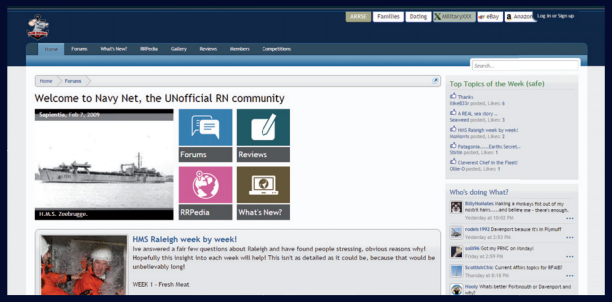

WHAT YOU CAN AND CAN'T POST ON SOCIAL MEDIA AND THE INTERNET

You **CAN'T** post Photographs taken inside Ships, Aircraft, and Submarines without official approval.

You **CAN** take photographs in authorised spaces and during public events (subject to local controls).

You **CAN** post photographs taken during public events if members of the public are allowed to take photographs.

You **CAN'T** post anything relating to the movement of your unit.

You **CAN** say where you are now (subject to local control), but not for how long, if this is attached to your unit's movements.

You **CAN'T** say where you are going to be in the future if this is attached to your unit's movements.

You **CAN'T** post information which may cause offence, bring the Service into disrepute, bring superiors into contempt, or discourage personnel.

You **CAN'T** compromise Naval Service capabilities and limitations. Don't discuss our problems.

You **CAN'T** indicate your, or anyone else's Security Clearance status.

You **CAN'T** compromise the status of Special Employment Group (SEG) personnel, especially the Submarine Service, Intelligence CB/crypto, Counter-IED, targeting and Special Forces personnel.

You **CAN'T** compromise, or post classified material, including official passes.

WHAT YOU CAN AND CAN'T DO ON SOCIAL MEDIA AND THE INTERNET

These Orders apply to all content made available on the Internet which can be accessed by multiple users, on demand, regardless of whether it is posted in a 'private' or 'public' domain.

SOCIAL MEDIA

Any material posted on social media is classed as 'Communicating in Public'.

Social media includes sites such as: Facebook, LinkedIn, Twitter, Instagram, Flickr, Youtube, blogs, chat rooms, or similar social media forums.

You **CAN** participate in unofficial social media forums, unless you are of certain Special Employment Groups.

DO NOT use social media forums to vent your frustrations, grievances and concerns on Service matters. The correct route is always through the Divisional system for Complaints and Representations.

'PRIVATE' MESSAGING COMMUNICATIONS

You **CAN** continue to use email and person-to-person messaging apps to discuss Service matters and Service life.

These must **NOT** be intended to allow access by a wider audience to the information being transmitted or communicate with the media unoffcially.

CLOUD SERVICES

You **CAN** store content in 'Cloud' services (such as iCloud and Dropbox). It does **NOT** constitute the 'public' domain, or 'Communicating in Public'. You **CAN** store photographs in the Cloud as long as they comply with the Orders and are not shared publically.

You **CAN'T** grant access to such storage with the specific intent of communicating information which is prohibited in these Orders.

If you have any questions on these Orders, or what you should be doing, contact your Command Chain or:

NAVY PSYA-INFOSEC TEAM MAILBOX (02392 25795)

For more information on Contact with Media and Communication in Public see - 2014DIN03-24 (Contact with the Media and Communicating in Public.)

navygraphics 15/1089

Back Pocket Brief

YOUR SAFETY, OUR SECURITY

Orders on the use of the Internet, Social Media and Communicating in Public

DANGERS AND RISKS OF INTERNET PRESENCE

Remember, if you reveal your employment in the Royal Navy or Royal Marines on social media, this disclosure may lead to you, your family, friends and connections being targeted by Foreign Intelligence Services, terrorists or other malign actors.

These Orders are intended to contribute to your personal security and that of those with close connections to you as a Service person, as well as the security, safety and reputation of the Service.

WHAT?

New ORDERS which will be incorporated into SGOs and FLAGOs governing Conduct of Naval Service personnel when engaged in activity on the Internet and social media.

These Orders also apply to all content presently posted on the internet and social media.

WHEN?

These Orders come into effect from 01 JAN 2016.

DON'T BE CAUGHT OUT, ACT NOW!

WHY?

To protect OPSEC, PERSEC of Naval Service Personnel and their families, friends and loved ones.

To embed a culture of security within the Royal Navy, instilling the risks associated with the Internet in general, and the use of social media in particular.

To prevent reputational damage to your Royal Navy.

WHAT YOU MUST DO

Ensure you have read and FULLY understood the new Orders.

Continually brief Family, Friends, loved ones and connections not in the Naval Service, on the sensitivities of information posted on the Internet and social media.

Remove any content presently held on the Internet and social media, which is in contravention of these Orders.

Any questions, queries and clarifications are passed up the Chain of Command through the divisional system.

SANCTIONS AND SERVICE PENALTIES ON BREACH OF ORDERS

- Breaches of these Orders on social media and Internet use are unacceptable.
- If you breach these Orders, they WILL result in Naval Penalty and Sanction.
- The decision to award (or not award) a Sanction for breach of these Orders will rest with the Commanding Officer.
- The severity of the breach is to be judged in accordance with the classification of the information compromised and the degree to which the breach is intentional.

DEFENSIVE INTERNET MONITORING

The Royal Navy and Ministry of Defence conducts Defensive Internet Monitoring (DiMon) of the Internet routinely and in accordance with MOD policy in order to ensure the security of its personnel and operations.

It is the responsibility of ALL personnel to highlight any security breaches and contravention of these Orders through the divisional system to their Unit Security Organisation.

BE AWARE

ALL personnel are subject to being targeted for malign purposes. This represents a significant threat to OPSEC and PERSEC, including the security of your family and friends.

If you are a Service person from certain SEGs, social, religious, or ethnic backgrounds and you reveal your employment status on the Internet, you may expose yourself and your family to an even greater risk of being targeted by terrorists, extremists, or affiliated individuals.

COMPROMISE OF INFORMATION BY FAMILY, FRIENDS, OR OTHER PERSONS:

If your Family, Friends, acquaintances, or connections place prohibited information on the Internet concerning you and you have NOT intended them to do so; this is **NOT** a breach of these Orders.

If this happens, you must make every personal effort to ensure that compromising material is removed immediately and to inform Unit Security Staff.

YOU ARE to ensure that you brief Family, Friends and connections on the risks and dangers associated with posting sensitive information on the Internet and Social media.