

Social media definition

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and business networking websites such as Facebook, MySpace, Bebo, Twitter and LinkedIn. Social media also covers video and image sharing websites such as YouTube and Flickr, as well as personal blogs. This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive. This policy applies in relation to any social media that employees may use.

Use of social media at work

Employees are only permitted to log on to social media websites or to keep a blog using the Company's IT systems and equipment outside their normal working hours (for example, during lunch breaks or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. This includes laptop and hand-held computers or devices distributed by the Company for work purposes. The Company nevertheless reserves the right to restrict access to this type of websites at any time. Where employees have their own computers or devices, such as laptops and hand-held devices, again they must limit their use of social media on this equipment to outside their normal working hours.

Employees may be asked to contribute to the Company's own social media activities during normal working hours, for example by writing Company blogs or newsfeeds, managing a Facebook account or running an official Twitter or LinkedIn account for the Company. Employees must be aware at all times that, while contributing to the Company's social media activities, they are representing the Company, and to be able clearly separate any social media interactions that are of their own personal activities compared to those on behalf of the Company.

Company's social media activities

Where employees are authorised to contribute to the Company's own social media activities as part of their work, for example for marketing, promotional and recruitment purposes, website updates, they must adhere to the following rules:

- use the same safeguards as they would with any other type of communication about the Company that is in the public domain
- ensure that any communication has a purpose and a benefit for the Company
- obtain permission from their manager before embarking on a public campaign using social media
- request their manager to check and approve content before it is published online
- follow any additional guidelines given by the Company from time to time.

The social media rules set out below also apply as appropriate.

In addition, such social media accounts which are operated for business purposes (and their contents) belong to the Company and therefore these accounts used by an employee during employment may not be used after termination of employment, or notice to terminate employment, without express written permission.

Social media rules

The Company recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Company in these

circumstances, employees must be aware that they can still cause damage to the Company if they are recognised online as being one of its employees. Therefore, it is important that the Company has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-Company computers outside the workplace and outside normal working hours, employees must not:

- other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, write about their work for the Company except in general and non confidential terms - and, in postings that could be linked to the Company, they must also ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of the Company
- conduct themselves in a way that is potentially detrimental to the Company or brings the Company or its clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content
- other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, use their work e-mail address when registering on such websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the Company, for example by criticising or arguing with such persons
- include personal information or data about the Company's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 1998 which is a criminal offence
- make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the Company, its employees, clients, customers, contractors or suppliers (an employee may still be liable even if the Company, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable)
- make any comments about the Company's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying - employees can be personally liable for their actions under the legislation
- disclose any trade secrets or confidential, proprietary or sensitive information belonging to the Company, its employees, clients, customers, contractors or suppliers or any information which could be used by one or more of the Company's competitors, for example information about the Company's work, its products and services, technical developments, deals that it is doing or future business plans and staff morale
- breach copyright or any other proprietary interest belonging to the Company e.g Company Documents, research work, bespoke machinery designs, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work - if employees wish to post images, photographs or videos of their work colleagues or clients, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by the Company.

Work and business contacts made during the course of employment through social media websites (such as the names and contact details of existing or prospective customers, clients and suppliers) and which are added to personal social and business networking accounts (in particular to LinkedIn), or which are stored on the Company's computer system, amount to confidential information belonging to the Company and accordingly must be surrendered on termination of employment.

On termination of employment or once notice to terminate employment has been given, employees must, on request, disclose to the Company a full list of all work and business contacts that they hold on all devices or on all social and business networking accounts. The Company may then require the departing employee to

delete any or all such work and business connections from their devices (including from personal devices) or from their social or business networking account, not keep copies of the same and not reconnect with those connections for a period of six months from termination of employment. The Company may also require written confirmation from the employee that these provisions have been complied with.

Employees should remember that social media websites are public fora, even if they have set their account privacy settings at a restricted access or “friends only” level, and therefore they should not assume that their postings on any website will remain private.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by placing their privacy settings at an appropriate level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should employees notice any inaccurate information about the Company online, they should report this to their manager.

Social media monitoring

The Company reserves the right to monitor employees’ use of social media on the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- promote productivity and efficiency
- ensure the security of the system and its effective operation
- make sure there is no unauthorised use of the Company’s time
- ensure that inappropriate, restricted or blocked websites are not being accessed by employees
- make sure there is no breach of confidentiality.

The Company reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee.

Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company’s disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee’s immediate dismissal.