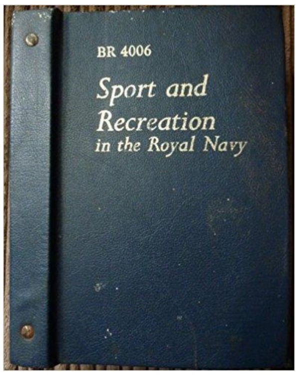
From The RNARS Chair 16th November 2017

RNARS SOCIAL MEDIA POLICY & GUIDANCE

INTRODUCTION

The RNARS was formed at HMS Mercury in 1963 as a hobby group with an interest in amateur radio. Since that time there has been an explosion in technology that now dominates both the civilian and military worlds of communications activities; computers, mobile phones, the internet and its associated websites that are grouped under the description of 'social media', and multi-mode radios that connect via the internet to establish worldwide links 24/7.

The Society has slowly caught up using social media and in using its own website as a window on the Society and its wider interests in amateur radio, and using a private or closed user-group care of one of the big internet providers. The big BUT is that the Society has not caught up with issuing its own policy and guidance on how to use the internet's social media sites safely, and on social media behaviour. There is also the issue of online security as well as that of RNARS branding. Since the RNARS is an affiliated organisation to the RN it is worth mentioning here that the Society occupies the first entry in BR 4006 *Sport and recreation in the Royal Navy Amateur Radio*, and it seems appropriate to look at what the Royal Navy has done in order to protect its own interests regarding the use of online communications and media services.



THE NEED

Clearly there is a need to formulate a policy to protect the Society's online and social media interests from misuse and abuse, and that includes the personal protection of its members from the same kinds of abuse that prevail at large on the internet. Meeting the need requires guidance and policy development on using the internet safely, personal security, privacy, media content, etc.

One of the first tasks of meeting the need is to establish, among other things, accountability and the authority to permit the use of the RNARS identity in online facilities by the individual "owners" who will sign up to the RNARS Social Media Policy as adopted by the Committee and included in the Society's constitution. For example, there have been two social media groups online for a while, in addition to our own webpage. Both have been set up in good faith by individual members of the society, but are unaccountable to the RNARS because the website providers consider that the individual who registers the media group to be the owner and, as has been claimed in the past, the user-group or forums therein do not come under the jurisdiction of the RNARS or its committee as the governing body. This has to change. This is the imperative behind the drive for adoption of a formal social media policy for the RNARS, requiring signatories who are authorised to use the RNARS identity online and manage such online media sites under the authority of the Committee.

As a consequence it would appear that the Committee may also be looking for a new functional area of responsibility; that of IT/Media Manager to oversee the day to day affairs of our social media policy, with the remit to look at the quality of materials (since it involves our brand ID), monitoring of content for bad practice and abuse, and disciplinary procedures where users are non-compliant.

GUIDANCE

Guidance forms a part of the intended structure of any social media policy. It is founded on common-sense and is intended to protect the organisation and users from getting in to difficulty and creating unforeseen problems from hacking, breaches of personal security, hate-mail, scams, hoaxes, frauds, phishing and blackmail and other forms of internet abuse. One aspect that we have to bear in mind is that we are also 'lodgers' onboard a shore establishment and as such we must be seen to be protecting ourselves on similar lines. There can be no excuses for allowing social media abuses to find their way into our online systems without first ensuring that all owners and operators are made aware of what is required of them, and how to ensure that intervention is appropriately applied. Attached is an abstract from a Royal Navy website that provides such guidance on using social media.

…the first entry in BR 4006 *Sport and recreation in the Royal Navy* is **Amateur Radio**…

For the interim it is proposed here that the Committee peruse this information for consideration to be adopted in principle, as a first step in bringing into our organisation a creditable policy on social media use, before it turns its attention to the terms and conditions of the social media policy itself. For the Committee there are other questions to answer regarding the management of social media as the 'authority' to whom both owners and users shall be accountable. Social Media Policies often contain Social Media Engagement rules that set out the limits of working online within an organisation. The definition for a social media policy is, *'a social media policy outlines the corporate guidelines or principles of communicating in the online world'* (the RNARS.org/social-media-engagement-guidelines). There are the behavioural constraints surrounding abuse, links to third party sites, ownership issues of internal materials, as well as, externally supplied materials, and caveats on opinions made by users, and so on. To help you see the kind of topics written about here I have included further material that might help us to build up a cogent social media policy. The term 'social media engagement policy' is broad and refers to not only how members represent themselves on behalf of the RNARS while online, but also how they engage socially with external organisations and individuals. While it is just as important to set out regulations and pull in the reins on members' use of social media in the pursuit of our hobby through the use of ethical guidelines for digital management.

PLANNING FOR A SOCIAL MEDIA ENGAGEMENT POLICY

A top level view with respect to defining our Society's external social policies, our development goals for the RNARS could be along the lines shown below:

- ❖ To identify the purpose of social media for our brand ID the RNARS
- ❖ To keep our Society's social media presence consistent, irrespective of how many members of the Society are actively representing our brand online
- ❖ To keep in line with our brand's voice, visual identity, goals and objectives

There are also two key components of online reputation management that should not be overlooked:

1. Preventing false or negative information from spreading
2. Encouraging the sharing of more desirable information.

(*Inc. Magazine*)

The first goal is to maintain a positive presence online via our webpage and user group(s)

The second goal is to acquire the skills to produce high quality repeatable presentations of our brand ID, the RNARS and activities related to our brand.

The third goal is to keep our goals and objective clear -our strapline and other visual aids in our website materials, e.g. good quality photos of equipment, rallies and events, etc. And social media management.

In any event, we cannot drift along ignoring the significant changes that have been made to incorporate internet safety protocols for organisational and individual behaviours. At our HQ we are subject to the Royal Navy authorities for our use of the internet, but I do wonder if anyone has ever signed up to them or even know what it is all about. Rather than jump in head first and inadvertently come up with an unmanageable beast of a policy, I would like to see if we can use some of these guidelines, if not all of them, as a basis for knitting together an almost water-tight social media policy that will protect the Society and its members from making mistakes that will have negative consequences.

SOCIAL MEDIA POLICY & GUIDANCE

POLICY

POSTING GUIDELINES

These guidelines are an example of what can be a constituent part of an effective social media engagement policy for our Society and its members. I have made amendments simply to reflect the identity of the RNARS in the following texts:

Posts include mentions, comments, and content sharing in our social media communities. We ask that you follow our posting guidelines, and note that posts will be removed if they violate the guidelines listed below.

•Do not post surveys, contests, pyramid schemes, chain letters, junk email, spamming, or any duplicative or unsolicited messages (commercial or otherwise).

•Do not self-promote or promote political causes.

•Do not defame, abuse, harass, stalk, threaten, or otherwise violate the legal rights (such as rights of privacy and publicity) of others.

•Do not publish, post, upload, distribute, or disseminate any inappropriate, profane, defamatory, obscene, indecent, or unlawful topic, name, material, or information.

•Do not upload or otherwise make available, files that contain images, photographs, software, or other material protected by intellectual property laws, including, by way of example, and not as limitation, copyright or trademark laws (or by rights of privacy or publicity) unless you own or control the rights thereto or have received all necessary consent to do the same.

•Do not use any material or information, including images or photographs, which are made available through the services in any manner that infringes any copyright, trademark, patent, trade secret, or other proprietary right of any party.

•Do not upload files that contain viruses, Trojan horses, worms, time bombs, cancelbots, corrupted files, or any other similar software or programs that may damage the operation of another's computer or property of another.

•Do not advertise or offer to sell or buy any goods or services for any business purpose, unless THE RNARS specifically approves such messages.

•Do not falsify or delete any copyright management information, such as author attributions, legal or other proper notices or proprietary designations or labels of the origin or source of software or other material contained in a file that is uploaded.

•Do not restrict or inhibit any other user from using and participating on the RNARS website page or social media pages

•Do not violate any code of conduct or other guidelines.

•Do not harvest or otherwise collect information about others, including email addresses.

•Do not violate any applicable laws or regulations.

•Do not create a false identity for the purpose of misleading others.

•Do not use, download or otherwise copy, or provide (whether or not for a fee) to a person or entity any directory of users of the services or other user or usage information or any portion thereof.

• The RNARS reserves the right to take immediate action, without notice, on any posting that in the sole opinion of the RNARS is inappropriate or violates the posting policies.

COMMITTEE VACANCY POSTINGS

Are allowed on our website as authorised by the Committee

JOB POSTINGS

Are not allowed on any of the online facilities of the RNARS

LINKS TO ANY THIRD PARTY SITES

Links in the social media communities may not be managed by the RNARS. Linked sites are not under the control of the RNARS and the RNARS is not responsible for the contents of any linked site or any link contained on a linked site, or any changes or updates to such sites. The RNARS is not responsible for webcasting or any other form of transmission received from any linked site. The RNARS may provide these only as a convenience, and the inclusion of any link does not imply endorsement of a site by the RNARS. Also, the appearance of external links on this site does not constitute official endorsement on behalf of the RNARS.

MATERIALS PROVIDED TO THE RNARS

The RNARS does not claim ownership of the materials provided to the RNARS (including feedback and suggestions) or post, upload, input or submit to any services or its associated services for review by the general public, or by the members of any public or private community, (each a submission and collectively submissions). However, by posting, uploading, inputting, providing or submitting (posting) a submission you are granting the RNARS, its affiliated organizations, and necessary sublicenses permission to use your submission in connection with the operation of their Internet businesses (including, without limitation, all of the RNARS core areas), including, without limitation, the license rights to: copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat your submission; to publish your name in connection with your submission; and the right to sub-license such rights to any supplier of the services.

SOCIAL MEDIA - FROM THE MINISTRY OF DEFENCE

Staying Safe in Social Media

Guidance

Think before you share online

In the digital age, "think before you share" is the mantra to live by. With the added potential sensitivity of sharing information about the Naval Service, "social media" use should live up to its name i.e. keep it social.

We strongly advise looking at this government guide * on best online practice, as well as taking a look at the following.

Personal Security

You should be aware of the security implications of using Facebook and other social networking websites like Twitter. Be careful with the amount of personal information you share here and elsewhere. We suggest you:

- Understand and use Facebook's privacy settings (accessible in the top right hand corner of your page)
- Do not add people that you do not know, or accept friend requests from strangers
- Have only genuine, verified friends in your friend list
- Set access permissions for your content to 'friends only'
- Remember that people on the internet may not be who they say they are

Refer to the government guide by using the link above: www.gov.uk/guidance/think-before-you-share.

www.royalnavy.mod.uk/welfare/keeping-in-touch/social-media#j344C3D5EC1C44BA38E7508B69DE0A351

Introduction

Social networking sites are great for keeping in touch with family and friends, and letting the world know what you're up to. The 'Online engagement guidelines' make it clear that we encourage the safe and responsible use of social networking sites.

This page contains guidance on how to stay safe and to think about what you post online. Remember, that there may be those who use such sites for unsavoury reasons.

Be extra careful if you have identified yourself as being a member of the military or an MOD civilian.

There is a short guide to appropriate social media behaviour for defence personnel.

You can also download the Personal security online (PDF, 1.55MB, 11 pages) file which contains some more detailed guidance.

Security and privacy settings

Whenever you join a social network, you should always look at the privacy and security settings. Do this frequently as settings are subject to change.

Each social network deals with privacy and security in different ways, and you shouldn't share information on their service until you know where that could end up.

Pictures and videos

Pictures are powerful and often revealing assets that can also pose a risk to personal and operational security if placed in the wrong hands.

Whether in a professional or personal capacity, you should always consider what information you are revealing through imagery you publish online.

Always consider how the images and videos you publish might be interpreted, and what level of information they are displaying. Remember, unless you have appropriate privacy settings activated, there is a strong chance your images can be viewed by the wider public. Consider whether you wish to identify yourself, your colleagues, family members or your location, and how you are representing your profession.

The timeline slider below uses WAI ARIA. Please use the documentation for your screen reader to find out more.

Location services and geotagging

Various social media services can use information about your location, either from a mobile device, or from your computer, and attach it to information you share on their site. Some social media is based solely around this (for example, Foursquare, where you 'check in' to places you visit).

Ask yourself what information are you giving away when you check into many locations over a long period of time? Is it possible that people could use your location to work out your routine, or where you live?

Friends and family

It's not just you who needs to think about your personal security online. Your friends and family will often know about your deployment, travel arrangements, and other information that should not be public.

Make sure that anything shared online is safe, and that you, your friends and family aren't giving away more than they mean to.

Commenting and debating

Be careful about giving away too much information as some blogs, news websites and forums are easier to search than sites such as Facebook and keep their information easily accessible for longer than sites such as Twitter.

Never share anything which could breach operational security in a comment section or forum, and be careful not to share personal information such as where you live, names of your family members, or information about anyone else unless you've received their permission in advance.

Scams, fraud, hoaxes, phishing and blackmail

Given the increasing popularity of social networking sites and the general improvement in email filters, scammers are now using these sites more and more in an attempt to harvest private information and commit varying levels of identity fraud.

Phishing, scams, frauds and hoaxes are a major source of cybercrime affecting many internet users. Most users have a basic awareness of computer viruses and a general notion of what constitutes identity theft, but a number of people don't realise the real threat that phishing, frauds and scams pose.

General tips

- use strong and unique passwords, with a different one for each site
- always check you're in the actual main site before entering any login information
- be wary of suspicious links, requests for passwords and unusual comments/messages/updates from friends/followers; scrutinise all requests carefully
- limit what information you share on your profile/account such as birth dates, phone numbers and use of geo-locating services (such as Facebook Places or Foursquare); use privacy settings to your advantage
- keep your computer software and browser up-to-date and virus-free
- select third-party applications with care
- if it seems too good to be true, it usually is, so, don't fall for it!

Related information

- Using social media: a guide for military personnel
- Defence personnel contact with the media and communicating in public)
- MOD green book: working arrangements with media organisations
- MOD online engagement guidelines