| Status | Draft |
| Version No. | 2.2 |
| Date of approval | 28 February 2023 |
| Author(s) | Huw Bevan – Associate Director of Group Technology Operations, Security and Data Transformation<br><br>Idris Evans – Information Governance Manager |
| Approved by | E.T. & Partnership Forum<br>RCNI Executive Team & Partnership Forum Council |
| Circulated to | All staff and individuals processing RCN Group data |
| Next review date | March 2026 |