

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

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers internet postings, blogs and video- and image-sharing websites such as YouTube and Flickr.

You should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. You should follow these guidelines in relation to any social media that you use.

This policy applies to use of social media for work purposes as well as personal use that may affect our business in any way. This policy covers all employees.

## **Compliance with related policies and agreements**

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:

- breach our IT and Communications Systems Policy;
- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations contained in those policies relating to confidentiality;
- breach our Disciplinary Procedure;
- breach our Anti-harassment and Bullying Policy;
- breach our Equal Opportunities and Diversity Policy;

- breach our Data Protection Policy (for example, never disclose personal information about a colleague online); or
- breach any other laws or regulatory requirements.

## Personal use of social media

Personal use of social media is never permitted during working hours.

## Prohibited use

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

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

Any misuse of social media will be investigated.

## Guidelines for responsible use of social media

Unless specifically authorised to post on social media on the organisation's behalf, you should make it clear in social media postings that you are speaking on your own behalf. 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 your employer.

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.

Any communications that staff make in a personal capacity through social media must not:

- bring the organisation into disrepute, for example by criticising or arguing with customers, colleagues or rivals; making defamatory comments about individuals or other organisations or groups; or posting images that are inappropriate or links to inappropriate content.

- breach confidentiality, for example by revealing trade secrets or information owned by the organisation; giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or discussing the organisation's internal workings (such as deals that it is doing with a customer/client or its future business plans that have not been communicated to the public).

- breach copyright, for example by using someone else's images or written content without permission; failing to give acknowledgement where permission has been given to reproduce something.

- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; using social media to bully another individual (such as an employee of the organisation); or posting images that are discriminatory or offensive or links to such content.

If you see social media content that disparages or reflects poorly on us, you should alert your line manager without delay.

## Monitoring

The organisation reserves the right to monitor your social media usage. The organisation considers that valid reasons for checking a workers internet usage include suspicions that the employee has:

- been using social media for personal/non-work-related reasons when he/she should be working; or
- acted in a way that is in breach of the rules set out in this policy.

Monitoring will consist of checking the social media sites that you have visited, the duration of such visits and the content that you have contributed on such sites.

Monitoring will be conducted in accordance with an impact assessment that the organisation has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the organisation's legitimate interests and is to ensure that this policy on use of social media is being complied with.

## Data Protection

Monitoring will normally be conducted by the organisation's directors. The information obtained through monitoring may be shared with external agencies where necessary, including with your line manager, managers in the business area in which you work and other staff if access to the data is necessary for performance of their roles.

However, information would normally be shared in this way only if the organisation has reasonable grounds to believe that there has been a breach of the rules set out in this policy.

The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

You have a number of rights in relation to your data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the organisation's Data Protection Policy.

If you believe that the organisation has not complied with their data protection rights, you can complain to the Information Commissioner.

## 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.

## Breach of this policy

Access to particular social media may be withdrawn in any case of misuse.

Breach of this policy may result in disciplinary action. 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.

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 in itself result in disciplinary action.

Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

**This policy is not contractual and may be varied by the organisation at any time.**