Ownership and use of social media by employees in the UK

Kathryn Dooks and Elizabeth Kirk
Kemp Little LLP

Social networks have revolutionised the way many businesses operate, both internally and externally, and Generation Y increasingly expects work processes to use a Web 2.0/social media format. In turn, this means the transition of workplace conversations into an online environment, the ability to access work data from a variety of platforms and locations at any time of day or night, a blurring of the divisions between work and home and difficulty for employers in controlling the release of information (including confidential information, such as client lists).

So how can UK employers:
- Manage employees’ use of social media (where use is excessive, inappropriate and/or leads to loss of productivity)?
- Protect themselves against liability for employees’ actions on social media sites?
- Monitor employees’ use of social networks without infringing their privacy?
- Protect themselves on the departure of an employee?

This article will examine each of these points in turn.

MANAGING EMPLOYEES’ USE OF SOCIAL MEDIA SITES

Employees’ use of social media sites may be inappropriate if, for example, their use of these sites during working hours is excessive and affecting productivity, or because the content uploaded is inappropriate. Employers are able to discipline (or even dismiss) employees in these circumstances, but the following themes which emerge from the English employment tribunal case law should be taken into account.

Employer’s social media policy

The employer’s social media policy must be clearly worded if the employer wishes to be able to rely on a breach of it in order to discipline or dismiss an employee. In the case of Grant and Ross v Mitie Property Services UK Limited (2009, unreported), two sisters were dismissed for excessive use of social media sites including Facebook. The employer’s IT policy permitted employees to access the internet "outside core working hours". The employment tribunal held that the dismissals were unfair because the policy was unclear about what "core working hours" meant.

In Preece v Wetherspoons (2010, unreported), following an incident at work in which two customers were abusive to a pub manager, the pub manager made comments about the customers on Facebook whilst at work. The employee thought her privacy settings meant that her posts could only be viewed by her friends but they could in fact be viewed much more widely, including by family members of the customers in question. Wetherspoons had a clearly worded IT policy which reserved the right to take disciplinary action should the contents of any Facebook page "be found to lower the reputation of the organisation, staff or customers and/or contravene the company’s equal opportunity policy". The employee’s dismissal was found to be fair in these circumstances.

Proportionality

If the employer is relying on damage to reputation as a result of the action on social media in order to discipline an employee, the disciplinary action taken must be proportionate to the damage caused.

Employers should carefully consider the severity of the comments made on social media when deciding whether to dismiss. In Whitham v Club 24 Ltd t/a Ventura (2010, unreported) Mrs Whitham posted on Facebook “I think I work in a nursery and I do not mean working with plants”. Immediately afterwards, she wrote: "Don’t worry, takes a lot for the bastards to grind me down” and a series of similar comments. Mrs Whitham was dismissed as the employer felt that the comments could have a detrimental effect on the relationship between the employer and one of its main clients. The Tribunal found that the dismissal was unfair as the comments were relatively mild, there was no evidence of any damage to the relationship with the client (which the employer had failed to investigate properly) and therefore the sanction of dismissal fell outside the band of reasonable responses which a reasonable employer would take.

Likewise, in Taylor v Somerfield Stores (2007 EAT, unreported), a manager posted a video on YouTube of two colleagues hitting each other with plastic bags in an anonymous storeroom. The video was taken down by the manager after three days. The employee was dismissed as the employer found that the video brought Somerfield into disrepute. However, the employment appeal tribunal held that the dismissal was unfair, as the video had only had eight “hits” on YouTube, most of which were as a result of the disciplinary investigation and the disciplinary panel viewing the video. The employer could not reasonably say that it had been brought into disrepute by the video and therefore the dismissal was not within the band of reasonable responses which a reasonable employer would have taken in such circumstances.


Increasingly claimants try to rely on a breach of the Human Rights Act 1998/ the European Convention on Human Rights (ECHR) in addition to claiming unfair dismissal, especially if they have been dismissed for using social media sites outside of working hours.

Employees often try to claim that the employer’s reliance on their activities on social media is either:
- A breach of the employee’s right to privacy under Article 8 ECHR.
- A breach of their right to freedom of expression under Article 10 ECHR.

Whilst, generally speaking, these cases will only be of direct relevance to public sector employers (as employees can only bring
a claim for a breach of the ECHR directly against a public sector employer), private sector employers should still have regard to their principles, as the English courts and tribunals are required as far as possible to interpret all legislation, whenever enacted, in a way that is compatible with the ECHR.

Right of privacy under Article 8. In Teggart v TeleTech UK Limited (NIIT 0704/11) Mr Teggart was dismissed for harassment after he posted an obscene comment about the promiscuity of a female colleague on his Facebook page while at home. The comment mentioned his employer and was read by his Facebook friends, which included some work colleagues. Mr Teggart claimed unfair dismissal and a breach of his right to privacy. The Northern Ireland Employment Tribunal found that when Mr Teggart put his comments on his Facebook page he had abandoned any right to consider his comments as being “private” (for the purposes of Article 8). Although an individual’s Facebook page is open to “friends”, it is not private, as comments can be copied and passed on to others.

In Gosden v Lifeline Projects Limited (unreported, 2009) Mr Gosden sent an e-mail containing racist comments from his personal e-mail account to the personal e-mail account of a colleague, outside of work hours. The employee had no control over where the e-mail ended up as he urged the recipient to “pass it on”. In these circumstances, the Tribunal found that there could be no expectation of privacy and that the dismissal was fair.

Right to freedom of expression. In Crisp v Apple Retail UK Limited (unreported, 2011) Mr Crisp was dismissed for posting derogatory comments on Facebook about Apple Inc. The employee argued that these posts were private as they could only be viewed by his friends and he had a right to freedom of expression under the ECHR. The Tribunal found that the dismissal was fair. It was critical to the Tribunal's decision that Apple had made clear in its policies and training materials that protecting its image was a “core value” and had drawn attention to the fact that making derogatory comments on social media was likely to constitute gross misconduct. In this case the Tribunal found that although the right to freedom of expression was engaged, the employer's action in dismissing Mr Crisp was proportionate to the harm caused by the posts. The court reiterated that there should always be a balancing act when relying on reputational issues.

PROTECTING EMPLOYERS AGAINST LIABILITY FOR EMPLOYEES’ ACTIONS ON SOCIAL MEDIA SITES

It is established law in the UK that an employer can be vicariously liable for discriminatory acts carried out by their employees. In particular, this principle is set out in the Equality Act 2010 which provides that an act done by a person “in the course of their employment” is treated as also having been done by their employer unless the employer can show that they took reasonable steps to prevent the action. Case law makes clear that the phrase “in the course of employment” is construed broadly and can include acts which took place outside the workplace (for example, at after work drinks) or on social media sites.

The greatest risk lies if the posts occurred during work time, but vicarious liability can also arise from postings outside working hours if the only reason that the two people have a connection is because they work together.

There is also the risk that employees will use social media sites to post negative or damaging comments or air grievances about their employers online or to leak confidential information. According to a survey by the recruitment agency MyJobGroup.co.uk, 40% of UK employees admit criticising their employers on social networking sites like Facebook and Twitter.

Managing the risks

Employers can manage these risks and attempt to limit their vicarious liability to some extent by having appropriate policies and procedures in place regarding acceptable usage, reinforced by appropriate training. Amongst other things, these policies should:

- Specify to what extent employees can access such sites, and where, including business and personal use.
- Make clear that employees should not disparage customers, suppliers, employees, and so on, on such sites.
- Make clear that employees should not disclose confidential information or trade secrets.
- Clarify the consequences of any breach.
- Confirm that the employer reserves the right to monitor employees’ use of e-mail and Internet, including access to social media sites.
- Make clear that employees should not hold themselves out as speaking on behalf of the company unless authorised to do so.

Of course, it is not enough simply to have such a policy. Employers should communicate its existence to employees, implement appropriate training and take steps to monitor compliance with it and, if necessary, to enforce it.

Finally, all employers should carry out a risk assessment in relation to employees’ usage of social media and should review the need for guidance and policies for their staff, so that the risks have been flagged to employees and rules regarding acceptable conduct have been made clear. This lays a clear path for any employer needing to take disciplinary or other action in the event of a breach.

MONITORING EMPLOYEES’ USE OF SOCIAL MEDIA

There is a wide range of legislation in the UK which governs monitoring:

- Data Protection Act 1998.

An employee does not need to provide consent to monitoring (including monitoring of the use of social media on work systems) provided that:

- An impact assessment has been undertaken.
- Monitoring is for legitimate purposes.
- The monitoring does not involve processing sensitive personal data.

If monitoring is to be carried out the EPDPC also recommends that:

- Employees should be given information if monitoring is to take place (circumstances, nature, how information will be used, safeguards).
- Staff with access to information obtained through monitoring should be limited and should have received appropriate training. Data obtained through monitoring should be secure.

In the UK there is a distinction between “systematic” monitoring (that is, where the employer monitors all the workforce (or particular groups) as a matter of routine) and occasional monitoring. It will usually be easier to justify occasional monitoring (for example, because wrongdoing is suspected) than systematic monitoring.
RIPA provides that businesses can intercept and record communications (including communications via social media) without consent to:

- Ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business.
- Ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.
- Prevent or detect crime.
- Investigate or detect the unauthorised use of the telecommunications system.
- Ensure the effective operation of the system.

Workers’ private lives extend into the workplace and employees are entitled to an expectation of privacy, even where they have been informed monitoring may take place. Covert monitoring may well be a breach of the ECHR, where the employee has an expectation of privacy. The employer will need to have a stronger justification for covert monitoring in such circumstances.

It is therefore always best to ensure that the employee is informed that monitoring will take place (typically via an IT/social media policy) and is reminded of this regularly.

**PROTECTING EMPLOYERS ON THE DEPARTURE OF AN EMPLOYEE**

Recent high-profile cases, such as staff atHMV using the official HMV twitter feed to tweet about the announcement of redundancies at their head office, highlight the importance of careful consideration of the departure of staff who have access to company social media accounts. But consideration should also be given to staff who use their own social media accounts for work purposes.

**Ownership of contact lists on social media**

Many employers actively encourage their employees to use sites like LinkedIn. On LinkedIn, members connect with each other and can share lists of their connections on their profile page. LinkedIn results in employees posting lists of clients and prospective clients in a public domain.

Upon arrival at a new company, an employee will update his or her LinkedIn profile, triggering an update to all of the contacts which announces the details of the new employer. Where the employee in question is a salesperson, trader, recruitment consultant or otherwise works in a business which is heavily dependent on client relationships, this could mean real damage to the former employer’s business.

LinkedIn’s own terms and conditions provide that ownership of a LinkedIn user account remains with the individual. But as we will see, the English courts have disregarded these terms (to some extent) where confidential information is at stake.

**Confidential information**

Ownership of the individual’s contacts is another question, particularly where the contacts are made during the course of employment and overlap significantly with the employer’s client list. An employer may be able to argue that its client list is confidential and that the employee has misused or disclosed this, in breach of their express or implied duties under their contract of employment.

In Hays Specialist Recruitment v Ions [2008] EWHC 745, Mr Ions worked for Hays as a recruitment consultant. Having decided to leave and set up a competing business, but before handing in his notice, Mr Ions sent LinkedIn invitations to some of Hays’ clients and candidates. Hays did not know the extent of Mr Ions’ attempts to “link in” with its contacts (having evidence of this happening on only two occasions) and therefore applied to the High Court for pre-action disclosure of certain relevant documents. They sought this disclosure in order to be able to assess the merits of issuing a claim in relation to Mr Ions’ alleged misuse of confidential company information.

Mr Ions accepted that he was linked in to an unspecified number of Hays’ contacts, but had two arguments as to why no pre-action disclosure should be ordered. First, he argued that this information was “part of his own knowledge base” gained over many years of working in the business (and therefore not protectable as confidential information). Second, he argued that once his LinkedIn invitations had been accepted by the relevant contacts, the information could no longer be said to be confidential. The basis for this assertion was that all of Mr Ions’ LinkedIn contacts would be able to access details of his other contacts, thus exposing the information to a wider audience. The Court gave this argument short shrift, finding that it was Mr Ions’ actions in uploading e-mail addresses to the LinkedIn site which involved a transfer of confidential information, meaning that Hays had an arguable claim, even if the information subsequently lost its confidential status.

Ultimately, the Court took the view that contact details obtained during the course of employment will remain the property of the employer. On this basis, the Judge granted the order for disclosure sought by Hays. However, the case did not go to a full merits hearing (presumably because a settlement was reached), and there was therefore no definitive ruling on this point. Unhelpfully, this means that for now, we cannot be entirely certain of the legal position regarding ownership of LinkedIn contacts.

In Whitmar v Gamage & Others [2013] EWCH 1881, three employees resigned from their employment with Whitmar to undertake a competing business. Amongst other matters, the ex-employees were accused of using a LinkedIn group which one of them had managed on behalf of Whitmar as a source of e-mail addresses for a press release for the new business. They refused to give Whitmar the user name, password or any other access details for the group. The court granted Whitmar a springboard injunction preventing the ex-employees from working for the new business for a period of time and also required them to give Whitmar exclusive access, management and control of the LinkedIn group.

This case is an important reminder to employers to ensure that those who create and manage social media accounts on behalf of their employer should be under an express obligation in their contract of employment to release passwords and other login details on termination of employment. Ideally, a number of employees should have access to the one account, to avoid such a situation arising.

**Database rights**

A client list which is imported onto a social network may amount to a “database” and therefore be protected under the Copyright and Rights in Database Regulations 1997. However, a database right only arises if there has been “a substantial investment in obtaining verifying or presenting the contents of the database”.

In the case of the British Horse Racing Board Limited v William Hill Organisation [2005] EWCA Civ 863 the European Court of Justice held that a database containing the times, dates and locations of horse races together with a list of runners and riders and gate numbers for each race did not require sufficient investment by the British Horse Racing Board to be afforded protection under the regulations.

It is therefore questionable whether adding individual contacts to, for example, Outlook or LinkedIn over a period of time will be sufficient.

In 2007, in the case of PennWell Publishing (UK) Ltd v Ornstein and others [2007] EWHC 1570 (QB), the High Court addressed the issue of ownership of an Outlook contacts list. A journalist, Mr Isles, had left PennWell Publishing, and took with him a CD containing...
his e-mail contacts list. He intended to use the list in order to set up a competing business. The list contained personal contacts that pre-dated Mr Isles' employment with PennWell, together with a large number of contacts he had made while working at PennWell. The Court granted a permanent injunction preventing Ms Isles from using the entire database, ruling that it belonged to his former employer. It may be that the courts would take this approach in relation to social media and contacts databases.

**Restrictive covenants**

Where appropriate, contractual provisions regarding ownership and deletion of client contact lists should be bolstered by well-drafted post-termination restrictions, which expressly prevent the employee from:

- Working for a competitor.
- Soliciting/dealing with clients and poaching staff for a period of time following the termination date.

Employers alive to the risks posed by use of LinkedIn might tailor these restrictions, for example, to provide that updating one's LinkedIn profile to refer to your new employer and setting up your account to ensure that your contacts receive notification of this will be regarded as an act of solicitation, or more likely, dealing with clients. Whether such a provision would be enforceable or regarded by a court as unduly restrictive of course remains to be seen, and as always with post-termination restrictions, will depend on the context. For this reason, such provisions should be in addition to, and separate from, more traditional wording around post-termination solicitation and dealing with clients and prospects. This will afford a court the opportunity to "blue pencil" (effectively cross out) any unenforceable provisions, whilst allowing the remainder to stand.

**Policing social media**

Those employers who have appropriate protection in place will still face practical difficulties when it comes to the departure of key employees with valuable contacts. Imagine such an employee confirms to you that she has deleted all of her company contacts from LinkedIn. If a colleague is still linked in to the departing employee and is willing to co-operate, this might enable the employer to check whether the contacts have in fact been deleted. However, even if they have, the employee could have retained the contact details in some other format, and may also re-connect to her contacts on LinkedIn soon after.

The practical difficulties associated with evidencing an employee's breach are illustrated by the Hays case. After having been threatened with injunctive proceedings by Hays, Mr Ions informed his former employer that he had in fact deleted his entire LinkedIn network, thus effectively destroying a potential source of evidence against him. One of the orders which Hays subsequently obtained therefore required Mr Ions to instruct LinkedIn to supply to Hays copies of all information in its possession relating to Mr Ions' account. The fact that LinkedIn is incorporated in the US could of course give rise to difficulties in enforcing such an order (an issue which was not discussed in the judgment).

This means in practice that in order for contractual protection to have any real effect, the employer may need to take (or at least threaten) court action, seeking an injunction against the employee. However, these challenges are no different from those existing in any other scenario involving breach of post-termination restrictions. Whilst the existence of such restrictions may have a useful deterrent effect, the only decisive way of dealing with former employees who insist on flouting their obligations is to threaten, and sometimes commence, court action.

As with all restrictive covenants, the remedy for breach is for the employer to obtain an injunction for specific performance. In order to do so, the employer must be able to show that the covenant goes no further than is necessary to protect the company's legitimate business interests. The duration and scope of the covenant are relevant in determining this and should therefore vary depending on:

- The seniority of the employee.
- The nature and location of their role.
- The lead time for new business.
- How quickly a client contact will go "stale".

Employers should seriously consider a forensic investigation of its IT systems where wrongdoing is suspected. In addition, the employer may be able to obtain an order for a pre-action disclosure, delivery of documents or for inspection of computers (including the employee's home computer) in order to gather evidence of the wrongdoing.

Whilst technology and social media are making it easier for employees to walk away with client lists and other confidential information, it is also becoming easier for employers to detect these actions by employees. Using a combination of the protections and remedies set out above should protect employers, but given the pace of development of technology and social media it is important to keep policies and practices under review.

In a sense, the rise of social media does not really create new issues for employers; rather it provides a new context for the same old problems. What can be said for certain, however, is that employers who have anticipated these issues, and put appropriate policies and contractual wording in place, will be better placed to protect their business than those who have not.
Practical Law Contributor profiles

Kathryn Dooks, Employment Partner
Kemp Little LLP
T + 44 (0)20 7710 1660
E kathryn.dooks@kemplittle.com
W www.kemplittle.com

Elizabeth Kirk, Employment Associate
Kemp Little LLP
T + 44 (0)20 7710 1616
E elizabeth.kirk@kemplittle.com
W www.kemplittle.com

Professional qualifications. England and Wales, Solicitor
Areas of practice. Employment and business immigration law.

Professional qualifications. England and Wales, Solicitor
Areas of practice. Employment and business immigration law.