RNARS

Computer Use & Operations Policy

Policy prepared by: **David Firth**

Approved by: **The Committee:** _____/_____/_____

Policy became operational on: _____/_____/_____

Next policy review date: _____/_____/_____

Draft Document for inclusion into the constitution

17th November 2017

CONTENTS

Topic	Page
Contents	2
Introduction	3
Why this policy exists	3
Policy Scope	3
Legal Considerations	3
Rights and Responsibilities	3
Existing Legal Context	4
Examples of Misuse	4
Additional Use Policies	5
Appropriate Use	5
Enforcement	5
General Information	6
Identity Theft	6
Related Documents	6
Acknowledgement Form	7

The RNARS Computer Use & Operations Policy

Introduction

This Computer Use and Operations Policy presents and explains the rules governing the use of the RNARS computing facilities at the RNARS HQ. It follows that this policy describes how RNARS members must use the Society's computer equipment and computer accounts. It also explains the rules concerning personal use. This policy is an integral part of the Society's *Data Protection Policy and related policies such as the RNARS Social Media Engagement Policy*

Why This Policy Exists

This policy exists to ensure that members use RNARS computer systems and their accounts in a safe and effective environment. Although other forms of communication that prospectively represents the RNARS brand image, poorly-judged or poorly timed activity can hurt the Society's reputation.

Policy Scope

The RNARS's Computer use and operations policy pertains to all members, as well as to contractors and volunteers, who log onto our social media platforms. Therefore, it applies to all computer use and activity that relies on RNARS computer systems on RNARS HQ, RN, or MOD premises.

Legal Considerations

The Human Rights Act 1998 Article 8
The Data Protection Act 1988
Criminal Law
Naval Regulations/The Military Code/SysOps

The RNARS provides computing, networking, and information resources to the HQ community of members, and Committee and to members at large throughout the UK and abroad.

Rights and Responsibilities

Computers and networks can provide access to resources beyond the RNARS HQ, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Members may have rights of access to information about themselves contained in computer files, as specified in the Data Protection Act. Files may be subject to search under court order or military authority. In addition, system administrators may access user files as

required to protect the integrity of computer systems. For example, following organisational guidelines, system administrators may access or examine files or accounts that are suspected of unauthorised use or misuse, or that have been corrupted or damaged.

Existing Legal Context

All existing laws, UK and EU, and RNARS regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

Misuse of computing, networking, or information resources may result in the restriction of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable RNARS policies and procedures. Complaints alleging misuse of RNARS computing and network resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of Misuse

Examples of misuse include, but are not limited to, the activities in the following list.

- Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner.
- Using the RNARS Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computing resources.
- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- Posting materials on electronic bulletin boards that violate existing laws or the RNARS's code of conduct.

- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Activities will not be considered misuse when authorised by appropriate RNARS officials for security or performance testing.

Additional Use Policies

The Computer Use Policy applies to use of all RNARS computing resources. Additional computer and network use policies and terms and conditions may be in place for specific electronic services offered by the RNARS.

In particular, the RNARS Data Protection Policy, Social Media Engagement Policy govern the use of these services. The RNARS Policy applies to the use of RNARS computers and networks for electronic communications. Users must familiarise themselves with all of these when they agree to use these services.

Appropriate Use

RNARS extends to members and the Committee, the privilege to use its computers and network. When members are provided access to the RNARS network, they are enabled to send and receive electronic mail messages around the world, share in the exchange of ideas through electronic news groups, and use Web browsers and other Internet tools to search and find needed information.

The Internet is a very large set of connected computers, whose users make up a worldwide community. In addition to formal policies, regulations, and laws which govern our use of computers and networks, the Internet user community observes informal standards of conduct. These standards are based on common understandings of appropriate and considerate behaviour. The Internet now has a much wider variety of users, but the codes of conduct persist in order to make using the Internet a positive, productive, experience. Members are expected to comply with these informal standards and be "good citizens" of the Internet.

Enforcement

Penalties may be imposed under one or more of the following: UK and EU laws, RN regulations, RNARS rules, policies and regulations,

Minor infractions of this policy or those that appear accidental in nature will be typically handled informally by electronic mail or in face to face discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

Infractions by members may result in the temporary or permanent restriction of access privileges, and notification or referral of the situation to the Committee. Those by a Committee member may result in referral to the Chair or to the Secretary.

Offences which are in violation of local or national laws may result in the restriction of computing privileges, and will be reported to the appropriate law enforcement authorities.

Identity Theft

Identity theft is a serious breach of data protection legislation and hence, of our own data protection policies and guidelines. It is a fraudulent act designed to steal money and or other information from the owners thereof.

Identity theft comes in two forms:

- Those who instigate identity theft
- Those who are victims of identity theft

The RNARS Data Protection Policy is quite clear about what happens when a case of identity theft occurs:

- ❖ Those who instigate identity theft will be permanently denied access to RNARS systems and online services, and be reported to the committee in accordance with the requirements of the RNARS data protection policies.
- ❖ Those who are victims of identity theft should immediately inform the RNARS so that their access to RNARS systems and online services under the stolen identity can be removed, pending the outcome of investigation and/or such system protection measures taken by the RNARS. When the victim has established a new identity and informs the RNARS that this has been done, then the member's access will be reinstated under the new identity.

General Information

For clarification of policies and guidelines applying to the RNARS computing and communications resources, including this Computer Use and Operations Policy, refer to the RNARS website or contact the Data Protection lead at the RNARS HQ. This and related policies are available online at the RNARS Policies page in the members area.

Related Documents:

RNARS Data Protection Policy

RNARS Social Media Engagement Policy

Acknowledgements: Berkeley University-California

Acknowledgement form

Please read policy documents carefully to ensure that you understand what is required of you before signing this document.

I confirm that I have read and been informed about the content, requirements, and expectations of the following RNARS Policy Documents:

RNARS Data Protection Policy

RNARS Computer User & Operation Policy

RNARS Social Media Engagement Policy

I agree to abide by the rules and guidelines contained in each of these RNARS policies as a condition of my continuing membership of the RNARS.

I understand that if I have questions, at any time, regarding the rules and guidelines of these polices, I will consult with the social media policy manager.

I understand that when my membership of the RNARS ceases, access to the RNARS website and social media will be discontinued and all personal data will be removed.

I understand that it is my responsibility to inform the RNARS of identity theft, and that my access to RNARS online sites will be closed as a measure of protection to myself and to the Society's online operations until I have reported that I have established a new identity.

Member Signature: _____

Member Printed Name: _____

Date Joined: _____

Membership Number_____

Received By:* _____Date:_____

*To be signed off by the Data Protection Manager or by a Committee member.