

Employer's Briefing

■ Look before you tweet

The growth of the use of social media by both individuals and organisations has led to a blurring of boundaries between the protection of business interests and the rights of privacy for individuals. This has led to an expansion of legal issues with which businesses are faced, reports Jamie Cameron of Burges Salmon LLP.

This article looks at some of the key points for businesses to consider in developing a social media policy and also addresses some of the issues that employers need to deal with in managing their employees' use of it.

Social media policy

Following some scare stories in the media, a number of businesses have taken the drastic step of issuing a blanket ban on all staff using social media at work. This does not, however, prevent employees from using social media outside work and also overlooks the fact that many employees have access to social media through their mobile phones which makes such a ban difficult to enforce.

The risks and potential benefits will vary from organisation to organisation. Whatever stance employers choose to take, it is important to analyse what impact social media may have on the business and to decide on a corporate approach. Having done so, employers should prepare a policy to support their stance. Although, it is important to protect the business, employers should avoid imposing disproportionate restrictions which may lead to them being ignored by employees as the restrictions prove unworkable.

Ideally, a social media policy should be balanced and should:

- (a) set out clear rules on the use of social media. If appropriate, provide some positive guidelines on responsible use
- (b) apply both in and out of working hours. There may be some different rules for out of hours behaviour but some obligations (eg confidentiality and not making

discriminatory comments) will apply equally

- (c) apply to all employees, although different rules may apply depending on their roles within the business
- (d) include a right to monitor its employees' communications. This potentially raises data protection issues so organisations need to ensure that employees are made aware that monitoring may take place and the extent of that monitoring
- (e) be subject to regular review to ensure it is up to date with developing technology and reflects the corporate approach of the organisation
- (f) be monitored and disciplinary action taken, where necessary, to ensure compliance.

Cyber-slacking

As a large proportion of employees now have easy access to social media while at work through mobile phones or computers, the temptation to check Facebook updates or twitter posts often becomes too great to resist. The term "cyber-slacking" is now recognised as describing one of the key concerns expressed by businesses about the use of social media in the workplace.

To deal with cyber-slacking it is important that employers set out clear rules on whether or not employees are allowed to use social media at work. Many employers will block access to sites such as Facebook altogether and may require employees to switch off their mobile phones. Others will allow access, but restrict access times. Provided that employees are aware of what is or is not permissible, employers will be able to deal with abuse through their disciplinary procedures.

Practical tip: it may not be practical or desirable to block access to social media sites altogether so consider allowing access to specific sites at set times of the day or providing a limited number of computers with unrestricted access in public areas.

■ Look before you tweet (cont'd)

Cyber-bullying

Surveys have shown that an increasing number of employees have fallen victim to cyber-bullying from colleagues through racist, sexist or homophobic comments. This type of behaviour can amount to unlawful harassment and discrimination.

It is important for employers to be aware of this as the business may be liable for the acts of employees who post discriminatory comments online, even if this is done outside work and on personal computers. To provide a defence to such a claim, employers need to show that they have taken all reasonable steps to prevent the conduct from occurring.

Practical tip: make sure any social media policy makes it clear that such behaviour will not be tolerated and will be treated as a disciplinary offence, and provide training to employees so that they are aware of and understand the policy.

Virtual misconduct

We have seen a real concern among some businesses about the damage that can be caused by the misuse of social media, for example, by employees making derogatory remarks about the business or its management. While some employers can overreact to these issues, there is an increasing body of helpful case law around this area which confirms the key principle that it is possible to fairly dismiss an employee for comments made online, even if the conduct takes place outside working hours and from non-work equipment.

Practical tip: avoid knee jerk reactions and treat issues of virtual misconduct in the same way as any other disciplinary matter.

Confidential information

A significant concern for many businesses is the apparent ease with which “private conversations” with friends on Facebook can be disclosed to a wider audience online and

confidential information (albeit unwittingly) be made public. The risk for businesses is that confidentiality is lost once information is published and employers should consider practical measures for protecting their confidential information, including reviewing employment contracts to ensure they are up to date and address this issue.

Practical tip: Introduce training for employees to ensure they are aware that their online conversations are public and that they risk losing control over information once it has been posted. Also that sensitive information is shared on a “need to know” basis only and that leaking information will be treated as a disciplinary offence even if it was non-intentional.

Recruitment

Finally, we have seen a growing trend of businesses using social networking sites to check the background of candidates, either as part of a formal process or through informal checks by their recruitment officers.

As well as giving rise to data protection issues, employers could face the risk of a claim for discrimination if an unsuccessful candidate were able to show that the reason he or she was unsuccessful was because of one of the protected characteristics under the Equality Act and that that information would not have been available otherwise. For example, many candidates no longer include their date of birth on an application form and yet their age may be ascertainable from their Facebook site. Employers should consider carefully whether they want or need to use this information as part of their recruitment process.

Practical tip: consider creating a list of legitimate sites that might be referred to, for example focusing on business sites such as LinkedIn and make it clear to prospective candidates that reference may be made to these sites as part of the recruitment process. Also, ensure that every recruitment decision is documented to show the (non-discriminatory) reasons explaining the decision. ■