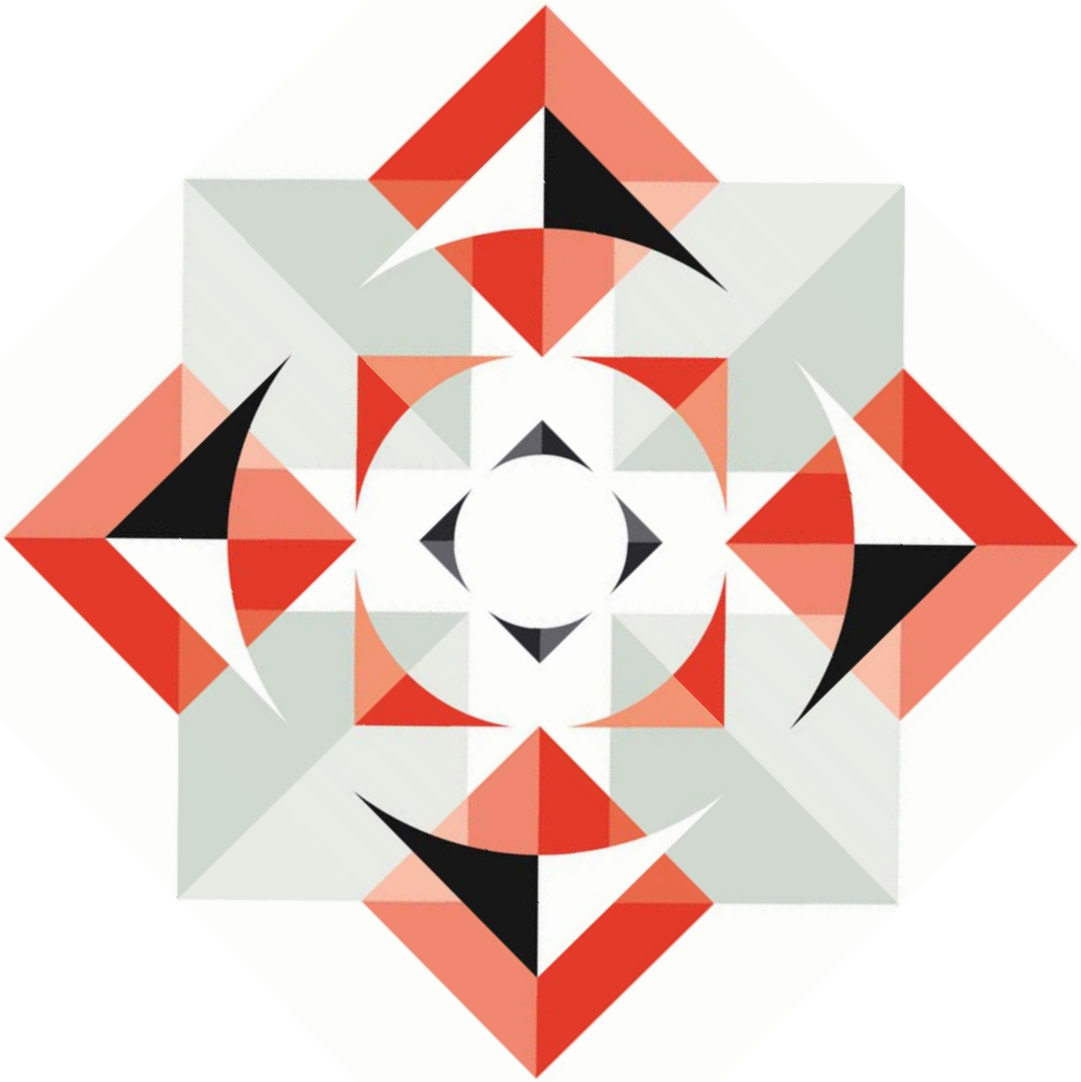
Ius Laboris UK Global HR Lawyers
LEWIS SILKIN

Social media and the workplace



Inside

Introduction

Businesses are embracing the benefits that social media brings but its recent massive growth in popularity is inevitably creating issues in the workplace as the interface between employees' work and personal lives becomes blurred.

This Inbrief focuses on the legal issues for employers raised by online activities, and explores some possible solutions.

The employment context

> Employers can reach a vast audience through social media and promote a positive image of the business or products.

> Virtual communities can contribute to increased cohesion between particular groups of employees.

> Networking with other professionals may lead to business opportunities (e.g. LinkedIn).

> An openness to modern forms of communication and interaction may enhance the appeal of the employer for recruitment purposes and enhance employee engagement.

> More controversially, the internet generally and social media in particular, can provide a rich vein of evidence in cases against an employee and can be a useful recruitment tool.

> One significant downside is that the information employees post online can cause potential damage to the business, lead to discrimination claims, or cause the leakage of confidential or proprietary information.

While these problems arrived with the internet, the escalation of social media usage means employers should revisit existing policies. In addition, if employers encourage employees to promote the business on professional networking sites such as LinkedIn and Twitter this can give rise to new problems which we look at below.

Monitoring online activity

According to research in December 2009 fewer than 15% of candidates believed that information found online could have any impact their job prospects whereas 41% of recruiters who responded said that they had rejected candidates based on their online reputations.

Where monitoring online activity takes place during employment, or to inform a recruitment decision, an employer will need to consider whether that monitoring will infringe an employee's right to privacy. If it does, the interference with that right must be proportionate. An employer also needs to be aware of its obligations under the Data Protection Act 1998 (DPA) and potential discrimination risks.

Privacy

An employee's right to privacy under the European Convention on Human Rights includes social interaction and the right to develop relationships with others.

A recent tribunal upheld a gross misconduct dismissal after an employee posted derogatory comments about his employer's products on Facebook. The dismissal was fair because the employer had a clear social media policy in place (which was explained to employees in the induction process) and he could have had no reasonable belief in the privacy of the comments. For the moment, this judgment casts doubt on the extent to which employees will be able to rely on any right to privacy for Facebook posts.

The situation may be different if an employer snoops online without an employee's knowledge or in circumstances where the employee has not authorised the content to be posted online. In this case, the employee may have a right to privacy and the employer will need to justify the interference on the basis that there was legitimate reason to act in this way and that the actions were a proportionate response to the issue identified.

Data protection

The DPA regulates the 'processing' of personal data. General obligations on employers relating to the processing of personal data become more onerous for 'sensitive' personal data (such as sexuality, race, political or other beliefs). The kind of information contained in the 'profile' section of most social networking websites typically includes sensitive personal data.

When an employer consults online sources of information to glean information about a job application, the employer is processing information for the purposes of the DPA. Although the Information Commissioner has not issued specific guidance on the use of "netrep" to inform recruitment decisions, Part 1 of the Employment Practices Data Protection Code (which contains best practice on vetting

exercises) is relevant. Failing to follow this guidance, although not of itself actionable, will be taken into account in considering any breach of the DPA. Recommendations in the Code include giving the candidate an opportunity to comment on the accuracy of the data obtained and providing specific information to candidates about the checks the employer undertakes.

There are also data protection concerns where monitoring occurs during employment. An employer must satisfy the preconditions to processing ordinary personal data and sensitive personal data (essentially that there is a permitted reason for the monitoring) and provide information to employees about the nature of the online monitoring. The employer must also meet the DPA's requirements concerning the accuracy, security and proportionality of the processing undertaken.

Discrimination

Given the types of information typically found on blogs or social networking websites, discrimination claims are also potentially a risk.

Protection from discrimination commences during the recruitment process so job applicants are afforded the same protection from discrimination as employees. A job applicant's sexuality or religious beliefs would never usually be included in their CV but employers can now gain access to such information with relative ease via the internet.

Using this information as the basis for refusing to recruit that person, or subjecting that person to a detriment, could constitute unlawful direct discrimination. Although most employers would provide a different reason for rejection, a successful claim would be likely if a job applicant were to become aware of the real reason.

The same risk of discrimination claims applies if an employer uses blogs or social networking websites to find out information about a current employee and then uses that information to that employee's detriment.

Possible solutions

An employer could ban researching job applicants over the internet. It may be better, however, to put in place clear guidelines enabling employers to take advantage of information available online in appropriate cases. For example:

> Consider which roles are appropriate for background checks and when it is appropriate to check—later on in the recruitment process would be advisable (i.e. rather than for all candidates).

> Only information that is directly relevant to the job applicant's ability to perform the role, such as information that contradicts their CV or demonstrates that the job applicant is untrustworthy should be considered.

> Ensure that only information relevant to the applicant's suitability for the job is passed on to the decision-makers.

> Give the candidate the opportunity to correct the information.

> Advise applicants where searches are undertaken that the recruitment process includes online background checks.

When monitoring online activity more generally, compliance with the Employment Practices Code, Part 3 is recommended. This requires the employer to give full information to employees about the extent of monitoring activities and ensuring that monitoring is undertaken in a proportionate way.

Protecting the business - specific issues posed by LinkedIn

LinkedIn has many advantages for business and it is not surprising that many employers actively encourage employees to use it extensively. However, it poses some new risks and embracing its use raises a number of legal questions to which there are no -or only partial - answers:

> Who owns LinkedIn connections?

> Do the business' trade connections cease to be confidential information simply because they are posted publicly on the site?

> Who owns any intellectual property that employees post on LinkedIn forums?

> Do changes to a profile when an employee changes jobs amount to a breach of non-solicitation provisions (because LinkedIn automatically tells all an individual's connections as and when the profile is updated with a new job title and place of work)?

> What do you do to regulate employees making 'recommendations' about other LinkedIn users?

> Can you capture the profile and connections when an employee leaves; and if so, how do you do this?

From a pre-LinkedIn world one case tells us that a contacts list created and kept by an employee on his employer's computer system (and which contained personal contacts and business contacts which the employee had made before joining the employer), belong to the employer. However, LinkedIn contacts may not be held on the employer's equipment and the account maybe in the employee's name.

In another case specifically dealing with LinkedIn, an employer suspected an ex-employee of having deliberately copied and retained confidential client contact information in LinkedIn. The court granted the employer's request for pre-action disclosure of the employee's LinkedIn contacts list. Where the copying is not deliberate this result may not be guaranteed.

Possible Solutions

Employers should give clear guidance on the use of LinkedIn including:

> imposing appropriate controls on content and providing guidance

> stating clearly that the account is set up for the express purpose of benefiting the employer's business

> clarifying that contacts remain the property of the business

> imposing express obligations to return information stored on such media on termination of an employee's contract

> establishing independent databases so they are not dependent on the employee's voluntary disclosure of their contacts

- reminding employees of their obligations on termination and in particular that activity on LinkedIn might breach non solicitation provisions

Restrictive covenants should also be reviewed. Pending further clarification of what amounts to an intention to solicit, non-dealing provisions may afford better protection than non-solicitation restraints.

Loss of productivity

With the increasing uptake of smartphones and tablet computing, access to social media sites is becoming boundless. If much of the access takes place at work, businesses must consider what approach to take to the consequent loss of productivity.

One case provides a salutary lesson for employers. Two sisters were dismissed for their internet usage - they said they only accessed the internet when work was slack and the employer's internet usage policy permitted access outside "core working times". The Tribunal found their dismissals to be unfair because the employer's rules about when employees could access the internet at work were unclear. If an employer does allow access during work, it must make the parameters in terms of what is permitted and when very clear.

Justifying dismissal

There may be circumstances where an employee's comments on social media are such that an employer will want to consider dismissal. Each case will turn on its facts, and provided that the employer has clear, well-publicised standards, dismissal may be appropriate (as it would be when the conduct occurs offline).

A more contentious issue is where the conduct concerns potential reputational damage alone, particularly where the conduct takes place off duty on the employee's own equipment. A fair dismissal will depend on whether:

- the employee's actions result in actual or speculative damage to the employer
- there is a breach of the employer's rules (and whether such a breach is minor or serious)
- there is a specific policy concerning the use of social media and whether this policy is clearly communicated to staff
- the conduct complained of conflicts with the employee's role (i.e. nature and seniority of the role and responsibilities)
- the employer has conducted an appropriate investigation and disciplinary procedure, and the sanction of dismissal is within the band of reasonable responses in the particular circumstances

Sensible use policy

Since much online conduct occurs off-duty on the employee's own equipment, blocking access or banning social media is unlikely to provide an effective solution. Such a draconian approach is also likely to be unpopular with employees.

A more effective way for employers to manage these issues may be to draw to employees' attention that anything they post is, in fact, public. The publication and implementation of a 'sensible use' policy can be a good way to do this. Such a policy might include:

- rules about accessing these sites at work (when is it permissible and for how long)
- information about what monitoring may be undertaken
- a reminder to employees that they must not disclose confidential information or trade secrets on such sites
- a reminder to employees not to make derogatory comments about the company, their colleagues or their clients on such sites
- a reminder that employees should not disclose other employee's personal data on these media
- a requirement that employees insert a disclaimer into any blog stating that any views contained on the blog are those of the employee and are not representative of the employer's views
- a cautionary note about 'at home' usage which might impact on the employer's reputation or business

For further information on this subject please contact:

Ellen Temperton
Partner
T + 44 (0) 20 7074 8424
ellen.temperton@lewissilkin.com