



Social Networking Guidelines

**Market House
14 Market Street
Lerwick**

A charitable company limited by guarantee registered in Scotland No. 165677
Registered Office Market House, 14 Market Street, Lerwick, Shetland ZE1 0JP
Company Secretary Catherine Hughson
Recognised by the Inland Revenue as a Scottish Charity - No. SCO 17286

Voluntary Action Shetland

Social Networking Guidelines

New technologies have turned the majority of people into publishers of information online. Pictures and videos can be taken at any time with a mobile phone or camera and they can be sent to a list of contacts and uploaded onto a blog or a social networking profile site in a minute. Photographs once online, remain online and can be seen by anyone years after they have been posted.

PROTECTING PERSONAL INFORMATION

Many employees use the web and social networking services such as Facebook, Flickr, MSN messenger for personal use. While VAS employees are private individuals, they also have professional reputations and careers to consider.

Additionally, employees are required not to do anything to endanger the health and safety of their colleagues or others. Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff also need to be aware that many employers and other agencies now carry out web and social network service searches to find online information about potential staff – background, interests, career experiences and self-presentation. All staff, perhaps especially new staff in training and induction, need to be advised to ensure that information available publicly about them is accurate and appropriate.

Lack of privacy on the Internet seldom means communications are entirely private, even messaging. Think of Internet communications as the equivalent of sending postcards.

ADVICE FOR EMPLOYEES

When publishing information about yourself or having conversations with others online, it is important to be mindful of how you present yourself, who can see your content and how you can manage this appropriately.

When publishing information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer or colleague viewing your content.

Make sure you understand who is allowed to view your content on the sites that you use – and how to restrict access to your account where necessary. If you are not clear about how to restrict access to certain groups of people, regard all of your content as publicly available and act accordingly.

You can also check to see that other people are not misrepresenting you or treating you unfairly online. If you find things you object to, you can ask the poster to take these down in the first instance. Where cases are work related, these should be reported to your line manager or to the appropriate person as soon as possible. More serious incidents, including cyberbullying, will require

a formal response from your employer, and will be dealt within disciplinary frameworks, or in more serious cases, legal frameworks.

You can check to see if others are creating or posting objectionable material about you online by:

- Using search engines to check what images and text are associated with your name. This will help establish what information other people can easily find about you
- Using search facilities within specific social networking sites – some may require you to be a logged in member
- Encouraging everyone to report any incidents they find, rather than being a passive bystander, is an important strand of cyberbullying prevention

'Friending' refers to the act of giving contacts permission to view information or contact you within web-based services. The terminology will vary from service to service – 'Friends' may be called contacts or connections, for example. Most social sites enable you to give different levels of access and set privacy levels on your own content and activity. These functions will vary from service to service but typically include:

- Information that is only available to the account holder
- Information that is accessible by contacts on the account holder's approved list, and
- Information that is made publicly available, either within the service or across the whole of the internet.

'Friends' does not necessarily refer in this case to people who are your actual friends, although you may choose to restrict your connections to that. 'Friends' in this context may also be work colleagues, family members, and people that you have met online.

Use the privacy settings offered by social networking services and select friends online that you can trust. Only publish your own photos after thinking carefully about the potential consequences and only publish pictures of friends with their permission.

If you have a social networking account, do not "friend" clients or add them to your contact lists. You may be giving them access to personal information and allowing them to contact you inappropriately. They may also be giving you access to their personal information and activities.

Also ensure, that if you are contacted by another member of staff or volunteer seeking work related support through social networking sites, be clear that it will be dealt with upon return to the office during office hours.

Whilst social networking sites are not accessible through SIC internet during normal office hours, due to the nature of our work, some staff may work out with usual office hours and also occasionally from home. VAS needs to

ensure that staff members are safeguarded out with the office and normal office hours.

RESPONDING TO INCIDENTS AND REPORTING

Staff should report all cyberbullying incidents to the designated manager at the earliest opportunity. The designated person will take responsibility for ensuring the person being bullied is supported, and will investigate the incident. Where the perpetrator is known to be a colleague, the majority of cases will be dealt with by VAS disciplinary procedures.

Staff should keep any records of the abuse - text, emails, voice mail, web site or instant message. Do not delete texts or emails. Take screen prints of messages or web pages, and be careful to record the time, date and address of the site.

The manager should contact the executive officer where it appears that a law has been broken – for example, where death threats, assault, or racially motivated criminal offences are involved. The executive officer will contact the police. Where a potential criminal offence has been identified, VAS should ensure that any internal investigation does not interfere with police inquiries. Staff are of course able to report incidents directly to the police.

VAS RELATED POLICIES

Induction Procedure
Health and Safety Policy
Risk Assessment