AIG

Employee misuse of social media...

...is your business prepared?

Improper use of social media by employees carries potentially significant legal risks to businesses, including unauthorised disclosure of confidential information, infringement of party intellectual property rights, and liability for discriminatory, bullying or defamatory comments posted by employees.

Without a clear and comprehensive social media policy in place, businesses are at an increased risk of successful claims for unfair dismissal in the event that an employee is dismissed for inappropriate use of social media. In addition, businesses are at an increased risk of vicariously liability for the inappropriate actions of their employees on social media.

As such, it is crucial for businesses to introduce a social media policy that clearly sets out standards of behaviour and the consequences of any breach of the policy.

AIG offers all PrivateEdge policyholders a free template Electronic Communications and Social Media policy, prepared by our expert legal panel. Please click here ▶ to download it.

We set out below some answers to common questions about employee misuse of social media in the workplace.

I want to implement a social media policy – how should I go about it?

It is not enough simply to have a social media policy in place. Businesses should also ensure that they make all employees aware of the policy and its implications. All staff should be provided with a copy or informed where a copy may be viewed (such as on the company intranet). Managers and supervisors should be trained in implementing and policing the policy. If the policy is breached, businesses should take steps to deal with the breach, including taking appropriate disciplinary action where appropriate, and act consistently.

As well as introducing a policy to deal specifically with social media, employers should update their disciplinary, grievance, equal opportunities and bullying/harassment policies to include social networking. They should also provide examples of what sort of behaviour will be regarded as gross misconduct – for example, offensive, bullying or derogatory comments about other employees.

Can I ban the use of social media and the internet at work?

Yes, provided that you have a policy in place that makes the position clear to employees.

If employees are to be permitted to access the internet social media for personal use during work hours, it is advisable for employers to set unambiguous guidelines as to the amount of use permitted by specifying the particular times that such use is allowed (for example, before 9am, between 12 midday-1pm, and after 5pm, and only where workload permits). If clear boundaries are not set, a decision to dismiss an employee for use of social media during work hours could be unfair.

Do employees have a right to privacy when using social media?

Employees are entitled to the right to respect for their private and family life and the right to freedom of expression under the Human Rights Act 1998, which implements the European Convention on Human Rights (the Convention).

There is nothing in law which prevents an employer from looking at publicly available material on the internet, which can include employees' Facebook or LinkedIn profile pages. However, employees who are dismissed for their online activities may be able to argue that their freedom of expression under article 10 of the Convention should be taken into account by an employment tribunal when determining a claim of unfair dismissal, but where the public online activities amount to an unlawful act, such as harassment, bullying or defamation, the Tribunals are likely to find the employee has chosen to abandon any right to have their comments treated as private.

Is it possible to monitor staff use of social media, the internet and emails whilst at work?

In the absence of a clear policy on monitoring employees' use of social media, the internet and email whilst at work, employees may have a reasonable expectation of privacy in their communications, even those sent from their work accounts. It may be unfair to dismiss an employee in circumstances where they had such an expectation of privacy.

The Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998 place limits on employers' ability to monitor. Some of the key principles are that:

- monitoring should be proportionate (meaning that an employer must consider less obtrusive alternatives);
- employees should be provided with details about the monitoring and how it will be carried out; and
- employers are required to carry out an impact assessment to balance the needs of the employer against the employee's right to privacy.

It is therefore important to introduce and brief out a social media policy that clearly specifies the circumstances in which staff use of social media, emails and the internet will be monitored, so that employees know that there is no expectation of privacy in their use of work computers and accounts.

Can I dismiss an employee for misusing social media?

Where dismissal is justified in any particular circumstance will depend on the seriousness of the offence. Employers should treat electronic behaviour in the same way as non-electronic behaviour. If the offence is so serious as to amount to gross misconduct, it may be appropriate to dismiss after taking into account any mitigating factors. For less serious misconduct, it will rarely be appropriate to dismiss unless the employee already has a live final written warning for misconduct.

Some examples of where it may be appropriate to take disciplinary action include:

- The employee uses social media at work during times the business has made it clear such use is not permitted
- The employee has used social media excessively in breach of an acceptable usage policy
- The employee's use of social networking has damaged or is likely to damage the reputation of the business – for a dismissal on this basis to be fair, there must be evidence that reputational harm is a genuine risk - the content must be accessible by the public and the business must be readily identifiable.
- The employee accesses pornographic or criminal material using work equipment
- The employee makes a false, defamatory, discriminatory, offensive, derogatory statement about the business or its staff - where comments are made on social networking sites that are critical of the business or a colleague, there is a difference between comments that are so serious as to undermine trust and confidence and comments that are merely an ill-judged expression of dissatisfaction by the employee. Businesses are expected to have a reasonable degree of resilience when employees publicly express their disgruntlement.
- The employee discloses confidential information about the business, staff or clients
- The employee publishes material in breach of copyright

The employee's misuse of social media took place outside work – can I still take disciplinary action?

Employees can potentially be fairly dismissed for gross misconduct on the basis of their social networking activities, even where these are carried out in their own time, away from work and involve acts that are not directly related to their work. However, the conduct must in some way impact on the employee when they are doing their work.

Some examples include:

- Sending an offensive email from a home email account to an employee of an important customer.
- Publishing a personal blog that contains comments that seriously damage the business' reputation (the business must be able to clearly be identified and the blog have a sufficiently wide readership to make reputational damage a real risk)
- Making serious sexist remarks about a manager on a Facebook status update in circumstances where the employee has many colleagues who are "Facebook friends" and the manager is readily identifiable.

Kennedys
Legal advice in black and white

MILLS & REEVE

WOMBLE BOND DICKINSON

AIG

GBL00001053 1218 Social Media