Social Media Policy

1. ABOUT THIS POLICY

1.1 This policy is in place to minimise the risks to our organisation through use of social media.

1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram, Vine and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our organisation in any way.

1.3 This policy covers all trustees, national executive committee members, members, employees, officers, consultants, contractors, volunteers, apprentices, work experience, casual workers and agency workers.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY

2.1 The National Executive Committee has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Chief Executive Officer and the Data Protection Officer.

2.2 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the Chief Executive Officer and the Data Protection Officer who will review this policy every 12 months to ensure that it meets legal requirements and reflects best practice.

2.3 Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that everyone understands the standards of behaviour expected of them and acting when behaviour falls below its requirements.

2.4 Everyone is responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Data Protection Officer immediately after becoming aware. Questions regarding the content or application of this policy should be directed to the Data Protection Officer.

3. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

3.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

(a) breach our IT and Communications Systems Policy;
(b) breach our obligations with respect to the rules of relevant regulatory bodies;
(c) breach any obligations contained in those policies relating to confidentiality;
(d) breach our Disciplinary Policy or procedures;
(e) harass or bully other staff or member in any way;
(f) unlawfully discriminate against other staff or member or third parties;
(g) breach our Data Protection Policy (for example, never disclose personal information about a colleague online); or
(h) breach any other laws or regulatory requirements.

3.2 You should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

3.3 Anyone who breaches any of the above policies will be subject to disciplinary action up to and including termination of employment or membership.

4. PERSONAL USE OF SOCIAL MEDIA

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

5. PROHIBITED USE

5.1 You must avoid making any social media communications that could damage our organisations interests or reputation, even indirectly.

5.2 You must not use social media to defame or disparage us, any member of the organisation or any third party; to harass, bully or unlawfully discriminate against staff or members or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

5.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.

5.4 You must not post comments about sensitive organisational-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

5.5 The contact details of business contacts made during your employment are our confidential information. On termination of employment you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.

5.6 Any misuse of social media should be reported to the Data Protection Officer immediately after becoming aware.

6. BUSINESS USE OF SOCIAL MEDIA

6.1 If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager or the Data Protection Officer, who may require you to undergo training before you do so and impose certain requirements and restrictions regarding your activities.

6.2 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to Data Protection Officer and do not respond without written approval.

6.3 The use of social media for organisational purposes is subject to the remainder of this policy.

7. BRANCH SOCIAL MEDIA SITES

7.1 Where there is a branch social media site you should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

7.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

7.3 You should also ensure that your profile and any content you post are consistent with our professional image.

7.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with The Data Protection Officer.

7.5 If you see social media content that disparages or reflects poorly on us, you should contact The Data Protection Officer immediately on becoming aware.

8. GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

8.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

8.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

8.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of us (unless you are authorised to speak on our behalf as set out in Paragraph 5.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients, members and colleagues.

8.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it.

8.5 If you see social media content that disparages or reflects poorly on us, you should contact The Data Protection Officer, immediately on becoming aware.

8. MONITORING

8.1 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

8.2 For further information, please refer to our IT and Communications Systems Policy.

9. RECRUITMENT

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

10. BREACH OF THIS POLICY

10.1 Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff 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.

10.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

10.3 Breach of this policy by a member of a Branch may result in a Branch taking such action as deemed appropriate in respect of the breach.