SOCIAL NETWORKING POLICY

Policy Number 25
Revised July 2015

Introduction

The aim of this policy is to ensure that all workers, employees and associates of the Society are aware of their role in using Social Networking Sites responsibly in line with current best practice. While Social Networking applications bring new opportunities to understand, engage, and communicate with our audiences, it is crucial that users are not only aware of their own responsibilities when using such sites but are also aware of the responsibilities of the Society as an employer. This Policy has been developed following an increase in the occurrences where these sites have been used for less positive reasons. Employees should be aware that the Society uses social media management tools to monitor social media websites for mentions of Scotmid, Semichem and other associated brand names. This information is used for business, marketing and reputational purposes. It is also used to enforce this policy and to protect the Society and the individual. Additionally, the Society maintains public social media profiles for the Society, Scotmid and Semichem.

This Policy is based on the ACAS code for Social Networking and other sources of best practice.

This document should be read in conjunction with the IT Policy, Corporate Communications and Marketing Standards, Bullying and Harassment Policy, Whistle-blowing Policy and Disciplinary Procedure.

Scope of the Policy

The Social Networking Policy applies to all employees of the Society who are in full or part-time employment, on permanent, fixed term or temporary contracts of employment. The procedure is liable to change from time to time following consultation with the recognised trade unions.

This Policy covers the use of Social Networking and Blogging Sites; examples include, but are not limited to, Facebook, Twitter, YouTube, Linkedin, Instagram, Tumblr and Pinterest, by all Society employees, both while at work and outside of work. This Policy does not define the Society's wider approach to the use of social networking as an emerging way of delivering services and engaging with the public.

It applies to the use of Social Networking Sites for both business and personal purposes, whether during business/working hours or otherwise. The policy applies regardless of whether the Social Networking Site is accessed using the Company's IT facilities and equipment or equipment belonging to individual Employees.

Under common law, employees should be aware that there is an implied duty of trust and confidence between an employer and employee. It is possible therefore that any inappropriate use of Social Networking Sites outside the workplace could result in disciplinary action if the content leads to the Society's professional reputation being damaged, or exposes the Society to potential liabilities.

Purpose of this Policy

The purpose of this Policy is not to prevent anyone from using Social Networking Sites; it is to set standards for all employees of the Society in using them. The aim of the Policy is to make employees aware of, firstly, the issues that can arise with Social Networking usage and, secondly, the ways in which complaints, concerns or possible disciplinary action can be avoided. In line with the ACAS Guide to Social Networking, the Society will treat 'electronic behaviour' the same way as 'non-electronic behaviour'; the Society will take a serious view of inappropriate use of Social Networking Sites.

The basic premise is that employees and those associated with the Society need to exercise common sense and to realise that what they post on Social Networking Sites is essentially in the public domain, even if they have privacy settings, or material is posted on a closed profile or group. All employees are expected to follow the same standards of conduct and behaviour online as would be expected offline.

Social Networking should never be used in a way that breaches any of the Company's other policies.

Business Use of Social Media

If an Employee's duties require them to speak on behalf of the organisation in a Social Networking environment, the Employee must still seek approval for such communication from Corporate Communications who may require the Employee to undergo training before they do so and impose certain requirements and restrictions with regard to their activities.

Likewise, under no circumstances should employees make comment about the Society for publication anywhere, including in any social media outlet, without permission from Corporate Communications.

Possible outcomes from Irresponsible Social Networking Usage

Irresponsible use of Social Networking Sites can take many forms. The following list, although not exhaustive, provides some examples:

- Use of any Society logo/branding is prohibited in any personal use of Social Networking Sites; usage may be regarded as gross misconduct to which the Society's Disciplinary Procedures apply which could result in summary dismissal.
- Any attempt to set up a site in the name of another person or to use a known person's name deliberately for malicious reasons in Social Networking Sites will be investigated under the terms of the Disciplinary Procedure.
- Any communications or content you publish that may cause damage to the Society, any of its employees or a third party's reputation may amount to gross misconduct to which the Society's Disciplinary Procedures apply which could result in summary dismissal.

- Any photos or information uploaded/tagged onto Social Networking Sites of Scotmid 'staff only' areas or Scotmid property, including uniforms, will be dealt with through the Society Disciplinary Procedure.
- Negative/damaging communication about the Society, suppliers, any organisation linked with the Society or an employee may entitle the Society to state that the implied term of mutual trust and confidence between employer and employee has been broken and may be regarded as gross misconduct in line with the Disciplinary Procedure which could result in summary dismissal.
- Any discriminatory information posted about an employee by another employee will be investigated under the Bullying and Harassment Policy.

Guidance/Advice for Responsible Social Networking Usage

If an employee's personal internet presence does not make any reference to and does not identify the Society, the content is unlikely to be of concern to the Society. Employees should be aware that the Society uses social media management tools to monitor all social media websites for mentions of Scotmid, Semichem and other associated brand names for marketing and other business purposes. The following are some suggestions that can help employees protect themselves and the Society through responsible usage of Social Networking Sites:

1. Employees should be aware that even if their online Networking account is not directly linked to the Society as an employer, their employment/employer should not be discussed or implied through their Social Networking Site as the Society is a local retailer and employer.
2. Employees should refrain from discussing work issues or colleagues through Social Networking Sites.
3. An individual is free to talk about the Society as long as it does not bring the Society into disrepute, threaten confidentiality or harm the Society's reputation in any other way. These instances may constitute gross misconduct and disciplinary proceedings will be applied. A Twitter feed or a blog is not the place to air what could constitute a grievance.
4. Employees should also make it clear in Social Network postings that they are speaking on their own behalf, write in the first person and use a personal e-mail address when communicating via social media. If an Employee's duties require them to speak on behalf of the organisation in a Social Networking environment, the Employee must still seek approval for such communication from Corporate Communications
5. Employees must comply with all Society policies when using Social Networking Sites.
6. Employees must not disclose confidential information relating to the business of the Society, to their employment at the Society or to the employment of a colleague.
7. Sites must not be used to verbally abuse, defame or threaten other employees or customers. Privacy and feelings of others should be respected at all times. Employees should obtain permission from the individuals involved before posting details or pictures. The use of language, which could be deemed as offensive, obscene, vulgar, deceptive, indecent or hateful to others, should be avoided.

8. Any misuse of Social Networking Sites that has a negative impact on the Society - including what might be read to be online bullying, stalking and harassment, or use of homophobic, sexist, racist, sectarian or prejudicial language by employees - will be investigated under the Disciplinary procedure.
9. Employees are reminded to consider all cultural differences and possible interpretation before 'posting' or 'sharing' any information on the internet.
10. If you are in any doubt about something you are about to post, then don't do it.

Remember that everything you share on a Social Networking Site could potentially end up in the worldwide public domain and be seen or used by someone you did not intend, even if it appears to be 'private' or is on a closed profile or group.

Failure to Comply with Policy

Employees are responsible for the success of this policy and should ensure that they take the time to read and understand it.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any Employee suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.