Social Network Policy

Navy Cadet Force

Navy Cadet Force

Social Network Policy

NB The title Navy Cadet Force has been shortened throughout this document to (NCF) purely to reduce costs of printing, by saving ink and paper, and thus be more environmentally friendly. This document is for internal use only.

APPLICATION

This Social Network Policy applies to all NCF officers, staff and cadets.

The policy relates to Facebook, MySpace, Bebo and other such social network sites. As a member of the NCF, whether officer, staff, member of a unit management committee or cadet the following guidelines apply to use of social network sites in relation to the NCF activities, association and the wearing of NCF uniform.

- Staff should not have cadets as friends on their page, nor should cadets have staff as friends on their page
- No photographs should be displayed without the person's permission
- It is recommended that individuals block their personal sites
- Names of officers, staff and cadets should not be tagged to photographs
- Nothing should be put on an individual's pages that would bring discredit on the NCF or compromise the integrity of the NCF
- Regular checks should be made on your pages
- Units and Staff groups may create closed groups on Facebook, provided a member of staff vets all comments being posted before they become visible to cadets.
- At no time should a member of staff send a private message to any cadet.

All new members of staff will be provided with a copy of this, and sign to confirm that they have read and understood the content.

ADVICE

It is important to take great care in relation to the information you provide on any of these sites to prevent identity theft or other problems. Advice in relation to the use of social networking sites can be found on:

http://www.commonsense.com/internet-safety-guide/social-networking.php

http://www.childnet.com/downloads/blog_safety.pdf

http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

At the end of this policy there are ten tips for avoiding problems with blogging and social network sites. These are from the Information Security Forum.

Ten ways to avoid problems with blogging and social networking sites

1 **Verify whether your organisation has an organisational policy on blogging or social networking**
In some cases these policies can apply even if you access these sites from home.

2 **Check what you are signing up to**
By accepting the terms and conditions of a blogging or social networking site, you may be giving other parties rights to use or sell things (such as personal data, details of friends, pictures) that you place on the site.

3 **Watch out for add-ons**
Be wary of loading additional features or applications that can change the original terms and conditions that you signed up to, or alter security settings.

4 **Withhold the elements of your personal life that you don't you want to make public**
Imagine that your personal details were to be published in a (global) newspaper – what would you not want to see in that paper?
If you are going for an interview, assume the interviewer has read your social networking entry – what would you not want them to have seen?

5 **Take control of your information**
Many blogging and social networking sites do offer ways of protecting your information on these sites. It often only takes a moment to check to see how you can secure your information.

6 **Resist the urge to make a blog entry when you are tired or upset**
Once it is made, it is very hard to remove a blog or social networking entry and they can be subject to legal action.

7 **Avoid placing information relating to the work you are doing on sites**
Generally organisations do not want corporate information on a social networking site and may take action if they find it.

8 **Consider how social networking and blogging sites mimic the day-to-day people interaction in the real world**
If behavior is not acceptable in the real world, then it is unlikely to be acceptable in the cyber-world.

9 **Examine carefully any e-mails coming from social networking contacts**
An e-mail may appear to come from a social network 'friend', but actually comes from a virus. Ensure that you have an up-to-date virus checker.

10 **Educate your family**
Children can be particularly attracted to social networking sites where they can be very vulnerable, and should be made aware of the dangers. Many social networking sites are not suitable for children and state on their terms and conditions that they should not be used under a certain age – follow this advice.

The Responsibility of this Policy falls to the Colonel of the Navy Cadet Force.

Signed: **Date: January 2023**

Print: Colonel Terry Fitzgerald

This Policy has been approved for distribution by the Chairman of the Navy Cadet Force.

Signed: **Date: January 2023**

Print: Luke Giles