

Social Media Policy

1 Introduction

This policy is intended to help staff/volunteers make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook and LinkedIn. The policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor use of social media and the action the Charity will take in respect of breaches of this policy.

2 Who is covered by the policy?

This policy covers all individuals working and volunteering at all levels and grades, including staff, consultants, contractors, trainees, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as 'staff' in this policy).

3 The scope of the policy

All staff/volunteers are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of the Charity, its services, staff, professional associates and competitors.

4 Responsibility for implementation of the policy

All staff/volunteers are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any questions regarding the content or application of this policy or any breach of this policy should be reported to the IT Manager.

5 Using social media sites the Charity's name

The Charity may choose, from time to time, to operate social media websites in order to promote the Charity, its services, its team and to improve communications with anyone associated with the Charity. The Charity will designate specific members of staff to act as social media editors on behalf of the Charity. Only those designated editors are permitted to post material on any social media website in the Charity's name and on the Charity's behalf. Any breach of this restriction could amount to gross misconduct. Passwords for access to social media websites should be changed regularly and in no circumstances should they be given to anyone who has not been designated as a social media editor.

Social media content may include news stories, events, developments in the Charity, developments in the law, and commentary on topics impacting on the Charity or its clients. The social media editors will be required to strictly observe the editorial guidelines of the Charity which does not permit the publication of any of the following:

- Anything that could potentially identify an individual client or case;
- Names of other parties involved in cases including, but not limited to, Judges, Counsel, expert witnesses, other solicitors etc.
- Personal contact details;
- Defamatory material;
- Publicity material not in accordance with SRA Code of Conduct, Chapter 8
- Instructions on new matters will not be accepted via social media.

The designated social media editors are responsible for the regular monitoring of the Charity's social media websites and will remove any content that could cause the Charity embarrassment or reputational damage.

6 Expectations

6.1 Use of social media at work

The Charity is aware that phone technology enables staff to access social media sites or other non-work-related sites on personal phone applications. Staff must not use their personal phones when they are supposed to be working or to the detriment of the expected level of performance. Furthermore when staff are working from home using personal computers to undertake Charity business they should not use social media sites or other non-work related sites when they are supposed to be working or to the detriment of the expected level of performance.

6.2 Use of social media on personal PCs/devices

The Charity recognises that a lot of staff make use of social media in a personal capacity. While they are not acting on behalf of the Charity, staff must be aware that they can damage the image of the Charity if they are recognised as being a Charity member of staff, and may bring the Charity into disrepute.

When using social media on personal PCs or devices all staff must adhere to the following guidelines:

- Avoid any postings or responses on social media which are bullying or harassing in tone towards other members of the Charity;
- Maintain confidentiality of clients and other staff when using social media. Under no circumstances should any client details or any photographs which may include images of clients be posted via social media;
- Behave professionally, and in a way that is consistent with the Charity's values and policies, if they have identified the Charity as their employer via social media.

And all staff must not:

- Post information about colleagues that they have been asked not to share, and should remove information about a colleague where instructed to do so;
- Make disparaging remarks about the Charity, its clients, members of the Charity, professional associates or competitors on a social media site
- Make any remarks on a social media site that may compromise the Charity;
- Air personal grievances related to any aspect of employment with the Charity where others may be able to read them;
- Post anything which may be considered unlawful or may otherwise bring the Charity into disrepute on their social media site / social media profile page;
- Take photos or videos on Charity premises and then post these via social media without ensuring there is anything in the photo/video that could breach client confidentiality, the Data Protection Act or that may bring the Charity into disrepute;
- Use social media to communicate on behalf of the Charity unless this is a normal, accepted part of their role;
- Unless specifically authorised, post messages under the Charity's name to any newsgroup or chat room.

Such breaches of this policy are taken very seriously by the Charity and may constitute misconduct or gross misconduct as detailed in the Charity's disciplinary procedures.

6.3 Professional Networking Sites

The expectation above relating to the avoidance of identification of the Charity on Social Media sites does not apply to professional networking sites, e.g. LinkedIn, where appropriate identification is permitted. However, all other expectations set out above still apply and contravention will be subject to the same sanctions as set out above.

7 Monitoring use of social media websites

Staff/volunteers should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under our disciplinary procedures. We reserve the right to restrict or prevent access to certain social media websites if we consider personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us. It may also cause embarrassment to us and to our clients. In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, could amount to gross misconduct (this list is not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- A false and defamatory statement about any person or organisation;
- Material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;
- Confidential information about us or any of our staff or clients (which you do not have express authority to disseminate);
- Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
- Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed under the Charity's disciplinary procedures and is likely to result in summary dismissal. Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

If you notice any use of social media by other members of staff in breach of this policy please report it to the IT Manager/Cybercrime Officer.