MEMBER IT POLICY
(own equipment)
Version 1.0

Document control summary

Title	Member IT Policy (Using non-RCN equipment to access RCN systems)
Status	Approved
Version No.	1.0
Date of approval	24 April 2014
Author(s)	Idris Evans - Information Security & Compliance Manager
Approved by	RCN Council
Circulated to	All Members who use non RCN equipment to access RCN systems
Next Review Date	October 2015

VERSION CONTROL SUMMARY

Version	Date	Summary
1.0	23 October 2013	• Approved

CONTENTS

Introduction

Policy Statement

Technology is transforming the way in which the Royal College of Nursing (RCN) 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. 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 members to work more effectively and efficiently wherever they are, it is essential that members also understand their responsibility when using technology to perform their roles. As such the Member IT Policy has been created to outline the responsible and acceptable usage of technology by members of the RCN.

It should be noted that the RCN will decide which members are permitted access to its IT systems and which of these members will be allocated RCN e-mail addresses.

The aims of this policy are to:

- ensure that everyone acting on behalf of the RCN understands the basis on which they should access the RCN's IT systems. This applies to members of the RCN, branch officials, accredited representatives and Council members;
- provide clarity on individual responsibilities so as to ensure the use of RCN systems is consistent with the RCN's business objectives; and
- protect confidential data; to protect systems from viruses, theft and misuse; to prevent unauthorised use and to prevent breach of copyright.

This policy complies with requirements in:

- The Computer Misuse Act 1990;
- The Copyright, Design and Patent Act 1988;
- The Data Protection Act 1998;
- 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; and
- 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 applies to all members accessing the RCN's systems; using non-RCN provided equipment, and should be read in conjunction with the Data Protection Policy for Members.

For the purposes of this policy the term members applies to all members of the RCN, branch officials, accredited representatives and Council members authorised to use the RCN systems. A breach of or failure to comply with this policy may result in removal of this access.

It should be noted that there is a separate IT policy for staff members.

Member policy on the use of Information Technology

1. Protection of the IT Environment

1.1. **User Accounts**

1.1.1. The RCN provides members with the facility to log-on (sign-on) at the beginning of each computer based work session using a unique personal Username and Password to identify themselves.

1.1.2. The use of user names (user identification) and passwords protect initial access to all computer systems and software. System software audits are continuously operated in order that any security incidents can be investigated.

1.1.3. All members are required to:

- select their own passwords and will be asked to change them at regular intervals, at least every 90 days;
- select passwords that are at least 9 digits long and a mixture of uppercase and lowercase letters and numbers or special characters and must not be a repeat of any of the previous 12 passwords used;
- keep passwords confidential. Use of another member's password or sharing of their own password may result in the removal of access.
- refrain from using offensive or obscene words or images, the use of which is strictly forbidden;
- change any passwords generated and issued by the Service Desk;
- lock computers using the standard computer lock in Windows, which can be accessed by pressing the keys "Ctrl,Alt and Del" simultaneously when leaving your desk unoccupied. This will prevent anyone else using your network account;
- log out and switch off their workstation at the end of their working day unless they need the PC for remote access;

- report immediately to the Service Desk if you have reason to suspect that someone has tried to access the RCN environment illegally and/or has been tampering with any IT equipment used for accessing RCN systems.

1.1.4. The RCN identifies usage of its systems by your username and password. On no account can usernames or passwords be divulged to anyone. Your computer use is directly related to the username and password. Any member sharing his or her password should be advised that this is not permitted and may result in removal of their access

1.1.5. All information on the RCN computer system is the property of the RCN. In order to maintain the balance between individual privacy and operational effectiveness however, the Information Technology Department will not grant access to a member's RCN mailbox without permission of the individual unless in accordance with the procedure to be followed as per sections 1.1.6 and 1.1.7 below.

1.1.6. There may be an operational requirement where a Regional or Country Director requires access to member's RCN mailbox in their absence, when there are legitimate reasons to do so, for example, where urgent correspondence has been sent to the mailbox by a another member. In these instances the Information Technology Department will access the member's RCN mailbox without their permission to retrieve the specified document(s) only. Only a Regional or Country Director can authorise this emergency access via the Information Security & Compliance Manager.

The authority will only be granted for operational reasons to access specific operational material. Managers will not be given general access to the member's RCN email account. Only the Information Technology department will be able to retrieve the requested information.

1.1.7. There may be occasions when access is required to a member's RCN systems and/or mailbox. A member of the Executive Team can request this with the written approval of the Director of Governance Support via the Head of Information Technology or the Information Security & Compliance Manager.

Any such access requests will be time limited and need to relate to a specific investigation/issue over a specified period of time. Only information relating directly to the issue under investigation will be supplied.

1.1.8. In both instances access requests will be time limited and need to relate to specific matters over a specified period of time.

1.2. **Virus Protection**

1.2.1. 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 which 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 operational data.

1.2.2. Viruses are usually transmitted via e-mail but are increasingly occurring as a result of files being downloaded from the Internet. Even shrink-wrapped new software has been known to carry a virus.

1.2.3. Steps have been taken to protect the RCN network against virus attacks but new strains are appearing every day. Therefore it is important that all members remain vigilant and report any suspected problems to the Service Desk immediately.

Do not:

- Load any unauthorised software on to the RCN network – this includes items such as screen savers, and free software supplied with some newspapers or magazines.

Do:

- Report immediately any suspicion you have about any form of virus on your workstation or the RCN network to the Service Desk.

1.3. **Reporting incidents**

1.3.1. In order to ensure that information security events and weaknesses with Information Technology can be acted upon they should be reported to regional officers and the Service Desk.as quickly as possible.

1.3.2. Examples of security events and incidents include, but are not limited to:

- Loss or theft of ICT Equipment
- Loss or theft of paper records, such as files, notebooks, governance papers/confidential/commercial information etc.
- Loss of service, equipment or facilities
- System malfunctions
- Human errors
- Non-compliance with policies or guidelines
- Breaches of physical security arrangements
- Uncontrolled system changes
- Malfunctions of software or hardware
- Access violations

1.4. **Responding to incidents**

1.4.1. All Incidents reported to the Service Desk.will be responded to as defined in current SLAs and will also be referred to the Information Security and Compliance Manager for any further investigation and action required.

1.4.2. The response to all incidents will follow the Information Commissioner's Office guidance on data security breach management. Any allegation of a breach of

data protection will be investigated by the RCN IT Operations Manager and the relevant Regional Director, who will produce a report for the Director of Finance.

2. Data and File Management

2.1. **Information Security**

2.1.1. RCN members who are accessing the RCN's IT systems using non RCN equipment must ensure the security of the information they are accessing.

2.1.2. Members must not download, store or record data that includes any personally identifiable information such as: Name, Address, Membership number or any other sensitive information, etc. which if lost or stolen could be used for Identity theft and would breach the Data Protection Act.

2.1.3. RCN representatives must not store any RCN member information on any equipment. All member information should be record in the Case Management system.

2.1.4. Members are responsible for ensuring that equipment used to access the RCN's network has up to date virus protection and that virus scans are performed regularly.

2.1.5. Members must safeguard unauthorised access to the RCN network by ensuring the devices are "locked" or the member is logged off when not in use.

3. Acceptable use

3.1. Members have an individual duty to ensure that their usage of Information Technology is consistent with acceptable practice and is consistent with the RCN's business objectives. It is generally unacceptable if the RCN's resources are used to obtain or transmit information for private purposes. Members should be aware that software is used to monitor all IT activity.

3.2. Examples of ***unacceptable usage*** are given below.

- The creation, transmission or use of any offensive, obscene or indecent images, 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's systems or data, including network security information and user names/passwords or pins.

- The creation, transmission or use of defamatory material, that makes a false claim, expressly stated or implied to be factual, that may cause offence and/or may bring the RCN in to disrepute.

- The transmission of material such that it infringes the copyright of another person, where the sender does not have the explicit permission of the owner or does not own the copyright themselves (See RCN Intellectual Property Policy).

- The transmission of material that breaches the duty of confidentiality, such as data from the membership database.

- The transmission of large volumes of material (for example, in excess of 20MB) that requires excessive amounts of network capacity and data storage.

- The transmission of unsolicited commercial or advertising material either to other RCN users, or to organisations and individuals connected to other networks, this could be considered as spam and have the potential to deviate from the Data Protection Act. Please refer to the Bulk Email Section for additional guidance.

- To dial up the network, using the free remote connections to the internet, for private/personal use.

- To use RCN hardware (for example, laptops) to access, store or transmit any of the above.

- The 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 using electronic media either during work time or outside.

4. E-mail

4.1. All email sent and received using RCN e-mail addresses will be archived and stored for a period of three years.

4.2. All email sent and received using RCN e-mail addresses will remain the property of the RCN.

4.3. The RCN has implemented a size limitation on messages and users are expected to zip large attachments over 5MB. Files larger than 10MB cannot be transmitted or received. Large files should always be zipped.

4.4. Certain file types which may be attached to mail are prohibited, as they represent an unacceptable security risk to the RCN, and will be blocked from the RCN network. Intended recipients will be notified that any message(s) has been blocked.

4.5. Each mailbox is subject to an automatic archiving process, where all email over 30 days old is archived

4.6. All members must be aware of the danger of inadvertently making or varying, by email, a legally binding contract on behalf of the RCN. No-one should correspond by this means with suppliers of goods or services to the RCN unless they are authorised to do so.

5. Maintenance of the policy

5.1. The content of this document is not exhaustive but indicates issues which the RCN considers serious in the management of information technology.

5.2. Should you require assistance on any issues arising out of your responsibilities, please discuss them with the Information Security & Compliance Manager or the Head of IT.

6. Monitoring and Reporting

6.1. Monitoring and auditing of IT systems, especially the internet and email, is performed continually to ensure integrity of the systems and policies, as well as compliance with legal and contractual obligations and capacity planning.

6.2. Individual emails are not opened but all mail will automatically be scanned by specialist software. . Members are reminded that any content may be highlighted for review by members of the Information Technology department.

7. Breach of this policy

7.1. This policy is intended to ensure that members working for or with the RCN understand the basis on which they should use RCN IT systems.

7.2. Access to the systems may be withdrawn by the RCN in any case of misuse of these facilities.

8. Impact Assessment Statement

8.1. This policy has undergone an equalities impact assessment process 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 Information Security & Compliance Manager to monitor and review this policy, and to present any necessary changes to the Executive Team and relevant Committees of Council. This Policy will be reviewed an annual basis.

Member IT Policy (own equipment) Acknowledgement

Full Name:

_____

(Last) (First) (MI)

Phone Number: _____

Branch:_____

Signature:

_____

Date: _____/____/_____