RCN GROUP IT POLICY

Version 7.3

Document control summary

Title	RCN Group staff IT policy (RCN Group staff policy on the use of information technology)
Status	Approved
Version No.	7.3
Date of approval	August 2020
Author(s)	Huw Bevan – IT Operations Manager Idris Evans – Information Security & Compliance Manager
Approved by	ET & Partnership Forum RCNi Executive team & RCNi Partnership forum
Circulated to	All staff
Next Review Date	September 2022

VERSION CONTROL SUMMARY

Version	Date	Summary
1.0	12 March 2008	The following policies were replaced: • Staff Policy on the Use of Information Technology (July 2006) • E-mail Privacy Guidelines (January 2008) • Policy on the Access to, and Usage of, E-mail and the Internet (August 2004)
2.0	27 November 2008	Minor revision
3.0	8 September 2009	Policy amended to include: • procedure on personal internet usage, and corporate social networking (section 4.0) further to the lifting of restrictions on the use of social networking sites from 17 August 2009; and • supporting guidance for staff on using the internet (Appendix 1).
4.0	20 February 2012	Approved by Partnership Forum
4.4	2 September 2013	Approved by Partnership Forum
5.0	24 September 2013	Approved by ET
6.0	1 March 2018	Review prior to new EU GDPR implementation. Make policy RCN Group wide.
6.1	16 April 2018	Changes following RCN, RCNi and partnership forum feedback
7.0	24 April 2018	Approved by ET
7.1	25 July 2019	Update of authorised access types and changes to reflect re-organisation of departments
7.2	13 September 2019	Updated following feedback from Senior Managers
7.3	25 June 2020	Updated following feedback form Group Sevretary

CONTENTS

Introduction

Policy Statement

Technology is transforming the way in which the Royal College of Nursing Group (RCN Group) functions as a business. The effective use of new technologies is key to enabling smarter working practices and shaping the way we work together to achieve our objectives for the RCN Group. With the right technology choices people may work just as well away from the office. Social networking enables greater flexibility in the way we interact with and learn from each other.

While technology has significant positive potential in supporting staff to work more effectively and efficiently wherever they are, it is essential that staff also understand their responsibilities when using technology during their work. The Group IT Policy outlines the responsible and acceptable usage of technology by staff within the RCN Group.

The aims of this policy are to:

- ensure that everyone working for or with the RCN Group understands the basis on which they must use RCN Group Information Technology (IT). This applies equally to all permanent staff, temporary staff, agency staff, accredited representatives, any RCN member holding a governance position, volunteers, secondees, and any person authorised to use RCN systems, such as students or trainees, those on temporary placements, contractor's staff and computer supplier employees.
- provide clarity on individual responsibilities to ensure that the use of RCN Group systems is consistent with the RCN Group's business objectives; and
- protect confidential data; to protect systems from viruses, theft and misuse; to prevent unauthorised use.

This policy complies with requirements in:

- The Computer Misuse Act 1990
- The Copyright, Design and Patent Act 1988
- The Data Protection Act 2018
- The European General Data Protection Regulation (GDPR) 2018
- 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)*

Scope of the Policy

This policy covers the RCN Group including RCN, RCNi and RCN Foundation, and applies to all use of IT equipment. A breach of, or failure to comply with, this policy may result in disciplinary action.

1.0 Protection of the IT Environment

1.1 User Accounts

1.1.1 Unique user names (user identification) and passwords protect initial access to all computer systems and software. System software audits continuously operate to identify and investigate security incidents.

1.1.2 As a user you must:

- select your own passwords in accordance with the specified requirements which you will be prompted to change every 90 days
- select passwords that are at least 9 digits long; these must be a mixture of uppercase letters, lowercase letters, and numbers or special characters (for example @~'#!"$%). They cannot be a repeat of any of the previous 12 passwords used
- keep passwords confidential. Using another member of staff's password or sharing your own password may result in disciplinary action. If you require day-to-day administrative access to another user's account, for example access by a Personal Assistant to their manager's account, please contact the appropriate IT team.
- refrain from using offensive or obscene words or images
- lock computers when leaving your desk unoccupied. You can do this by pressing the "Ctrl, Alt and Del" or the "Windows key and L" simultaneously.
- 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 RCN / RCNi IT department if you have reason to suspect that someone has tried to enter the computer environment illegally and/or has been tampering with any IT equipment.

1.1.3 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.

1.1.4 All information on RCN Group computer systems is the property of the RCN Group. In order 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 1.1.6 or 1.1.7 below apply.

1.1.5 There may be occasions when your manager or another staff member requires access to your system, for example where urgent correspondence has been sent to an absent member of staff. In these

circumstances the relevant IT Department (RCN or RCNi) will access the users H: Drive and/or email account without their permission to retrieve the specified document(s) only. Only a Senior Manager can authorise this access via the IT Operations Manager or Information Security & Compliance Manager for RCN access and the IT manager for RCNi access.

1.1.6 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 IT Operations Manager or Information Security & Compliance 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 for the retrieval of information relating directly to the matter only.

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

1.1.8 A senior manager can authorise another staff member's "write" access to a new staff member's calendar prior to their start date so that meetings can be scheduled. The manager should notify the staff member of this on their first day and how it can be removed.

1.1.9 There may be occasions when, in order to comply with legislation (such as the Data Protection Act 2018 or GDPR) searches of emails or H: Drives may be needed without the prior permission of the mailbox/H: drive owner- -for example in order 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 or the Information Security & Compliance Manager and each search will be logged and the Group Secretary will be notified and the search will only be undertaken with the express consent of the chief Executive & General Secretary . This will be undertaken by the RCNi Head of IT for RCNi staff

1.2 IT Staff

1.2.1 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 1.1.6, 1.1.7 and 1.1.8 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)*

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

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

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

1.3 IT equipment

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

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

As a member of staff you should:

- avoid eating near computer equipment
- not leave equipment in a position where it is at risk i.e.balancing on a narrow bookcase, 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 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.
- store files on the main file server to ensure that they are backed up and available for other team members.
- Laptops should be taken home each night where possible.

1.3.3 The IT Department purchase and install all IT equipment.

1.3.4 Staff are informed and appropriate arrangements made when equipment needs replacing.

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

1.3.6 Equipment is allocated to posts rather than to individuals, the exception being where specialist equipment may be required to support staff with their individual needs. It is the line-managers responsibility to ensure the equipment belonging to the post is retained and allocated to the individual covering the post

1.4 Unauthorised Changes to the system

1.4.1 Users must not alter their computer system set-up. The IT Department is responsible for all system set-up including the corporate and local networks.

1.5 New Software

1.5.1 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.

1.5.2 The relevant IT Department purchase and install all software.

Where applications (apps) are installed onto RCN Group provided mobile phones, 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.

1.6 Virus Protection

A virus is a small program that attaches itself to certain other software files. As these files are used, the infection spreads to other files, and can spread across an entire network. The minimum effect is to create much confusion and concern; the more serious types can cause catastrophic and permanent damage to RCN Group data.

Viruses are usually transmitted via e-mail or by downloading files from the Internet. Even shrink-wrapped new software 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.

You must never:

- Load any unauthorised software on to an RCN Group owned portable device, PC or network – this includes items such as screen savers, and free software supplied with some newspapers or magazines.
- 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.

1.7. Reporting incidents

1.7.1 In order to ensure that information security events and weaknesses with Information Technology can be acted upon they must be reported to line managers/ Information Asset Owners and the appropriate IT team.as quickly as possible. (*Information Asset Owners are senior members of staff responsible for specific systems or data sets – if you are not sure of the relevant Information Asset Owner, report it to your line manager and the relevant IT team)*

1.7.2 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.

1.7.3 Any personal data breach, where there is a risk to the rights and freedoms of individual, 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 be reported by completing the Data Breach form on the RCN Intranet. RCNi Staff must notify the RCNi head of IT and the RCN Group Data Protection Officer
Our 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) becomes aware of it. This is a requirement of the General Data Protection Regulation (GDPR).

1.8. Responding to incidents

1.8.1 The appropriate IT team will respond to all incidents in line with their SLAs. They will also be referred to the Information Security and Compliance Manager for any further investigation and action.

1.8.2 We will follow Information Commissioner's Office guidance on data security breach management.

2.0 Data Protection and File Management

2.1 The RCN Group has appointed the RCN's IT Operations Manager as its Data Protection Officer.

2.2 You are responsible for managing the information stored within your system. Data should be organised so that it is easily understandable

and retrievable by other authorised users, where appropriate. Data should only be stored on the network drives, and kept up-to-date/deleted when no longer needed, in line with the departmental retention requirements.

2.3 In general, all staff should only be able to see (read) and have (write) access to information or data to which they are authorised. A range of data protection methods enable this and allow exceptions to be managed.

2.4 You should not store personal data including music or photograph files on any RCN Group equipment.

2.5 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. Devices must be kept locked away when not in use.

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

2.7 All sensitive 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 (cross cut shredder).

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

It is strictly prohibited to store:

2.8.1 The contents of the payment card magnetic stripe (track data) on any media.

2.8.2 The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media.

2.8.3 The PIN or the encrypted PIN Block under any circumstance.

2.9 Back-Up

2.9.1 To ensure that no data is lost, it must be stored on either the user's home drive (H), or the departmental group (G) or shared drives. These drives reside on central file servers and are backed-up daily to ensure data is not irretrievably lost should one of your drives become lost or corrupted.

2.9.2 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.

2.9.3 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.

3.0 Acceptable use

All IT activity is monitored. As a member of staff, 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.

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

Breaching any of the provisions in this policy may result in disciplinary action even if the breach occurred outside of working hours and regardless of whether RCN Group equipment or facilities are used.

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 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, 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, in excess of 200MB) that requires excessive amounts of network capacity and data storage. This includes streaming of video content that is not work related on RCN equipment and connecting personal equipment to RCN Wifi 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 Bulk Email Section 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 isn't sensitive data please refer to the Data Protection Policy.
- Unauthorised representation of the RCN Group using electronic media either during work time or outside.
- 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 for which you have not been authorised to do.
- Allowing unauthorised use of any equipment in your possession.
- Interfering or tampering with hardware or software.
- Using RCN Group hardware (for example, laptops) to access, store or transmit any of the above.

4.0 Internet

4.1 Personal use of the internet

4.1.1 Access to the internet is provided for business use. The RCN Group recognise that some staff may wish to make occasional use of the internet for personal purposes.

4.1.2 Staff are permitted to access the internet for personal use at times. These are:

- before and after working time
- during breaks.

4.1.3 Access to the internet should not interfere with staff responsibilities or productivity.

4.1.4 All use of the internet should be conducted in accordance with the principles of acceptable usage outlined in section 3.0 above.

4.1.5 If your manager has concerns regarding excessive or inappropriate personal use of the internet, they should discuss this with you in the first instance where appropriate.

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

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

4.2 Corporate Social Networking

4.2.1 'Corporate social networking' is the use of social networking sites such as Facebook and Twitter for RCN Group business purposes.

4.2.3 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.

4.2.5 Staff undertaking corporate social networking are representing the RCN Group.

4.2.6 You must never claim to be representing the RCN Group unless authorised to do so.

4.3 **Personal use of social media**

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

- post, express their support for content 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 our Respect at Work policy and Equality, Diversity & Human Rights 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 of the RCN Group.

4.3.2 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.

4.3.3 You are personally responsible for what you communicate on social media in a personal capacity. Remember that what you publish maybe read by the masses for a long time.

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

4.3.5 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.

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

4.3.7 If you are suspected of breaching any part of this policy, you must comply with our investigation so far as is reasonable. This may involve providing relevant passwords and login details.

4.4 Security and identity theft

You should:

- ensure that no information is made available that could provide a person with unauthorised access to the RCN Group and/or any confidential information.
- refrain from recording any confidential information regarding the RCN Group on any social networking website.

5.0 E-mail

5.1 All emails sent and received using RCN Group equipment are archived and stored for a maximum of seven years. Microsoft Teams Sites will be retained for seven years, Microsoft Teams Channel Messages will be retained for seven years. Skype for Business Instant Messages (IMs) and Microsoft Teams Chat messages are retained for 60 days.

5.2 Certain file types which may be attached to emails are prohibited as they represent an unacceptable security risk to the RCN Group, and will be blocked from the RCN Group network. Intended recipients will be notified that these have been blocked.

5.3 All staff 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 about the nature or scope of service to be provided by the RCN Group.

6.0 Bulk Email

6.1 Bulk e-mail, by definition, is unsolicited e-mail sent quickly in large quantities, and can be an efficient, cost-effective, and environmentally friendly way of facilitating communication.

6.2 Generally speaking, bulk e-mail is appropriate for:

- Messages that directly relate to carrying out the business of the RCN Group.
- Messages that relate to changes in RCN Group policy or time sensitive issues.

- Messages that inform a select group of people (e.g. members, staff, interested parties etc.) of an announcement or event related to the RCN Group.

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

  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.
- Messages that are personal in nature.
- Messages that have not been approved by a senior manager.

6.3 Sending Bulk E-mail

Bulk Email is intended to allow the RCN Group to meet its obligations under the GDPR, the Data Protection Act 2018 and the Privacy of Electronic Communications (EU Directive) Regulations 2003. The policy ensures that bulk member and 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.

A bulk email is defined as any email with more than 20 member recipients, where some or all of the recipients are not personally known to the sender. It should be brief, self-explanatory, clear and concise, and only used for important messages relevant to all recipients. You should avoid frequent or repeated messages.

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.

7.0 Remote access

The RCN Group provides its staff with remote access facilities which enable them to work from non-RCN locations as though they are in an RCN office. All key applications are available via remote access.

When using the RCN Group remote access facility this policy still applies.

For further information, please contact the IT Department.

8.0 Law

Use of the RCN Group's computer equipment is subject to legislation. Five pieces of legislation place direct legal responsibilities on users and these are:

- The 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

8.1 The General Data Protection Regulations (GDPR) and Data Protection Act 2018

The IT Operations Manager is the RCN Group's Data Protection Officer and is responsible for all personal information within the RCN Group under the Data Protection Act.

All staff must complete General Data Protection Regulation (GDPR) training on an annual basis.

The 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 staff are responsible for day-to-day compliance.

You must:

- Shred documents containing personal data that are no longer needed.
- Maintain personal data as accurately as possible.
- Store all personal data securely.

8.2 Copyright, Designs and Patents Act (1988)

This Act covers the illegal copying and theft of software and all users must comply with software copyrights.

Any abuse of these Acts will be the responsibility of the user and will be a breach of RCN Group disciplinary rules. You may be liable to prosecution.

It is an offence to copy, publish, adapt or use computer software without the specific authority of the copyright holders.

8.3 The 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.

8.4 Health & Safety

The Health & Safety at Work Act 1974 requires employers to regularly review equipment, premises and systems of work to identify hazards and reduce the risks to employees, contractors and the self-employed.

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

The majority of RCN Group staff are users of this equipment (computers, laptops, smart phones etc.).

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

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

.

9.0 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.

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

10.0 Monitoring and Reporting

10.1 IT systems, especially the internet and email, are continuously monitored and audited to ensure their integrity, as well as compliance with legal and contractual obligations, and allow capacity planning.

10.2 Although individual emails are not opened, all email will automatically be scanned by specialist software. Content may be highlighted for review by members of the IT Department for the purpose of security.

11.0 Breach of this policy

This policy is intended to ensure that staff working for or on behalf of the RCN Group understand the basis on which they should use RCN Group IT systems.

Access to the internet or email may be withdrawn if they are misused.

Where appropriate, disciplinary action may be taken in accordance with the RCN / RCNi Disciplinary Policy and Procedure.

12.0 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.

13.0 Policy Review

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 negotiating changes with the respective recognised trade unions.