Social Media in The Workplace

CURRENT PRACTICE VS BEST PRACTICE

How is your business doing?

AN EMPLOYER'S GUIDE

FAEGRE BAKER DANIELS

INTRODUCTION

SOCIAL MEDIA IS HERE TO STAY.

Whether you are a reluctant LinkedIn networker or a voracious tweeter, your company almost certainly views social media as essential for its effective running and profitability.

Virtually all FTSE 100 companies now have a presence on LinkedIn and Twitter, often with dedicated teams to ensure they are used effectively.

A FORCE FOR GOOD

THERE ARE OF COURSE SIGNIFICANT BENEFITS TO SOCIAL MEDIA:

Increasing Brand Awareness

With millions of individuals and companies having social media accounts, it is easy to get your message out.

Learning About Your Target Audience

You can find out who is reading your social media posts, which posts are read most frequently and what people are saying about your brand.

Better Customer Service

Customers can give instant feedback, and complaints can be addressed quickly.

Learning About Competitors

A quick search of the internet will tell you what your competitors are doing.

Utilising Developments in Technology

Operating a globalised workforce, for example with remote working, can now be achieved with greater ease and efficiency.

All of these are enhanced by the fact that social media can interact with vast yet targeted audiences globally, instantly and cheaply. Used effectively, social media can increase the profitability of a business.

ON THE OTHER HAND...

THE BENEFITS USUALLY OUTWEIGH THE DOWNSIDES, BUT THE CHALLENGES CAN BE SERIOUS.

EXAMPLES INCLUDE

1. Loss of **PRODUCTIVITY** caused by employees spending time on personal social media accounts during work time.
2. Damage to **EMPLOYEE RELATIONS**, for example through cyber bullying, harassment and defamation.
3. **CONFIDENTIALITY** issues, for example inadvertent disclosure of customer, client, employee or patient details.
4. Damage to the company's **REPUTATION**, for example disgruntled employees bad-mouthing an employer's attitude toward its staff.
5. Keeping up with a **QUICKLY CHANGING TECHNOLOGICAL LANDSCAPE** and the resulting legislation, for example around the microchipping of employees which is now being put into practice in Sweden and the U.S.

THESE ARE ALL COMPOUNDED BY THE VERY THING THAT MAKES SOCIAL MEDIA ATTRACTIVE...

the ability to communicate with a large audience instantly and cheaply. In the wrong hands, social media can cause an enormous headache and threaten the reputation and profitability of a business.

THIS REPORT

This report guides employers through the potential pitfalls of social media and gives practical guidance on how to avoid them. We interviewed almost 100 CEOs, HR directors and other senior executives to find out how they manage social media in the workplace and deal with any problems that crop up, giving a rare insight into how social media is used in practice.

THE OUTCOME...

The use of social media has risen so quickly that employers have yet to catch up in terms of protecting themselves against the potential pitfalls. The law is also struggling to keep up with the speed of change. There are, however, steps which employers can and should take now to manage these risks effectively. As always, prevention is better than cure.

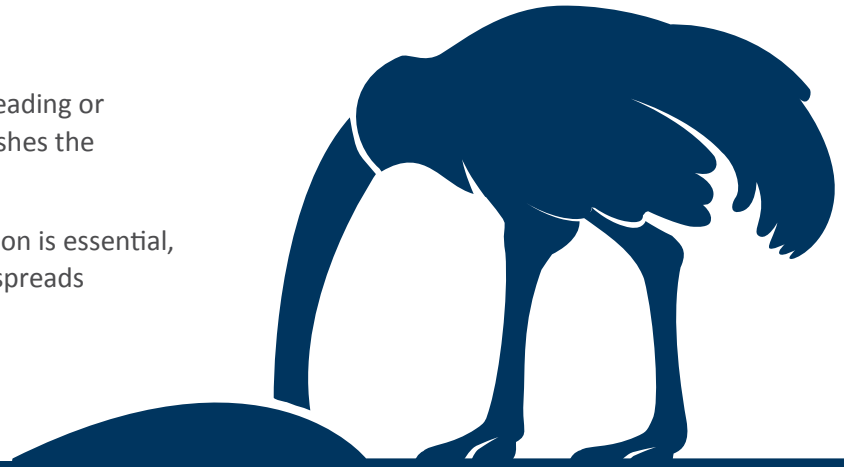
MONITORING

COMPANIES CANNOT AFFORD TO STICK THEIR HEADS IN THE SAND...

WHEN IT COMES TO WHAT IS BEING SAID ABOUT THEM ON SOCIAL MEDIA.

Monitoring to some degree is essential to ensure:

- The **MESSAGING IS ON TRACK**.
- **NO UNHELPFUL COMMENTS** are being made. These could include misleading or defamatory comments, breaches of confidentiality or anything else that tarnishes the company's reputation.
- Any **PROBLEMS ARE ADDRESSED** as quickly as possible. Damage limitation is essential, particularly given the speed at which messages are spread online. Negativity spreads like wildfire in an environment that is open 24/7. Any online content, whether positive or negative, impacts how a business operates and is viewed.



What are Companies Doing?

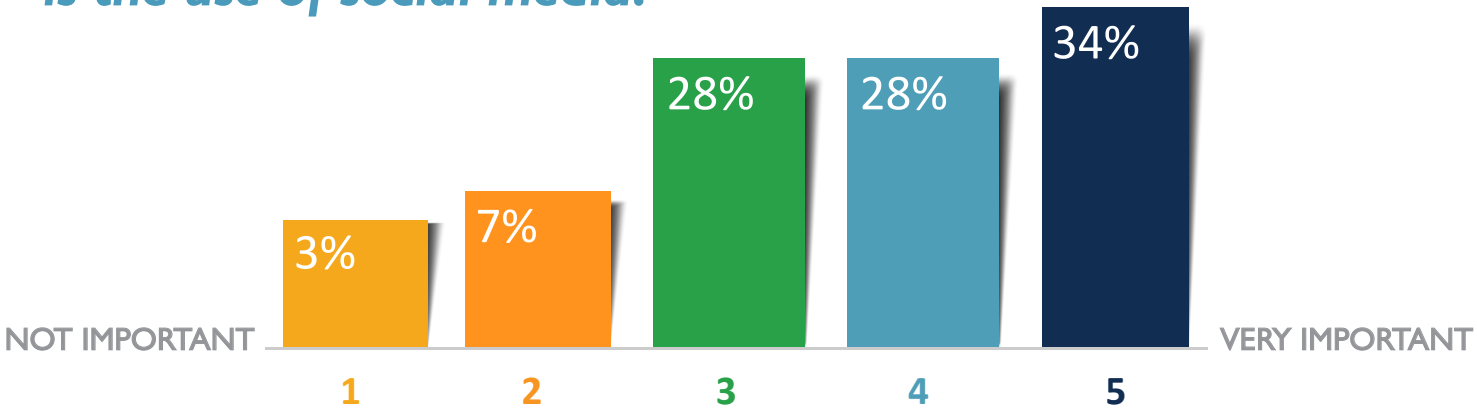
The vast majority of businesses surveyed have a corporate social media account. Twitter was the most popular platform (91 percent), closely followed by Facebook (88 percent). Interestingly, LinkedIn came in at only third place (86 percent) despite being the most corporate-orientated site. Other social media platforms such as YouTube, Google Plus and Instagram were significantly less prevalent (around 40-50 percent).

Unsurprisingly, the use of social media was viewed as fairly important or very important by most businesses.

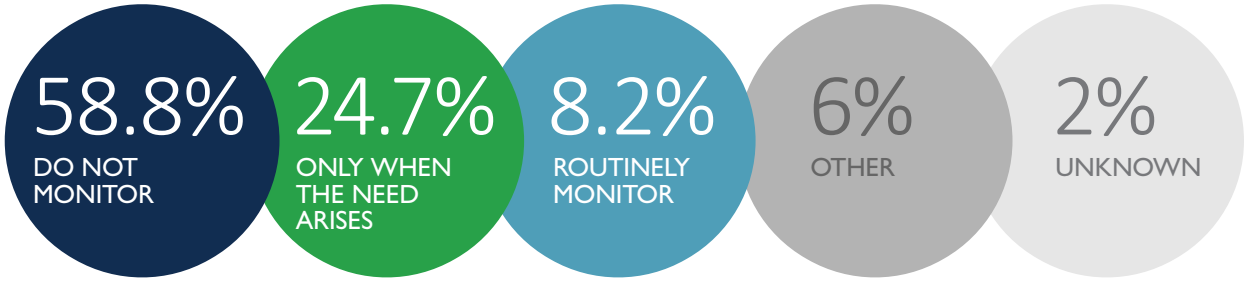
Despite the importance of social media, however...

ONLY HALF OF OUR RESPONDENTS HAD AN AUDIT PROCESS IN PLACE *to ensure that corporate posts are overseen by senior management. This suggests that, while the use of social media has been embraced by companies, corresponding checks and balances have not yet been implemented to ensure the messaging is on track. This is highlighted further by the fact that the majority of companies also do not monitor employee (as opposed to corporate) social media accounts.*

How important to your business is the use of social media?



To what extent do you monitor individual employees' social media activity in the workplace?



A POTENTIAL MINEFIELD

Monitoring of employees' social media is restricted by a range of legislation. This includes the Data Protection Act 1998, the Human Rights Act 1998 and unfair dismissal legislation. While the detail of this legislation is beyond the scope of this note (and of course some of it may change as a result of Brexit), it is worth noting that employees DO have a basic right to privacy at work and there is a duty of trust and confidence which underlies all employment relationships. This will become all the more important with the advancement of wearable technology and the corresponding capacity to monitor and collect employee data more fully. Added to this is the fact that compensation for some claims is uncapped and U.K. employees are often well-informed about their rights. Employers must therefore monitor with caution.

How can you monitor employees?

?

There are two key steps an employer can take to monitor fairly:

1 Have a comprehensive **SOCIAL MEDIA POLICY.**

2 Carry out an **IMPACT ASSESSMENT** before monitoring.

Our survey revealed that just over half of respondents (54 percent) have a social media policy whereas only a third (33 percent) are aware of the need for an impact assessment before monitoring. This again highlights the lag between the increase in use of social media and compliance with best legal practice.

SOCIAL MEDIA POLICY

HAVING AN EFFECTIVE SOCIAL MEDIA POLICY IS ESSENTIAL.

HR policies are all too often overlooked, but a social media policy is increasingly important to let employees know what is and isn't acceptable. Used properly, it can prevent misuse of social media in the first place and allow an employer to react quickly and effectively if a problem does arise.

What should a social media policy include?

- Importantly, it should be **TAILORED TO THE BUSINESS**. Social media policies are not one size fits all. Some companies, for example, actively encourage blogging whereas others discourage all social media except LinkedIn. In an ideal world the policy would also be tailored to different groups of employees, if appropriate. For example, one set of rules might apply to manual workers (who should not be on social media while working), while another might apply to the marketing team (for whom social media may be a large part of their jobs). Our survey showed that 75 percent of social media policies are standardized across all employees, although 17 percent are tailored to particular teams or individuals.

- State whether **PERSONAL USE** of social media is allowed. Companies should take a realistic approach here. Regulators take the view that a blanket ban on communication for personal reasons (although not necessarily social media specifically) is impractical and enforcement may require a disproportionate level of monitoring. Be clear when drafting: the policy should not state that personal use is forbidden if in fact it is accepted during lunchtime breaks.

- State that employees will be **MONITORED**. It should say what monitoring will take place, and why and who will have access to the results of monitoring.

- Remind employees that they must not disclose **CONFIDENTIAL INFORMATION**. Companies should also of course have standalone confidentiality, discrimination, bullying and harassment policies. The policies should state that any breach will result in disciplinary action up to and including summary dismissal.

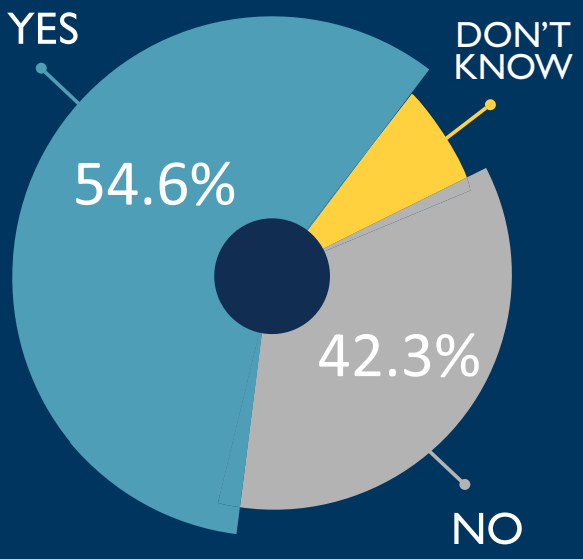
- **BRING IT TO EMPLOYEES' ATTENTION REGULARLY**. It is not enough to have a policy tucked away on the intranet. This is particularly important because social media is a new and evolving area, so employees must be told what is acceptable. Ideally companies should bring the policy to employees' attention at least once a year (and again after any changes) and should ask employees to expressly acknowledge and agree to comply with the policy. Our survey showed that only half of companies bring their policy to employees' attention at least once a year and only one-third require their employees to sign the policy.

- **ENFORCE IT CONSISTENTLY AND FAIRLY**. It will undermine an employer's case if one employee is dismissed for misuse of social media but another is given a verbal warning for the same offence.

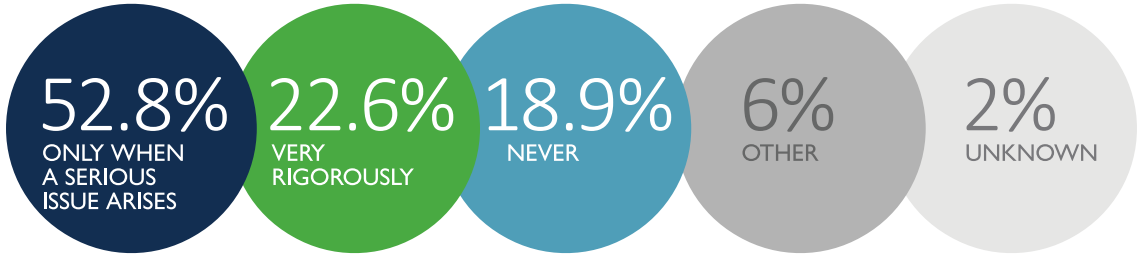
Following the above guidelines will help avoid mishaps (because everyone will know what is and isn't allowed) and will allow any mishaps to be dealt with quickly and easily. It will be significantly more difficult to enforce appropriate use without such a policy.

MONITORING

Do you have a social media policy?



How rigorously is your social media policy enforced? ▶



(Minor breaches tend to be ignored)

How is your social media policy brought to employees' attention?

IMPACT ASSESSMENTS

IMPACT ASSESSMENTS: THE BASICS

What is an impact assessment?

This is a process to decide whether monitoring is justified. It involves weighing the benefits (e.g., uncovering misconduct) against the downsides (e.g., the intrusion into the employee's private life and the impact it may have on employee relations).

When do I need one?

Whenever an employer wishes to monitor employees. The monitoring may be collective (e.g., through automated email checking software for all employees or CCTV) or individual (e.g., reading a specific employee's emails). In practice, an assessment is particularly advisable when the monitoring is intrusive and likely to be contentious.

How do I do it?

Ideally it should be in the form of a written document which considers the following:

- The purpose of the monitoring
- The results it will deliver
- Any adverse impact of the monitoring
- Any alternative, less intrusive ways to monitor
- The obligations which arise from the monitoring
- Whether the monitoring is proportionate and justified, taking the above into account

The assessment does not need to be particularly long or formal. However, the more intrusive the monitoring, the more detailed the report is likely to be, because greater consideration will need to be given to these issues.

What if I don't do an impact assessment?

It is possible that the monitoring (or lack of impact assessment) will go undetected, but employees are increasingly aware of their rights and the courts are increasingly willing to enforce them. The worst case scenario is that the employer is exposed to claims by employees (for example constructive dismissal and discrimination), fines from the data protection authority (currently up to £500,000 for the most serious breaches, but due to increase to a maximum of 4 percent of global turnover under the forthcoming General Data Protection Regulation) and negative publicity.

In summary, impact assessments provide significant protection for an employer and are highly recommended before all monitoring, particularly where the monitoring is intrusive and/or may lead to litigation.

MONITORING

DO WE NEED TO GET EMPLOYEE CONSENT BEFORE MONITORING?

NO.

The basic position is that employers need a legal basis to monitor employees as it involves the processing of their personal data. Simply obtaining employee consent is insufficient as a legal basis as the likelihood of real or potential prejudice arising from the employee not consenting means that consent is, in nearly all cases, not freely given, and therefore not valid.

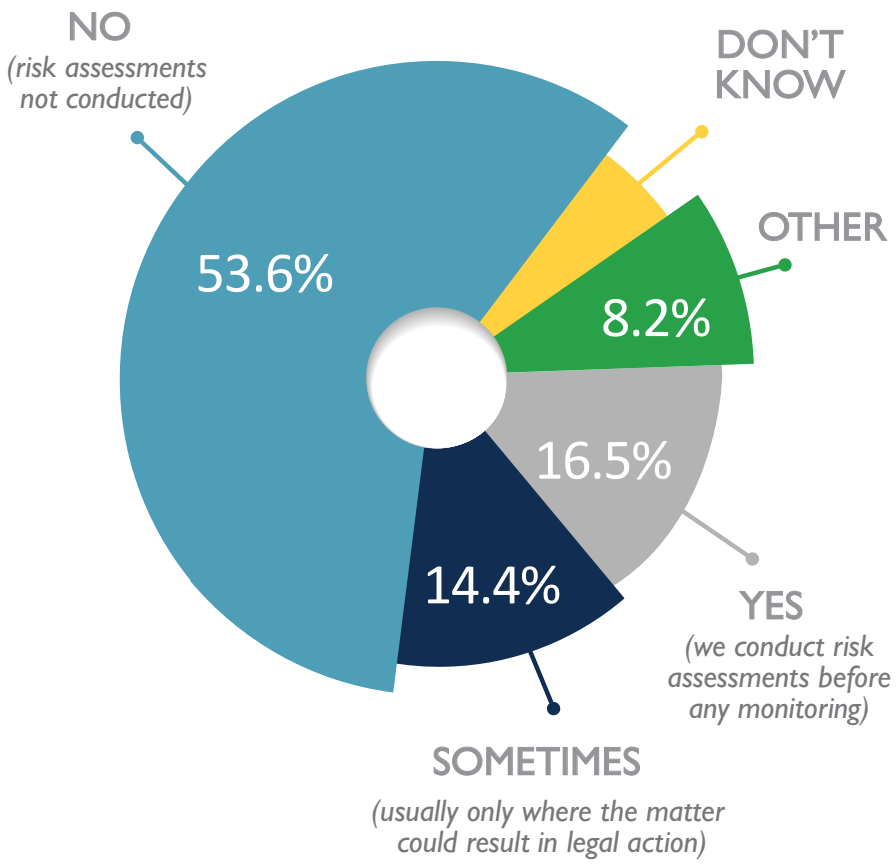
The most relevant legal ground on which to justify the monitoring of employees is on the basis of a **LEGITIMATE INTEREST**. In order to monitor employees on this basis, employers must ensure that the chosen method of monitoring or specific technology used is necessary for the interest pursued. The monitoring must be proportionate to the business need and implemented in the least intrusive manner. The employer should also be able to demonstrate that the employees' rights are adequately protected. This may involve introducing geographical, data-oriented and time-related constraints which limit the scope of any monitoring. An impact assessment, performed correctly, allows an employer to consider these issues in depth and document its analysis and action taken.

Most employers will not want to alert an employee to the fact they are being monitored. Fortunately, employers who can justify covert monitoring on the basis of an impact assessment and the processing of employee personal data on the basis of their legitimate interests, do not generally need the consent of individual workers.

However, employers should ensure that any covert monitoring is only undertaken in exceptional circumstances and is targeted for a specific purpose. Transparency is an important general requirement of data protection law and requires that employees are aware of the existence of any monitoring, its purpose, and any other information needed to guarantee fair processing.

The European position is similarly restrictive. In September 2017, in the case of *Barbulescu v Romania*, the European Court of Human Rights found that a Romanian employer had acted unlawfully when it monitored an employee's Yahoo messenger account without telling the employee.

Do you use risk assessments in practice?



RECRUITMENT

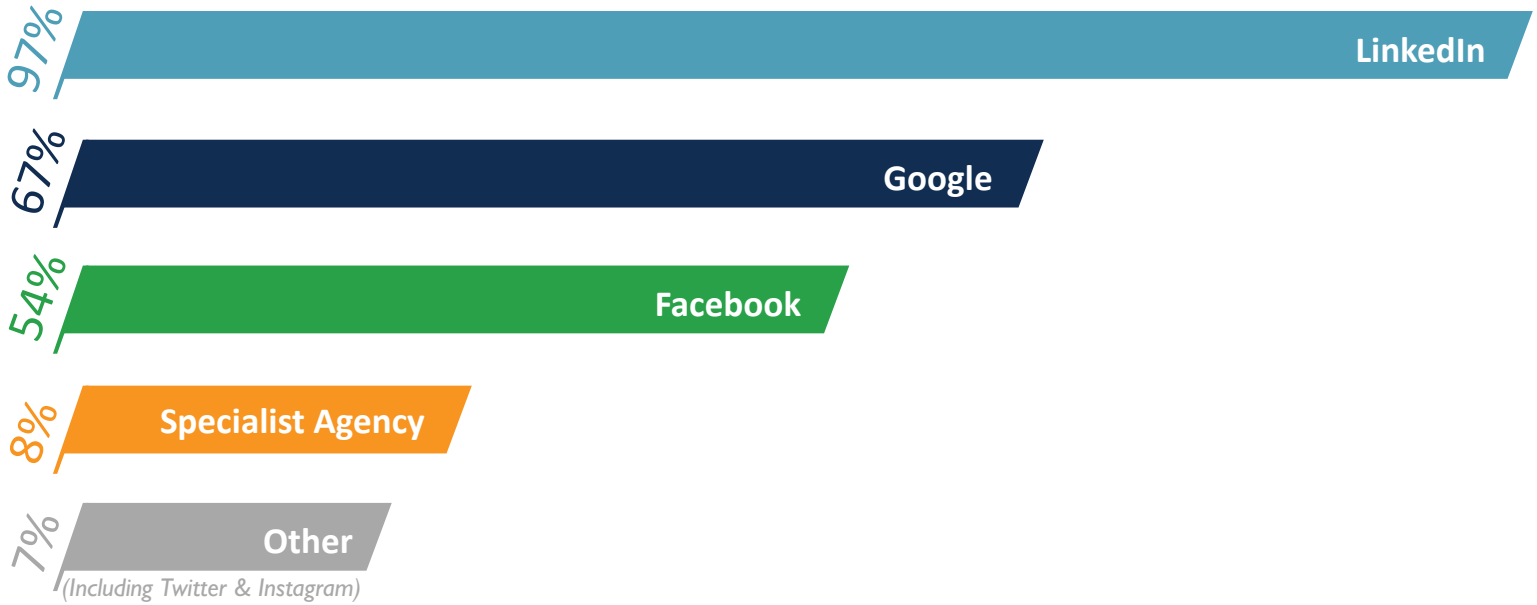
THERE ARE TWO MAIN WAYS *in which social media is used in recruitment. First, it is an effective and cheap way to advertise a role. Many jobs are now publicised on LinkedIn and/or Twitter. Second, social media is used by companies to learn more about applicants.*

JOB ADVERTISING

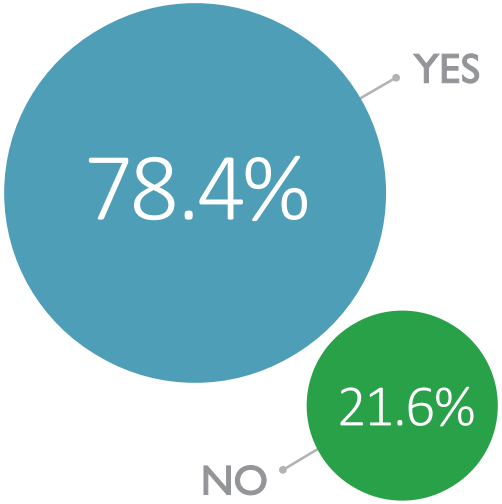
LinkedIn provides a cheap and effective way to advertise a role. The wide audience and ability to target particular groups mean that the quality of candidates is often higher than through traditional forms of recruiting. The vast majority of companies choose to advertise in this way.

Bear in mind however that social media should not be the only way the role is advertised. Limiting the advertising in this way could exclude legally protected individuals — for example older workers who do not use social media — leading to allegations of indirect discrimination. In our experience these claims are rare (perhaps because the protected individuals never know about the job) but are still worth bearing in mind.

Which methods have you used?



Have you or a representative of your organization ever searched online for information about a job applicant?



RESEARCHING CANDIDATES

The natural impulse when trying to find out about someone is to Google them. Companies are no different. Much information is available online, and our survey revealed that three-quarters of respondents search online for information about prospective employees. But is this legal?

There is nothing to stop an employer from searching the internet for publicly available information. However, there are two important points to consider:

1

A company should **AVOID EXCESSIVELY INTRUSIVE SEARCHES**. A company should not assume that merely because an individual's social media profile is publicly available, they are then allowed to process those data for their own purposes. Publicly available information about candidates should only be reviewed if doing so is necessary for the job, and if candidates are correctly informed that this is being done. It would not be appropriate, for example, to dig into an applicant's private Facebook posts by searching through a joint personal contact. Such activity is likely to be difficult to justify under data protection laws and may damage the company's reputation.

2

A company must not use any information (however found) in a **DISCRIMINATORY** way. It would be unlawful, for example, to reject an applicant because they appear to be too young, too old or pregnant on their Facebook profile photo. Of course, most employers would give a different reason, but if the candidate were to make a data subject access request which resulted in the production of an incriminating email, this could make life difficult for the employer in any subsequent claim.

DO WE NEED TO TELL OUR APPLICANTS?

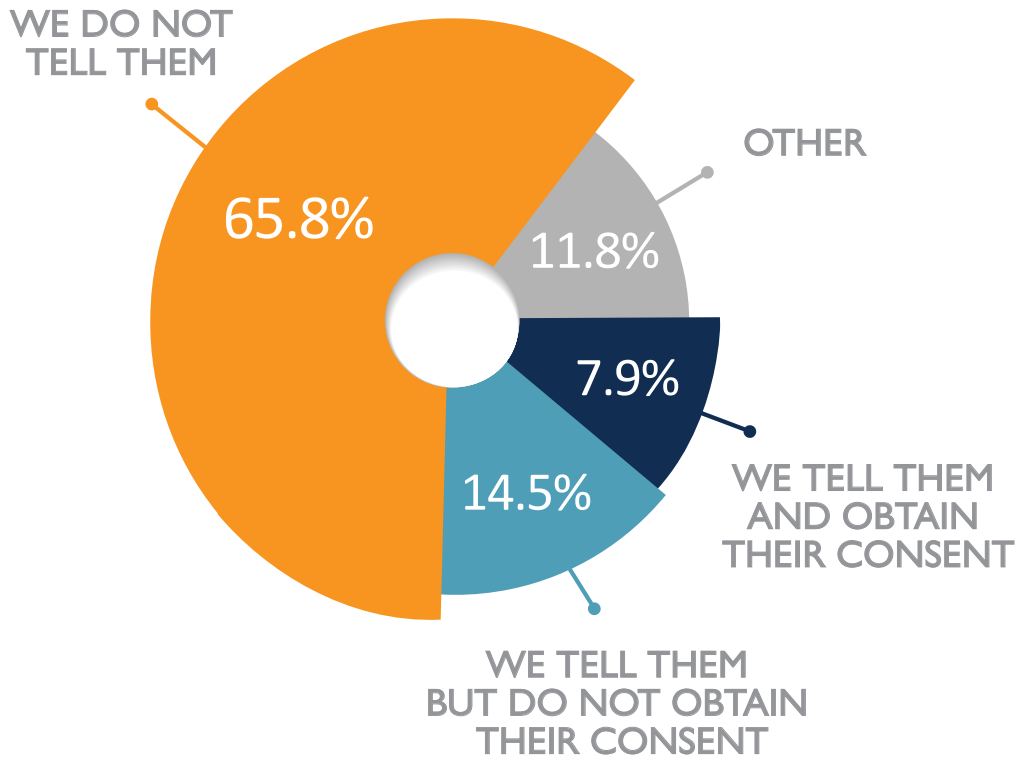
Ideally, yes.

It is good practice to tell applicants you will search publicly available information and the data protection authority recommends this. In practice however, it seems that few employers actually do so.

In our survey, **TWO-THIRDS** of companies who search online do **NOT TELL** the applicants they are doing so. Perhaps this is because notifying applicants in this way opens the door to allegations by rejected applicants that the reasons for rejecting them were unlawful.

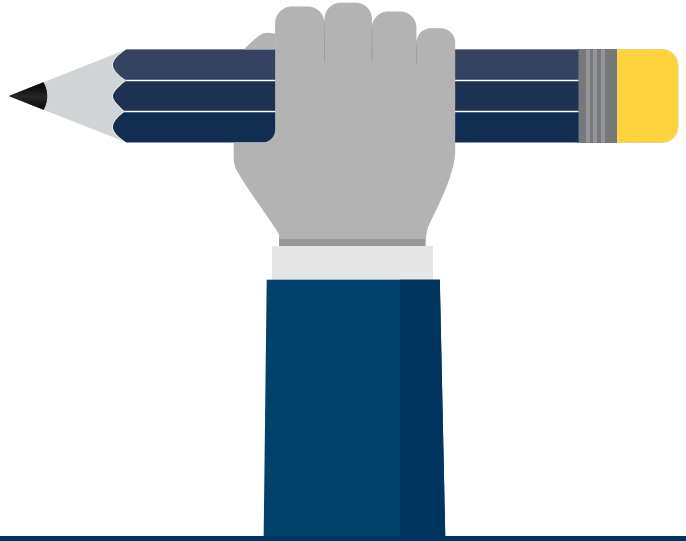
A written record of the real reasons for rejection will help rebut any such allegations.

To what extent do you tell job applicants about this?



BEST PRACTICE ADVICE

FOR MANAGING YOUR RISK AND COMPLYING WITH LAWS AND REGULATIONS WHEN ADVERTISING JOBS



INCLUDING

1 ADVERTISE WIDELY
Use hard copy adverts and recruitment consultants as well as online media.

2 AVOID DISCRIMINATION
Avoid discrimination in the job specification. Of course this means you cannot use protected criteria such as sex or age to limit applicants.

3 KEEP RECORDS
Keep a clear written record of reasons for rejecting applicants. These should be objective and non-discriminatory.

4 NOTIFY APPLICANTS
Notify applicants that you will search publicly available information (see above).

More on Avoiding Discrimination...

Less obviously, however, avoid criteria which may be *indirectly* discriminatory, such as (i) requiring a minimum number of years' experience (which may indirectly discriminate against younger applicants) or (ii) requiring applicants to be "physically fit" (which may discriminate against disabled applicants) — the better approach would be to explain the physical requirements, for example lifting boxes, so the candidate can assess whether they meet the criteria.

SOCIAL MEDIA TURNS ANTISOCIAL

SOME MISHAPS MAKE THE NATIONAL PRESS

When **HMV** made some employees redundant it found that one disgruntled employee had accessed the corporate Twitter account and told all followers about the “mass execution of loyal employees who love the brand”. Unfortunately, no one in senior management knew the Twitter password so they were unable to stop it.

US AIRWAYS replied to a customer tweet but accidentally included a link to a pornographic image. The company explained that it had meant to flag the photo as inappropriate, not tweet it, but that it was somehow “inadvertently included in a response to a customer”.

SAINSBURY’S recently launched a “50 pence challenge” which encouraged staff to upsell to customers. Unfortunately one of the posters explaining the challenge was displayed in a shop window by mistake and within hours was shared on social media, leading to a huge backlash. Apart from bad publicity, Sainsbury’s competitors benefitted — Lidl launched its own 50 pence challenge which encouraged staff to help customers “save as many 50ps as possible”.

Although social media can help a business grow, it can also cause a management headache.

WHAT WORRIES EMPLOYERS THE MOST?

OUR SURVEY SHOWS THAT EMPLOYERS **WORRY** MOST ABOUT THE FOLLOWING *(with the most important first):*

Damage to the company's reputation

This can be caused by any number of factors, including disgruntled employees bad-mouthing their employers' treatment of staff or customers.

Breach of confidentiality

This may not necessarily be malicious; a member of Parliament breached patient confidentiality when he tweeted a picture of himself visiting a hospital but failed to spot a noticeboard in the background showing patient names.

Loss of productivity

People are increasingly glued to their phones; a recent study showed that the average young person checks their phone 85 times a day and spends five hours a day browsing the internet and using apps[1]. Inevitably this will have an impact on productivity at work.

Damage to employee relations

This can happen in a number of ways, including online bullying, harassment and defamation.

Other concerns

These included false reviews, abuse such as use of pornography, not using social media enough, loss of control of the company's persona and not handling bad reviews correctly.

Comments made on social media by "external" posters are outside the scope of this report. There are, however, ways in which businesses can challenge online content and mitigate the risk of damage. Our survey showed that 16 percent of respondents had taken action against an external poster, and this figure is only likely to rise.

[1] *http://www4.ntu.ac.uk/apps/news/180892-15/People_check_their_smartphones_85_times_a_day_(and_they_dont_even_know_the.aspx*

What steps can an employer take to PREVENT employee mishaps?

?

As noted above, the best protection is to have a robust **social media policy**. Bear in mind that a policy is no good unless it has been tailored to the business and employees know about it.

What steps can an employer take AFTER the event?

As you might expect, this depends on the severity of the misconduct. Sanctions range from a verbal warning to dismissal for gross misconduct.

One important point is that there are no specific new employment laws relating to misconduct in the context of social media. All misconduct cases are dealt with according to existing laws.

The test — as confirmed by the judge in a Twitter-related case — is...

*"whether the employer's decision and the process in reaching that decision fell within the **range of reasonable responses open to the reasonable employer on the facts of the particular case**. That test is sufficiently flexible to permit of its application in contexts that cannot have been envisaged when it was laid down. The questions that arise will always be fact-sensitive and that is true in social-media cases as much as others. For us to lay down a list of criteria by way of guidance runs the risk of encouraging a tick-box mentality that is inappropriate in unfair dismissal cases.[2]"*

[2] *Game Retail Ltd v Laws UKEAT/0188/14/DA*

PRACTICAL GUIDANCE ON DEALING WITH MISCONDUCT

The following is a brief summary of the key steps to take when dealing with misconduct. Bear in mind that the process can sometimes be shortened (for example, if the employee doesn't have the required length of service to claim unfair dismissal), but the same general principles will apply.

Act quickly.

Damage limitation is crucial given the speed at which comments are spread online. This often means removing the offending comment or asking the employee to do so, although screenshots should be taken to avoid losing evidence.

Investigate.

This is important; a dismissal can easily be found to be unfair if the company hasn't investigated the misconduct properly. Legally, the employer must (a) have *reasonable grounds for believing the employee is guilty* of the misconduct and (b) at the time it holds such belief, have carried out *as much investigation as is reasonable*. In practice, this means that the more serious/complex the misconduct, the more thorough the investigation should be. Usually an investigation will involve speaking to all relevant witnesses. Ideally it should also be conducted by someone who won't be involved in any subsequent disciplinary process.

Prepare an investigation report.

Although not legally required, a written report by the investigating officer will show that proper consideration has been given to the issue and will help the employer defend any subsequent claim.

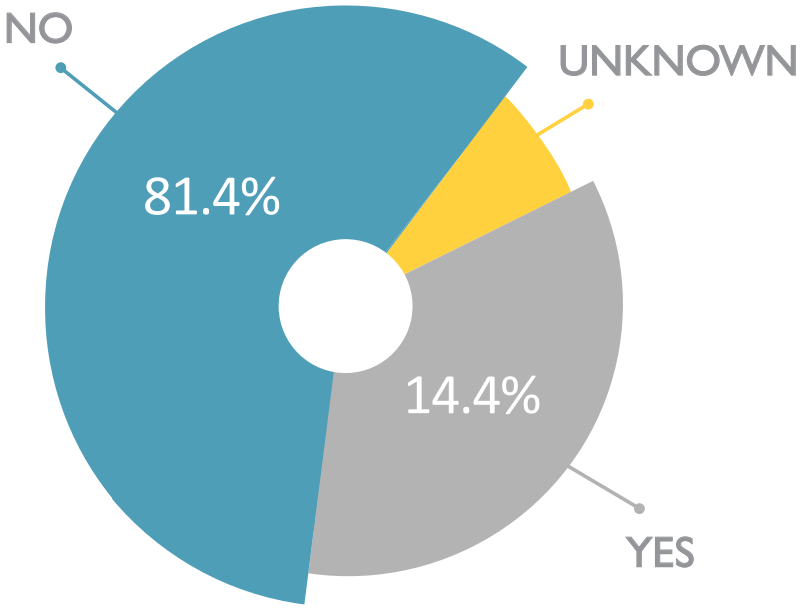
Conduct a disciplinary process.

The employer will need to comply with the ACAS Code of Practice on Disciplinary Procedures as well as with any internal disciplinary policy. This would involve inviting the employee in writing to a disciplinary hearing, conducting the disciplinary hearing at which the employee has the right to be accompanied, informing the employee of the decision in writing, and giving the employee a right of appeal. When deciding on the appropriate disciplinary sanction the general principles below should be borne in mind.

Comply with contractual obligations.

Throughout the whole process, the company must comply with all contractual obligations; this includes the employment contract (for example giving the correct notice period if the employee is dismissed) and any other documents such as contractual social media or disciplinary policies.

Have you ever taken disciplinary action based on an employee's social media activity?



FACTORS TO CONSIDER BEFORE DECIDING WHAT DISCIPLINARY ACTION TO TAKE

When an employer is deciding what disciplinary action to take, it should consider the factors below. This is particularly important where the employee has unfair dismissal rights.

The **ACTUAL IMPACT** (rather than perceived or feared impact) of the misconduct. When an employee posted on Facebook "*I think I work in a nursery and I do not mean working with plants*" she was dismissed for damaging her employer's reputation. The dismissal was held to be unfair; her comments were relatively mild and there was no evidence that the employer's reputation had in fact been damaged[3]. Similarly, when a manager was dismissed for posting a video on YouTube of two colleagues in a storeroom hitting each other with plastic bags, the dismissal was held to be unfair; the video only had eight hits on YouTube (some of which were part of the disciplinary process), so the employer could not reasonably say that its reputation had been damaged[4]. ▶

[3] *Whitham v Club 24 Ltd (t/a Ventura) ET/1810462/10*
[4] *Taylor v Somerfield Stores Ltd ETS/107487/07*

How **APOLOGETIC** and **CONTRITE** the employee is. When an employee removed an offensive Facebook page as soon as he realised it breached the company's social media policy and apologised for his actions in his disciplinary hearing, his subsequent dismissal was found to be unfair[5].

The employee's **AWARENESS OF THE SOCIAL MEDIA POLICY** and whether it has been **BROUGHT TO THEIR ATTENTION**.

How **CLEAR** the social media policy is. When two sisters were dismissed for excessive use of social media, their dismissal was found to be unfair because the company's IT policy was unclear; it permitted access to the internet "outside core working hours", but it was unclear what "core working hours" meant[6].

Whether all employees are treated **CONSISTENTLY**. A tribunal will take a dim view of an employer that treats two employees differently for the same misconduct. However, the standard of conduct may be higher for certain types of employees; for example, a school-worker who mentored vulnerable pupils sent sexually explicit images and photos from a work computer, and her dismissal for gross misconduct was found to be fair even though the social media policy did not expressly state that her conduct constituted gross misconduct[7].

Whether the employee had **LIMITED** their audience, for example by amending their privacy settings. When a pub manager posted derogatory comments about two abusive customers on Facebook she thought her settings were private, but her comments could in fact be viewed much more widely, including by family members of the customers in question. Her dismissal was held to be fair[8].

PREVIOUS CONDUCT. An unblemished disciplinary record will usually count as a mitigating factor, particularly where the misconduct is relatively minor. Where an employee had over 10 years' service with an unblemished disciplinary record and no previous warnings, his dismissal for gross misconduct was found to be unfair[9].

Whether the disciplinary action is **PROPORTIONATE**. It was not reasonable to dismiss an employee who "liked" a Facebook comment about her manager being "*as much use as a chocolate teapot*" and added a comment that it had been her worst year in the company. In contrast, it was reasonable to dismiss an employee for gross misconduct after he made vulgar comments about the sexual promiscuity of a colleague, then refused to remove them and instead posted further comments[11].

[5]Stephens v Halfords plc ET/1700796/10
[6]Grant and Ross v Mitie Property Services UK Limited (2009, unreported)
[7]Henderson v London Borough of Hackney [2011] EWCA Civ 1518
[8]Preece v JD Wetherspoons plc ET/2104806/10
[9]Walters v Asda Stores Ltd ET/231748/08
[10]Young v Argos Ltd, ET/1200382/11
[11]Teggart v TeleTech UK Ltd NIIT 00704/11

Results

Our survey revealed that relatively few employers (14 percent of respondents) have taken disciplinary action based on an employee's social media activity. Of those who have, the most common issue was time wasting, followed by damage to the company's reputation and then disclosure of confidential information. As a law firm, however, we are seeing increasing incidents of misconduct around social media, particularly among larger companies and/or where social media is used widely in the business.

DOES IT MAKE ANY DIFFERENCE WHETHER THE COMMENTS ARE MADE ON THE EMPLOYEE'S OWN TIME OR USING THEIR OWN EQUIPMENT, OR ON PRIVATE SOCIAL MEDIA ACCOUNTS?

NOT NECESSARILY.

This question often crops up in the context of social media. The lines are increasingly blurred between home and private life, with employees having internet access 24/7, and the same mobile phones, tablets and laptops being used for both work and personal matters.

The courts seem to be taking a sensible approach. Key considerations include whether the misconduct is **CONNECTED TO WORK** (for example, because the employer is named or the post is clearly about work), how **PUBLIC** the offending comment is (for example whether the employee's privacy settings allow others to view posts) and the **IMPACT ON THE EMPLOYER** in practice.

Employees often claim their employer has breached their right to privacy or to freedom of expression under the Human Rights Act 1998 (HRA). While this has some relevance (the courts currently must take the HRA into account when interpreting employment legislation) it certainly does not give employees an unfettered right to say what they like.

Who Owns LinkedIn Contacts?

This is an increasingly important issue for employers. Often a company will encourage its employees to use LinkedIn to build their network, but those connections can work against the employer when the employee leaves. Can you force an employee to delete their contacts? Or prevent them from updating their place of work when they leave?

The case law in this area is still developing. It seems that courts will step in, but so far only in extreme cases, for example where an employee has actively made connections just before leaving, or where a company LinkedIn account was used to assist a competing business.

The Court Steps In...

1

MAKING CONNECTIONS WITH A VIEW TO COMPETING: A recruitment consultant sent LinkedIn invitations to a number of clients just before he left to set up a competing business. The court took the view that the contact details obtained during employment remained the property of his employer, and accordingly ordered the employee to disclose further details of his conduct[12].

2

USING A COMPANY LINKEDIN GROUP: Three employees left Whitmar to set up a competing business. One of them had previously managed four LinkedIn groups for Whitmar but refused to give Whitmar the usernames or passwords. The court concluded that the LinkedIn accounts had been operated for Whitmar's benefit and ordered the employees to hand over the login details[13].

3

CONTACT LISTS ON AN EMPLOYER'S SYSTEM: A journalist kept all his contacts on his employer's computer system. He took the contact list when he set up a competing business, arguing that he owned the list because it contained personal contacts and contacts which pre-dated his employment. The High Court disagreed; it said that a database which is kept on the employer's computer system and backed up by the employer belongs to the employer[14].

▼

But what about the more common situation where an employee's own contacts are intermingled with work contacts and built up over several years? Can an employer force an employee to delete work-related contacts? Or stop them from notifying their contacts about a new job? There are very few reported cases on these specific points, perhaps suggesting that employers are taking a more relaxed approach. This is backed up by our survey. Importantly, there are some fundamental practical difficulties in policing LinkedIn activity.

[12] *Hays Specialist Recruitment v Ions [2008] EWHC 745*
[13] *Whitmar Publications Ltd v Gamage [2013] EWHC 1881 (Ch)*
[14] *PennWell Publishing (UK) Ltd v Ornstein and others [2007] EWHC 1570 (QB)*

CHALLENGES IN RETAINING EMPLOYEES' CONTACTS

Often an employee's contacts are a mixture of connections from their current employment, previous employment, education, family, social connections and friendships. It can be difficult to pinpoint which of the contacts are sufficiently linked to the current employment to be protectable. There is also the question of who would be responsible for working through the contacts and deciding which should be deleted.

Even if it were possible to identify the work-related contacts and require the employee to delete those contacts, it would be relatively easy for the employee to re-establish the contacts once they have left and/or copy the contact details into a different format.

Legal protection is given to "databases" (under the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032)) but only where there has been a "*substantial investment in obtaining, verifying or presenting the contents of the database*". Given that many LinkedIn connections are automatically suggested by LinkedIn or instigated by other LinkedIn users, it is questionable whether a "substantial investment" has been made.

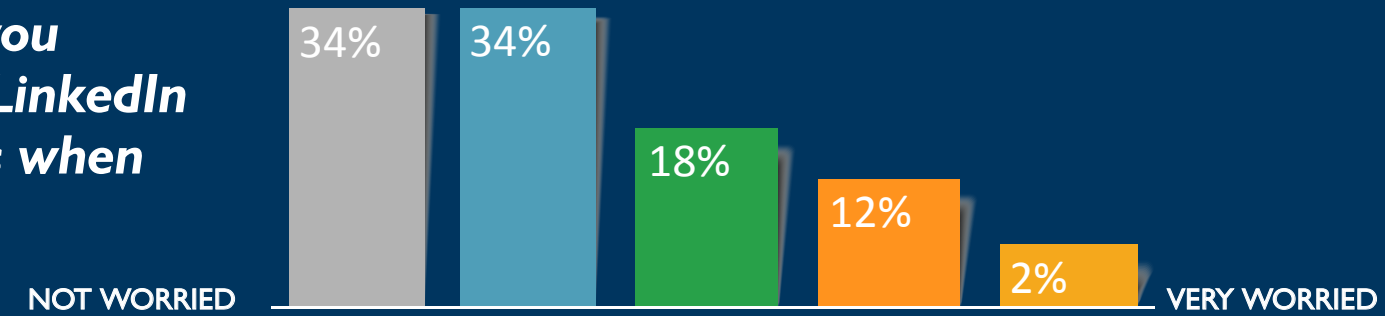
The LinkedIn terms and conditions state: "*as between you and LinkedIn, you own the content and information that you submit or post to the Services*". They also require users to keep their password "secure and confidential" and "not to transfer any part of [their] account". This arguably makes it more difficult for the employer to control an employee's personal account.

From a general fairness perspective, many companies are taking the view that all employers are in the same position so there is little point trying to clamp down. Every employer gets the benefit of its employees' prior connections when they join, so it seems unfair to punish the employees when they leave.

Litigation is time consuming and expensive. As always, employers should weigh up the benefits and downsides before launching into legal action, particularly where the outcome is uncertain.

Interestingly, our survey showed that relatively few respondents are concerned about protecting LinkedIn and other contacts when an employee leaves. Two-thirds said they are not worried or are only slightly worried.

How worried are you about employees' LinkedIn and other contacts when they leave?



DESPITE THE PRACTICAL ISSUES MENTIONED...

THERE ARE A FEW RELATIVELY STRAIGHTFORWARD STEPS THAT EMPLOYERS CAN TAKE TO PROTECT THEIR BUSINESS:

CONFIDENTIALITY: Strengthen the confidentiality clauses in the employees' employment contracts. They should state that all customer, client and contact lists — however and wherever created — belong to the employer and must be deleted or returned to the employer when the employee leaves.

RESTRICTIVE COVENANTS: Covenants are some of the best ways to protect the business after an employee leaves. Typically they prevent the employee from competing, soliciting other employees and/or soliciting clients and customers for a limited period. Additional protection is possible with "non-deal" covenants, where there is no need to show that solicitation has taken place. As always, of course, covenants must be carefully and narrowly drafted to be enforceable.

GARDEN LEAVE: Putting an employee on garden leave during their notice period (where they stay away from the office and clients but remain employed) is a relatively easy way to protect valuable information and contacts. The garden leave clause should give the company maximum flexibility in terms of what the employee can be required to do (and not do) during their garden leave period. Generally speaking, an employee should only be put on garden leave for up to six months, and post-termination covenants should be reduced by any time spent on garden leave.

SOCIAL MEDIA OBLIGATIONS: In addition to the standard protections above, it may be worth including specific social media protections in employment contracts and in any social media policies. These could include:

- A requirement to provide login details for any company LinkedIn accounts.
- An obligation on termination to delete any LinkedIn contacts created during employment and a commitment not to reinstate them for a certain period afterward.
- A restriction on alerting contacts to a new job, for example by ensuring that LinkedIn settings are adjusted so that no automatic email is circulated when they update their place of work.

Importantly however, given the current uncertainty about whether these obligations would be enforceable, they should be kept separate from the other terms of the contract so that they can be 'blue pencilled' (i.e., deleted) by a court if they are deemed unenforceable.

Only 30 percent of the respondents we surveyed have protections in place to deal with social media risks when employees leave. The most common form is restrictive covenants, but a small minority have specific requirements including: (i) an obligation to copy the employees' contacts into the company database; and (ii) a requirement to delete LinkedIn contacts made during employment.

A PRACTICAL APPROACH

Many of our respondents took a pragmatic view of LinkedIn, accepting that a company shouldn't seek to control an employee's network when they leave.
Some quotes include:

Given the practical difficulties of policing LinkedIn accounts and the bad feeling that would be generated if companies clamped down heavily, it seems unlikely to us that much will change in the short term. Employers should however still rely on the traditional methods of protecting their business by ensuring their employment contracts include well drafted confidentiality, non-solicitation, non-deal and garden leave clauses.

CONCLUSION

IN SUMMARY

Social media shows no sign of diminishing in importance, and the majority of business leaders we surveyed feel it's important. Social media offers many advantages to businesses, particularly for marketing and recruiting, but corporate leaders should proceed with caution, as it also presents numerous pitfalls, including the potential for negative reflections on the company's public image.

Unwise social media use can lead to disputes with current and potential employees. Companies would be wise to monitor corporate posts but should be cautious about monitoring employees' social media use. Similarly, social media is a valuable tool for researching job candidates, if done wisely and legally, and the majority of businesses who participated in our survey do so. When and how to take disciplinary action over an employee's inappropriate social media use is a challenging decision for employers, and most of our respondents have not taken such action.

Both employers and the law are struggling to keep up with recent changes in technology and social media. A solid social media policy and plan of action can help employers manage risk in these changing times. In our survey, just over half of respondents had a social media policy in place. This is an action all businesses can take to help protect themselves.

PARTICIPANTS

CallWell
Pandrol UK
4net technologies
Amillan
Together
The Belfry
Jobhop
Kingston Noble
HCB Accountants
Spartan Global Servicea
John Street
SteadyGo Digital
Dobell
Brighter Directions
SimkissGuy Recruitment Ltd
Exposure Ninja
Glassworks Hounsell
Koru Kids
British Business Energy
Faber Design & Architecture
Aardvark Marketing Consultants Ltd
Ginger Energy
XKeys Ltd
GrowBeyond Ltd
HTFT Partnership
Wundr Media
Millennium Point
The Wedding Secret Ltd.
Stargazer
David Hore
Reuben Sinclair
Rigs Fitness
Shoreditch
Packt
Weave Marketing
Stuart Mosley
Buckt
VOX Digital
ICON
Hopper HQ
MakeMeASuccess
ShotBox Ltd T/A Aimee Spinks
Wilde Thing PR & Events
Barnetson & Co
Real Point
Kixo IT Solutions
PHd design
Blackberry Design
Print This Print That Ltd t/a GARMENT PRINTING
Sport Birmingham
Flourish Education
Innovation Birmingham
Hunnington
Taylor & Hart
Eurostar
Distraction Box
Inferno Media
Curious Kat's Adventure Club
Node
CrowdControlHQ
Dobell Menswear
People HR
Presence Marketing
CareToShare
Zikodrive Motor Controllers
Jerm Pro Cleaners London
Kendlebell
Rise Art
Origym
Sky
Marketing Flare Ltd
Jaguar Land Rover

ABOUT JC SOCIAL MEDIA

JC Social Media is a specialist social media agency based in Birmingham, U.K. The agency provides social media management, training and consultancy to clients all over the world, predominantly in health care, education, professional services and hospitality. Members of the team regularly appear on television and radio contributing to social media thought-leadership on topical issues.

ABOUT FAEGRE BAKER DANIELS

Faegre Baker Daniels is dedicated to serving the legal needs of regional, national and international businesses. With more than 750 legal and consulting professionals in the United States, United Kingdom and China, FaegreBD is one of the 75 largest law firms headquartered in the U.S. We collaborate with clients to solve the most complex transactions, regulatory matters and litigation that businesses face. We partner with clients ranging from emerging startups to multinational corporations in more than 85 practice areas and industry segments, providing advice uniquely suited to each company's needs. Our practices are complemented by experience across a wide range of industries, with a strategic focus on energy and natural resources, financial services, food and agriculture, and life sciences. Based in Washington, D.C., Faegre Baker Daniels Consulting is our national advisory and advocacy division that integrates public policy and regulatory capabilities with the rest of the firm's legal services.

KEY CONTACTS

HUW BEVERLEY-SMITH
Partner, London
T: +44 (0) 20 7450 4551
huw.beverley-smith@FaegreBD.com

ALEX DENNY
Partner, London
T: +44 (0) 20 7450 4568
alex.denny@FaegreBD.com

FAEGRE BAKER DANIELS