RCN GROUP IT POLICY

Who does this policy apply to? This applies equally to all • permanent staff • temporary staff • agency staff • 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 • volunteers • secondees • 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. • anyone in the above roles carrying out the activities described regardless of location including remote working
Purpose and description of the document This policy sets out the responsible and acceptable usage of information technology (IT) within the RCN Group for all authorised people, and underlines that it is essential that staff and members understand their responsibilities when using Group IT for work purposes. The policy seeks to do this in context of supporting staff and members to work more effectively and efficiently wherever they are
Document name RCN Group IT Policy
Author/s Huw Bevan – Associate Director of Group Technology, Operations, Security & Data Idris Evans – Information Governance Manager
Cross Reference RCN Group Confidentiality Policy RCN Group Data Protection Policy
Status and version Approved – final v7.5
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
Date policy approved and by whom: RCN Council - TBC 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 2024
Department responsible for Review: Transformation, Innovation and Digital

CONTENTS

1 Introduction

Purpose

1.1 This policy sets out the responsible and acceptable usage of information technology (IT) within the RCN Group for all authorised people, and underlines that it is essential that staff and members understand their responsibilities when using Group IT for work purposes. The policy seeks to do this in context of supporting staff and members to work more effectively and efficiently wherever they are.

Aims

1.2 The aims of this policy are to:

- ensure that everyone working for or with the RCN Group, or undertaking duties as a member, understands the basis on which they must use Group IT
- provide clarity on individual responsibilities to ensure that the use of Group systems is consistent with business objectives
- protect confidential data
- protect systems from viruses, theft, and misuse
- prevent unauthorised use

Scope

1.3 This policy covers the RCN Group including its entities RCN, RCNi and RCN Foundation, and applies to all use of IT equipment owned by the RCN Group, or any other IT equipment used to store, process, or transfer RCN Group data. A breach of, or failure to comply with, this policy may result in disciplinary action.

1.4 This applies equally to all

- permanent staff
- temporary staff
- agency staff
- 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
- volunteers
- secondees
- 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.

- anyone in the above roles carrying out the activities described regardless of location including remote working

1.5 Throughout this policy the term 'users' is used to refer to anyone in any of the above roles who have cause to make use of RCN Group IT systems and equipment.

2 Protection of the IT Environment

User accounts

2.1 Your system access use is linked to your username and as such, any activity undertaken within an account will be attributed to you as its owner.

2.2 Unique usernames (user identification) and passwords protect initial access to all computer systems and software. For remote access to systems Multi Factor Authentication (MFA) will be used in addition. Automated tools are used to continuously monitor user accounts, including user behaviour and changes to privileged groups. Identified abnormal activity or security incidents will be investigated.

2.3 As a user you must:

- select your own passwords that are at least 9 characters long; passwords must be a mixture of uppercase and lowercase letters, and numerical or special characters. Passwords cannot be a repeat of any of the previous 12 passwords used. You will be prompted to change every 90 days
- keep passwords confidential. Using another person's user account or sharing your own password may result in disciplinary action. If you require day-to-day access to another user's account, for example access by a Personal Assistant to their manager's account, please contact the appropriate IT team
- lock computers when leaving your desk unoccupied (regardless of location)
- log out and switch off your computer at the end of your working day unless there is a legitimate reason for leaving it on
- report immediately to the relevant IT team if you have reason to suspect that someone has tried to enter the computer environment illegally, accessed your own or anyone else's user account and/or has been tampering with any IT equipment.

2.4 All information on RCN Group computer systems is the property of the RCN Group. To maintain the balance between individual privacy and operational effectiveness, the IT Department will not grant access to

a user's system and/or mailbox without permission of the individual unless sections 2.5 to 2.9 below apply.

2.5 There may be occasions when your manager, another staff member or senior Region/Country officer requires access to your system, for example where urgent correspondence has been sent to an absent party. In these circumstances the relevant IT Department will access the user's OneDrive and/or email account without their permission to retrieve the specified document(s) only. Only a Senior Manager (for staff) or Region/Country Director (for members) can authorise this access via the Associate Director of Group Technology Operations, Security and Data Transformation or Information Governance Manager for RCN access and the IT manager for RCNi access. The task will be performed by the Information Governance team and at no stage will the manager / department lead have access to personal items. For issues relating to RCN Foundation and RCNi, approval and notification will be made to the relevant senior manager.

2.6 There will also be occasions, such as potential and ongoing disciplinary matters, when greater access to a user's IT account and/or equipment may be required. A senior manager can request this, with the approval of the Director of People and OD, via the Associate Director of Group Technology Operations, Security and Data Transformation or Information Governance Manager for RCN access and the senior management team via the IT manager for RCNi access. For further information, please see the RCN /RCNi Disciplinary Policy and Procedure.

Access will only be granted where there are legitimate reasons and will be provided for a time-limited period to a named individual for the retrieval of information relating directly to the matter only.

2.7 Amending Teams Call Forwarding settings/Voicemail/Out of office message on a user's account or redirecting incoming emails/calls to another user (e.g. during annual leave/unplanned absence) must be authorised by a senior manager.

2.8 A senior manager can authorise another staff member's "write" access to a new staff user's calendar prior to their start date so that meetings can be scheduled. The manager should notify the user of this on their first day and how it can be removed. In the case of members this same authorisation applies to senior officers such as Region or Country Directors.

2.9 There may be occasions when, to comply with legislation (such as the Data Protection Act 2018 or UK GDPR) searches of emails or an individual's OneDrive may be needed without the prior permission of the

mailbox/OneDrive owner - for example to comply with Subject Access Requests or to comply with notification requirements for data breaches. These searches will only be undertaken by the RCN's Data Protection Officer, the Information Governance Manager, or the Information Governance Officer and each search will be automated and logged. This will be undertaken by the RCNi IT Manager for RCNi staff.

IT Staff

2.10 So that IT staff can carry out their duties, they have elevated privileges including the ability to access other users' data. This will only be used in line with 2.6, 2.7 and 2.8 above or with the permission of the user or Information Asset Owner to resolve support calls. (Information Asset Owners are senior members of staff responsible for specific systems or data sets).

2.11 IT Staff have separate accounts – one for routine tasks and another for system administration tasks.

2.12 IT Staff must not use any IT equipment or system access for any activity that they are not specifically authorised to carry out.

2.13 Access logs to IT Server Rooms and secure locations are reviewed at least every six months and access codes change accordingly.

IT Equipment

2.14 Your computer is a valuable piece of equipment – please treat it as such.

As a member of staff or a member who has been provided with equipment, you should:

- avoid eating and drinking near computer equipment
- not leave equipment in a position where it is at risk – e.g. balancing on a narrow surface, close to a source of liquid etc
- ensure that your workstation and/or equipment are not left unprotected, e.g. by locking your account during periods of inactivity, using the lock function on your docking station where this is available and/or locking your equipment away for prolonged periods. It is the responsibility of all staff and members to safeguard RCN Group equipment and information
- not leave equipment on view in a public location or unattended in a vehicle. If leaving equipment in a vehicle is unavoidable it must be stored securely out of sight in the boot, and the vehicle must be locked. Equipment should not be left in a vehicle overnight

- always carry the equipment in the cabin and not place it with checked-in items when travelling by air, subject to the local and airline regulations and law
- store files on the main file servers to ensure that they are backed up and available for other team members

Laptops should be taken home each night where possible.

2.15 The RCN Group, as employers, will provide an environmental and IT infrastructure that seeks to protect the health and safety of staff and members.

2.16 The IT Department purchase and install all business laptops, desktops, tablet computers, mobile phones and printers. These tasks are not to be carried out by staff or members.

2.17 Staff and members who are provided with equipment will be informed when equipment needs replacing. Appropriate arrangements will be made including the return of the equipment to be replaced.

2.18 The IT Department will fully encrypt all RCN Group owned mobile devices, including but not limited to laptops, smartphones, and tablets.

2.19 Equipment is allocated to posts/roles rather than to individuals, the exception being where specialist equipment may be required to support users with their individual needs. It is the line-manager's or senior Regional officer's responsibility to ensure the equipment belonging to the post is retained and allocated to the individual covering the post when a staff member is away from the organisation on a long-term basis.

2.20 The management of IT equipment allocated to activists is the responsibility of local regional/country offices. It is important that conversations take place in supervision sessions to ensure that reps are using their equipment. If the equipment is not being adequately used then it can be reallocated to another rep who can use it.

Unauthorised changes to the system

2.21 Users must not alter their computer operating system, set-up or configuration. The IT Department is responsible for all systems' set-up including the corporate and local networks.

2.22 Standard user accounts will not have administrative permissions assigned to them.

Use of own devices (sometimes known as 'bring your own device' or BYOD)

2.23 With the move to Cloud-based systems, there is increasing access from personal devices such as smartphones and tablets. This is permitted on the basis that the following conditions shall apply:

- Where equipment has been provided by the RCN Group to enable you to undertake your role, this equipment must be used unless there are specific reasons why it cannot be used, and these reasons need to be reported to the IT Service Desk
- Access to RCN data will be controlled by Application Protection Policies defined by RCN IT and will include forcing the encryption of RCN data on non-RCN devices.
- The device must lock itself with a password or PIN if it is idle for five minutes.
- After five failed login attempts, your domain account will lock. Contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network or RCN data.
- The RCN data on an individual's device may be remotely wiped if
  - the device is lost
  - the individual's employment/engagement with the RCN Group is terminated
  - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure. This will not affect the individual's own data or applications on their device
- At no point will the individual to be permitted to attach non-RCN equipment to the core RCN network, only "guest access" networks out to the Internet will be permitted.

New software

2.24 In order to protect the RCN Group network, software must never be downloaded from the internet. If a piece of software is identified as a potential valuable business tool, please contact the relevant IT team. They will investigate compatibility and license implications and check for a suitable alternative in our software library before proceeding. It is essential that no software licences are breached.

2.25 The relevant IT Department purchase and install all software.

Where applications (apps) are installed onto RCN Group provided mobile phones and tablets, you must ensure that no RCN Group data is placed at risk. Unless the IT Department has provided the app, you will be responsible for any costs incurred i.e., initial purchase fee or 'in

app' costs. Please contact the IT Department if you have any questions or concerns.

Malware protection

2.26 Malware is any software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system or data. The minimum effect is to create confusion and concern; the more serious types can cause catastrophic and permanent damage to RCN Group data.

2.27 Viruses and other forms of Malware are usually transmitted via e-mail or by downloading files from the internet. Even software obtained directly from legitimate vendors has been known to carry a virus. Although steps have been taken to protect the RCN Group network against virus attacks, new strains appear every day. It is important for you to remain vigilant and report any suspected problems to the relevant IT team immediately.

2.28 You must never attempt to access any external software packages via the internet using RCN Group equipment unless authorised by the relevant IT team. If you suspect that there is any form of virus on your workstation or RCN Group networks, you must report this to the appropriate IT team immediately.

Reporting incidents

2.29 In order to ensure that information security events and weaknesses with IT can be acted upon they must be reported to line managers/ Information Asset Owners (see 2.10 above) and the appropriate IT team (RCN/RCNi) as quickly as possible. If you are not sure of the relevant Information Asset Owner, report it to your line manager and the relevant IT team.

2.30 Examples of security events and incidents include but are not limited to:

- loss or theft of IT equipment
- loss of RCN data
- provision of RCN data to unintended recipients
- loss or theft of paper records, such as files, notebooks, governance papers/confidential/commercial information etc
- loss of service or facilities
- system malfunctions
- breaches of physical security arrangements
- uncontrolled system changes
- access violations

2.31 Any personal data breach, where there is a risk to the rights and freedoms of individuals, must be reported. It is vital that ALL data breaches are reported immediately to the RCN Group Data Protection

Officer by contacting data.protection@rcn.org.uk or call 02920 546400 to make them aware of the breach. All breaches must also be reported by completing the Data Breach form on the RCN Intranet. RCNi Staff must notify the RCNi IT Manager and the RCN Group Data Protection Officer (see also section 3 below).

The Data Protection Officer must report breaches to the supervisory authority (the Information Commissioners Office) without undue delay and where feasible no later than 72 hours after we (the RCN Group) become aware of it. This is a requirement of the UK GDPR. Guidance on the reporting process can be found at Data breach reporting | ICO.

3 Data Protection and File Management

3.1 The RCN Group's Data Protection Officer is the RCN's Associate Director of Group Technology Operations, Security and Data Transformation.

3.2 You are responsible for managing the information stored within your system. Data should be organised so that it is easily understandable, clearly labelled and retrievable by other authorised users, where appropriate. Data should only be stored on Microsoft Teams, Microsoft OneDrive or the network drives and kept up to date/deleted when no longer needed, in line with the departmental retention requirements.

3.3 In general, individuals should only be able to see/read and modify/write information or data for which they are authorised. A range of data protection methods enable this and allow exceptions to be managed where these are necessary.

3.4 You should not store personal data including music or photographic files on any RCN Group equipment that is not related to your role.

3.5 Use of removable media should be avoided where possible, but if you are downloading data onto a removable storage device (e.g. a USB stick) you must keep this secure and erase it after use. You must never store sensitive or personal data on these devices unless it is encrypted. Such devices must be kept locked away when not in use.

You must never remove sensitive data from RCN Group premises without it being encrypted, unless you have authorisation from both the Information Governance Manager and your Senior Manager. This includes all files and/or programs stored on removable storage devices.

3.6 All credit card data stored and handled by the RCN Group and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the RCN

Group for business reasons must be discarded as soon as possible in a secure and irrecoverable manner (such as a crosscut shredder).

3.7 If there is no specific need to see the full credit card PAN (Primary Account Number), it must be masked when displayed. Unprotected PANs must not be stored or sent to the outside network via end user messaging technologies like chats, messenger etc.

3.8 It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media
- The CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of the payment card) on any media
- The PIN or the encrypted PIN Block under any circumstance

Back-up

3.9 To ensure that no data is lost, it must be stored on either the OneDrive or the departmental group (G:, S: or Z: Drives) or Microsoft Teams. These are backed-up daily to ensure data is not irretrievably lost should one of your local drives become lost or corrupted.

3.10 The local drive (C) is not backed up and therefore must not be used for data storage as these files will not be backed up.

3.11 The Infrastructure Team within the IT Department will regularly test and practise a 'restore' procedure that meets the operational needs of all centrally backed-up data and systems.

4 Acceptable Use

4.1 All IT activity is monitored. As a user of RCN IT equipment, you must ensure that your use of IT is consistent with acceptable practice and the RCN Group's business objectives.

It is generally unacceptable to use the RCN Group's resources and equipment to obtain or transmit information for private purposes.

4.2 In accordance with our Data Protection Policy, you must maintain the confidentiality, integrity and availability of any personal data or information that you have access to.

4.3 Breaching any of the provisions in this policy may result in action, such as under the Disciplinary Policy & Procedure for employees or Resolution process for members, even if the breach occurred outside

of working hours and regardless of whether RCN Group equipment or facilities are used

4.4 Examples of unacceptable usage include but are not limited to:

- The creation, transmission, or use of any offensive, obscene, or indecent images, language, data, or other material
- The creation, transmission or use of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety, including the sending of chain e-mail and Spam (that is, unsolicited or undesired bulk electronic messages)
- The creation, transmission or use of material which is designed or likely to compromise the security of the RCN Group's systems or data, including network security information and usernames/passwords or PINs
- The unauthorised transfer of any RCN information (either person identifiable or RCN corporate information) in any format, electronic, video, paper based or photographed
- The creation, transmission or use of defamatory material that makes a false claim, is expressly stated, or implied to be factual, may cause offence and/or may bring the RCN Group into disrepute
- The transmission of material that infringes the copyright of another person or organisation, where the sender does not have the explicit permission of the owner or does not own the copyright
- The transmission of material that breaches the duty of confidentiality, such as data from the CRM
- The unnecessary transmission of large volumes of material (for example, more than 200MB) that requires excessive amounts of network capacity and data storage. This includes using RCN equipment for the streaming of video content that is not work related, and connecting personal equipment to RCN Wi-Fi resources to stream video content
- The transmission of unsolicited commercial or advertising material either to other RCN Group users, or to organisations and individuals connected to other networks. This could be considered as spam and have the potential to breach data protection legislation. Please refer to the sections on Bulk Email (5.11-5.16 below) for additional guidance
- Excessive or inappropriate access to, or use of, the RCN Group network for private/personal use
- The storage and/or transfer of any sensitive information such as member information / staff information without encryption or approval. For guidance on the definition of what is or is not sensitive data please refer to the Data Protection Policy
- Unauthorised representation of the RCN Group using electronic media during or outside work time
- Connecting any unauthorised device to the RCN Group network

- Entering any computer system or trying to use any program for which you do not have authority
- Accessing data for which you do not have authority
- Modifying, changing, or deleting data which you have not been authorised to do
- Allowing unauthorised use of any equipment issued to you
- Interfering or tampering with hardware or software
- Deliberately disclosing (leaking) information that should not be shared
- Using RCN Group hardware (for example, laptops) for any of the above prohibited activities, regardless of location – i.e. when using the equipment remotely such as working from home or during trips away from the office or branch

Internet Usage

4.5 Access to the internet is provided solely for business use. The RCN Group recognises that some users may wish to make occasional use of the internet for personal purposes via Group equipment. This is permitted provided it is limited to outside working hours and during breaks, kept within discretionary reasonable levels and conducted in accordance with the principles of acceptable usage outlined in 4.1 to 4.4 above. Access to the internet should not interfere with users' responsibilities or productivity.

4.6 If a manager has concerns regarding apparently excessive or inappropriate personal use of the internet by a team member, they should discuss this with the colleague in the first instance where appropriate.

4.7 The RCN Group reserves the right to restrict access to websites.

4.8 Any accidental access to an inappropriate site should be terminated immediately.

Corporate Social Networking

4.9 'Corporate social networking' is the use of social networking sites such as Facebook and Twitter for RCN Group business purposes. Where corporate social networking is part of your role, your manager will work with you to set clear objectives and parameters for the use of these sites.

4.10 Staff undertaking corporate social networking are officially representing the RCN Group. You must never claim to be representing the RCN Group on any public platform unless authorised to do so.

Personal use of social media

(See also the RCN Social Media Policy 2019 (for members))

4.11 The RCN Group respects your right to privacy while protecting its confidentiality and reputation. IT users must therefore not use social media to:

- post, express their support for, and/or distribute content which contains derogatory or disparaging comments about the RCN Group, its members and its affiliates including staff, customers, and suppliers
- harass, bully, or unlawfully discriminate in any way including in breach of our Respect at Work Policy and Equality, Diversity & Inclusion Statement
- breach any other law or ethical standards – for example, using social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements
- take any action which would damage working relationships between members of staff and/or members/customers of the RCN Group, or adversely affect the Group's reputation and standing

4.12 You should always check the latest guidance on Social Media usage on the Intranet

4.13 You must not post comments about sensitive business-related topics, such as the RCN Group's performance.

4.14 If you see content in social media that disparages or reflects poorly on RCN Group, please notify your manager. All staff are responsible for protecting the RCN Group's reputation.

4.15 You should make it clear on social media where you are speaking on your own behalf – e.g. by writing in the first person and using a personal e-mail address on your personal accounts.

4.16 You are responsible for what you communicate on social media in a personal capacity. Remember that what you publish may be publicly accessible in perpetuity, and that questionable or unacceptable comments – even if made a number of years previously – can be referenced and used in a way that could adversely affect your reputation, and that of the RCN Group.

4.17 You may be required to remove social media or other online content which breaches this or other RCN Group policies.

4.18 If you are suspected of breaching any part of this policy, you must comply with any ensuing investigation as far as is reasonable.

Security and Identity Theft

4.19 You are responsible for all activity on your IT account. You must keep your IT password(s) secret (including your email password if different) and should refrain from writing it down. Do not share your IT credentials with anyone – be especially aware of potential phishing scams – and do not attempt to obtain or use anyone else's IT credentials. Safeguard all data to which you have access, and respect everyone else's data.

4.20 Do not leave your device unlocked when your workstation is unattended. Doing so creates a risk that someone may be able to access your account and e.g. obtain confidential information for which you have responsibility, and/or send an email using your identity. (See also guidance on use of email and messaging in section 5 below).

4.21 You must:

- ensure that no information is made available that could provide a person with unauthorised access to the RCN Group's systems and data and/or any confidential information
- refrain from recording any confidential information regarding the RCN Group on any social networking site or other public platform

5 Email and Messaging

5.1 Communication channels within the RCN Group, including email and MS Teams accounts, are provided strictly for business purposes. Messages sent via these channels should be as concise as possible, accurate, courteous (see also 5.5 below) and necessary.
A limited amount of personal communication and non-work messaging is acceptable as long as it is kept within reason.

5.2 Messages should not be sent to a larger audience than is reasonably justifiable, particularly when they contain attachments. Repeated 'reply-all' and copying-in of groups of colleagues 'for information' (however well-intended) can be aggravating for recipients and time-consuming for them to check messages which may not be relevant to them. Ensure that ongoing email conversations involve only those who need to be directly addressed.

5.3 Carefully check all incoming email attachments. Before clicking on them to open them up ensure that they are genuine document files (.DOC, .XLS, .PDF etc) and are not executable files (.COM, .EXE, etc) which may carry viruses and other threats. Certain attachment file types are prohibited

due to the unacceptable security risk they represent; these will be blocked from the RCN Group network, and the intended recipients will be notified of this action.

If you are in any doubt about a potential danger from any email attachments, or the veracity of an email itself, always check with the relevant IT team.

5.4 Keep your email folders in good order and arranged according to appropriate headers rather than simply keeping everything in your inbox. Also ensure that redundant messages are regularly deleted to avoid amassing large numbers of old emails.

5.5 Ensure that e-mail is not used to defame others, as this may become the basis for legal action even if the email in question is from some time ago and even if you have deleted the email from your account folders (see also 5.6 below regarding retention). Bear in mind that there have been cases where organisations have been found liable for the email activities of their employees/system users and have had to take severe disciplinary proceedings against offenders.

5.6 RCN Group retention protocol is that all emails sent and received using Group equipment, Microsoft Teams sites, and Microsoft Teams Channel messages will be retained for a maximum of seven years. Microsoft Teams Chat messages are retained for 60 days.

5.7 Bear in mind that emails may be treated as written evidence in law. Any email which forms part of a commercial negotiation or contract for goods, services or employment might be required as evidence in a court of law and should be carefully stored in a folder where it is unlikely to be deleted accidentally.

5.8 All users must be aware of the danger of inadvertently making or varying, by email, a legally binding contract on behalf of the RCN Group. No-one should correspond by this means with suppliers of goods or services to the RCN Group unless they are authorised to do so. Where such authority exists, communications should contain appropriate disclaimers stating that the content of the email is non-binding or subject to contract. Care should be exercised when communicating with members and customers about the nature or scope of service to be provided by the RCN Group.

5.9 The email system enables sensitivity labels, which should be used wherever appropriate. These control what can be done with emails when they are sent; for example, ensuring that emails can only be sent internally, blocking forwarding of the email by the recipient, and preventing the copying or printing of the email content. More information on the use of sensitivity labels can be found on YourSpace

at Must read: cyber security and sensitivity labels in Outlook - Your RCN Group Space

5.10 When IT are notified of a user leaving (staff member, rep, Council member) the user's mailbox will normally be deleted after their last day in that role. Mailboxes may be retained in certain specific circumstances, but these would need to be approved by either an ET Director for staff/rep accounts or Chair of Council for retaining any Council/Committee member accounts.

Departing users should always, before they leave, check their email account to ensure that any personal information is deleted before they leave their role and that any work that needs to be handed over is passed on.

Bulk Email

5.11 Bulk e-mail is unsolicited e-mail sent quickly in large quantities, and can be an efficient, cost-effective, and environmentally friendly way of facilitating communication. A bulk email is defined as any email with more than 20 recipients, where some or all the recipients are not personally known to the sender. It should be as brief as possible, clear and concise, and only used for important messages relevant to all recipients. You should avoid frequent or repeated messages. See 5.13 and 5.14 below for further guidance on bulk email content.

5.12 The use of bulk email is often a part of RCN Group business, and can be a useful way of enabling communication across and outside the Group, and within divisions. However, unless carefully managed, unsolicited bulk email can lead to annoyance and complaints, and may result in Group email addresses being blocked by external parties if they perceive the mails to be a nuisance. The following are guidelines to assist Group email users to employ bulk emails as effectively as possible.

5.13 Bulk email is usually appropriate for messages that:

- directly relate to carrying out the business of the RCN Group
- relate to changes in RCN Group policy or time-sensitive issues
- inform a select group of people (e.g., members, staff, other interested parties) of an announcement or event related to the RCN Group.

Please seek approval from the RCN Communications Department or RCNi Marketing Department if you wish to send bulk email for any other purpose.

5.14 Inappropriate use of bulk email includes, but is not limited to messages that:

- are not in line with the aims and objectives of the RCN Group
- are personal in nature
- have not been approved by a senior manager

Sending Bulk E-mail

5.15 Bulk Email is intended to allow the RCN Group to meet its obligations under the UK GDPR regulations, the Data Protection Act 2018 and the Privacy of Electronic Communications (EU Directive) Regulations 2003. The policy ensures that bulk member/customer communications are co-ordinated by the Member Engagement and Campaigns team and restricts how many can be sent in a given period. It is primarily aimed at limiting marketing and member services communications. It is not permitted to share passwords for the bulk email system.

5.16 There are no restrictions on sending bulk emails to members in their capacity as activists, providing that they are not advertising a product, event, or service.

6 Remote Access

6.1 The RCN Group provides users with remote access facilities which enable them to work from non-RCN locations or carry out member duties as though they are in an RCN office. All key applications are available via remote access using appropriate safeguards and layers of security.

6.2 When using the RCN Group remote access facility all the provisions of this policy still apply. (See 2.14-2.20 in particular).

7 Legislation

7.1 Use of the RCN Group's computer equipment and IT systems is subject to legislation. The following five pieces of legislation place direct legal responsibilities on users:

- The UK General Data Protection Regulations (GDPR)
- The Data Protection Act 2018
- The Copyright, Designs and Patent Act 1988
- The Computer Misuse Act 1990
- The Health & Safety at Work Act 1974

The application of the above legislation is discussed in further detail below.

7.2 UK GDPR and the Data Protection Act 2018:

The Associate Director of Group Technology Operations, Security and Data Transformation is the RCN Group's Data Protection Officer and is responsible for all personal information within the RCN Group under the Data Protection Act.

The UK GDPR protects the rights of individuals about whom information is recorded on a computer as well as personal information that is held and processed manually.

All users must complete UK GDPR training on a two-yearly basis, and are responsible for day-to-day compliance. Under the provisions of this legislation you must:

- shred physical documents and delete electronic files containing personal data that are no longer needed
- maintain personal data as accurately as possible
- store all personal data securely

For more information see the Group Data Protection Policy.

7.3 The Copyright, Designs and Patent Act 1988

This Act covers the illegal copying and theft of software, and all users must comply with software copyrights. It is an offence to copy, publish, adapt, or use computer software without the specific authority of the copyright holders.

Any abuse of this Act will be the responsibility of the user and will be a breach of RCN Group disciplinary rules. Users found to have breached the Act may also be liable to prosecution.

7.4 Computer Misuse act 1990

This Act aims to ensure that only authorised personnel use computer equipment, software, and peripherals and that these are used only for authorised purposes.

7.5 Health and Safety at Work Act 1974

This Act requires employers to regularly review equipment, premises, and work systems to identify hazards and reduce the risks to employees, contractors and the self-employed.

Detailed guidance about use of visual display units (computers, laptops, smart phones etc) is available in the Health and Safety (Display Screen Equipment) Regulations 1992 (amended in 2002).

Please refer to the relevant RCN Group Health & Safety policies for further information.

Users must contact the relevant IT team to report any damage or other health and safety concerns relating to IT equipment.

8 Breach of this policy

This policy is intended to ensure that staff and members understand the basis on which they should use RCN Group IT systems.

Access to the internet, email and all other applications and features of the IT system may be withdrawn if they are misused. Where appropriate, disciplinary action may be taken in accordance with the RCN/RCNi Disciplinary Policy and Procedure. Anyone in breach of this policy may be liable to prosecution where the breach is unlawful under the provisions of the relevant legislation as set out in section 7 above.

9 Maintenance of the policy

9.1 The content of this document is not exhaustive but indicates issues that the RCN Group considers most pertinent in the management of information technology.

Should you require assistance on any issues arising out of your responsibilities, please discuss them with your manager, or the relevant IT team.

10 Impact Assessment Statement

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

11 Policy Monitoring and Review

11.1 It is the responsibility of the Director of Transformation, Innovation and Digital to monitor and review this policy, and ensure that any changes are presented to the RCN and RCNi Executive Teams for approval, and ensure that any required changes have been negotiated with the respective recognised trade unions.

12 Compliance

This policy complies with requirements in:

- The Computer Misuse Act 1990
- The Copyright, Design and Patent Act 1988
- The Data Protection Act 2018
- UK General Data Protection Regulation (GDPR)
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications Regulations 2003
- The Health and Safety at Work Act 1974
- The Health and Safety (Display Screen Equipment) Regulations 1992 *(as amended 2002)*
- Waste Electrical and Electronic Equipment (WEEE) Regulations 2006
- Health & Safety at Work (NI) Order 1978 and Health & Safety (Display Screen Equipment) Regulations (NI) 1992 *(as amended 2002)*

Title	RCN Group IT policy (RCN Group policy on the use of information technology)
Status	Draft
Version No.	7.5
Date of approval	
Author(s)	Huw Bevan – Associate Director of Group Technology Operations, Security and Data Transformation Idris Evans – Information Governance Manager
Approved by	ET & Partnership Forum RCNi Executive team & RCNi Partnership forum Council
Circulated to	All staff & members representing RCN Group
Review cycle and next review date	30/03/2024