Technology in the Workplace: Gift Horse or Trojan Horse?

Chris Middleton, Kemp Little LLP
January 2013
Technology in the workplace: gift horse or Trojan horse?

1. Introduction
Technology has undoubtedly brought many benefits to the workplace. It makes flexible working – including working from home – a viable option for most employees. Legislation is slowly catching up with the technology – since its original introduction in 2003, the right to request flexible working has gradually been expanded from carers of children under the age of six (or disabled children under the age of 18) to, potentially under the latest proposals, all employees with at least 26 weeks’ service.

From an employer’s perspective, flexible working can be a valuable tool in motivating and/or retaining employees.

Similarly, technology also allows an employer greater flexibility about where its staff are based – back office staff no longer necessarily need to be based in the same location as front-line employees.

Technology can also bring benefits in service delivery – thanks to Blackberries/similar devices employees can remain contactable whilst travelling. More recently, employers are using technology to increase employee engagement. A survey by the Hay Group found that office workers who were actively engaged were 43% more productive. Ways of achieving this can include giving employees visibility of their performance relative to expectations or the mean, and giving employees details of activity-based costing.

But all of these benefits can bring challenges –

- is the boundary between work and private life being blurred?
- does more freedom for employees equate to a loss of control for employers?
- what are the implications for employee expectations of privacy?
- at the same time as businesses are becoming more dependent on data/IP, data is also becoming far more portable than ever before;
- and what about the health and safety considerations of employees always being connected or working from home?

We discuss below how employers can manage these and other similar risks.

2. Blurring the boundary between work and private life
The short answer to this question - is the boundary between work and private life being blurred? – is undoubtedly yes.

Employees can work from home as well as the office. There is an increasing expectation that employees will be available via mobile devices outside office hours. Whilst in the office, employees will often access social media (for personal as well as work-related reasons). Finally, social media provides greater scope for employees to interact with colleagues in a personal capacity.

This blurring of the boundary can have implications for how employees should manage their employees, employees’ expectations of privacy and an employer’s duty of care to its employees – all of these are discussed below.

---

1 http://www.bis.gov.uk/assets/biscore/employment-matters/docs/m/12-1269-modern-workplaces-response-flexible-working.pdf
2 http://www.psychologytoday.com/blog/wired-success/201005/does-employee-engagement-really-drive-productivity
3. **A loss of control over employees?**

Whilst technology can be empowering for employees it also gives them more scope to do damage to their employer’s business.

**Employees going rogue…**

At its simplest, this might involve an employee posting inappropriate statements on social media or sending an inappropriate email – what previously might have been a careless remark at the water-cooler may now manifest itself in (semi-) permanent electronic form.

Part of the answer to this will be to educate employees as to what is and is not acceptable and to advise them what the consequences will be (for example, disciplinary action) if they breach acceptable standards. Organisations should also have a strategy for dealing with unwanted posts if/when they do arise – the approach of the American Red Cross to rogue posts on its Twitter feed have been held up as an example of how to deal with this type situation3.

Employers may, as noted above, also want to take disciplinary action against their employees. The extent to which this is justifiable will depend on the nature of what the employee has done, and also whether the employer has clear guidelines that have been communicated to employees regarding what is and is not acceptable.

By way of example, the case of *Preece v JD Wetherspoons plc*4 concerned a pub manager who posted on Facebook whilst at work concerning about two customers at the pub. The customers had previously verbally abused and threatened Miss Preece.

The customers’ daughter subsequently became aware of and complained about the posts. After an investigation, Miss Preece was dismissed. She brought an unfair dismissal claim, but the Employment Tribunal found that her dismissal had been fair. Amongst other things, it noted that whilst the customers’ actions towards Miss Preece had been abusive, her Facebook entries had been made over a long period of time after the situation had calmed down. The entries risked damaging the employer’s reputation and whilst Miss Preece had believed that her Facebook settings meant that they could only be seen by her work and school colleagues, the reality is that they could be seen by a wider audience and were therefore in the public domain. The employer was also undoubtedly assisted by the fact that it had an email, intranet and internet policy that spelt out that posts on social media (and other) sites that damaged the its reputation could result in disciplinary action. So where once Miss Preece might have let off steam in a quick conversation, she created a public post and lost her job.

Contrast, however, that decision with the case of *Smith v Trafford Housing Trust*5. In that case, Mr Smith posted a link on his Facebook page to a BBC news article - “Gay church ‘marriages’ set to get the go-ahead”, adding the following comment of his own: “an equality too far.” Mr Smith had 45 colleagues amongst his Facebook friends. In response, one of them asked if he didn’t approve. Mr Smith replied “no, not really, I don’t understand why people have no faith and don’t believe in Christ would want to get hitched in church the bible is quite specific that marriage is for men and women if the state wants to offer civil marriage to same sex then that is up to the state; but the state shouldn't impose its rules on places of faith and conscience”

Mr Smith was subsequently disciplined and demoted. Amongst other things, the Trust found that one of Mr Smith’s colleagues had been deeply offended by the post, Mr Smith had disclosed that he was a

---

3 http://www.huffingtonpost.com/2011/02/16/red-cross-rogue-tweet_n_824114.html
4 ET2104806/10
5 [2012] EWHC 3221
manager of the Trust (thereby linking his views to the Trust) and had breached the Trust’s Code of Conduct by bringing it into disrepute.

In a subsequent Hearing, the High Court found that Mr Smith’s demotion had been unlawful. The High Court found that although Mr Smith had disclosed that he was a manager of the Trust no reasonable person would believe that he was speaking on behalf of the Trust. Moreover, his views were expressed moderately and were made outside working hours so were unlikely to lead a reader of them to think less of the Trust.

What the Smith case shows is that, as in other areas of employment law, a question of proportionality is likely to come into play. This is further illustrated by the case of Taylor v Somerfield\(^6\). The case concerned the dismissal of an employee who had posted a video on YouTube which showed him and a colleague play-fighting with plastic bags. He was dismissed for bringing the company into disrepute. The Employment Tribunal found that the dismissal was unfair as there was no evidence that the video had in fact brought the company into disrepute. The video had only been viewed 8 times, and 3 of those occasions were by the employee’s managers.

…and the employer being liable for it

Another area of concerns for employers is where they may be liable for what their employees say and do.

It is already a well-established principle that an employer may be vicariously liable for its employees’ actions. This can arise out of discrimination, harassment or tort.

For example, the Equality Act 2010 (the “Equality Act”) provides that a discriminatory act done by a person in the course of their employment is treated as also having been done by their employer\(^7\). An employer has a defence if it can show that it took “all reasonable steps” to prevent the discriminatory act.

The phrase ‘in the course of employment’ is construed broadly\(^8\) and can even encompass acts outside the workplace – in the case of Chief Constable of the Lincolnshire Police v Stubbs\(^9\), the employer was held liable for the sexual harassment of one of its employees by a colleague, even though one of the two incidents in question occurred in a pub after work at the leaving party of another police officer.

Similarly, an employer may be liable for the actions of its employees under the Protection From Harassment Act 1997 (the “Harassment Act”). The Harassment Act provides that a person must not pursue a course of conduct which amounts to harassment of another and which he knows or ought reasonably to know amounts to harassment of the other\(^10\). The person who is the victim of such conduct can bring a claim for damages\(^11\).

Majrowski v Guy’s and St Thomas’ NHS Trust\(^12\) involved a claim from an employee under the Harassment Act who claimed that he had been bullied, intimidated and harassed by his manager during the course of his employment. The House of Lords ruled unanimously that Mr Majrowski’s employer could, in principle, be liable for the harassment.

---

\(^6\) Unreported  
\(^7\) s109  
\(^8\) Jones v Tower Boot Co Ltd 1997 IRLR 168  
\(^9\) 1999 IRLR 81  
\(^10\) s1  
\(^11\) s3  
\(^12\) 2006 UKHL 34
Finally, it is a long-established principle that an employer may be liable in tort for acts of its employees if that there is a sufficiently strong connection between the employee's wrong-doing and their employment\textsuperscript{13}.

So if an employee does something unlawful at work, or in a situation connected to work, their employer may well be liable for it. This could extend to, for example, cyber-bullying, or posting of discriminatory comments about a colleague on Facebook. Moreover, with the blurring of the lines between work and private life, the scope for something to be (sufficiently) connected with work, even if occurring outside the office/outside office hours, is surely increasing.

4. **The implications for employee expectations of privacy**

The flip side of the blurring of the boundary between work and private life is that there may also be implications for employee expectations of workplace privacy.

*Employees do have a right to privacy, but not an absolute right*

The good news starting point for employees is that they do have some right to privacy in the workplace. That right derives from **Article 8 of the European Convention on Human Rights and was explored in** Pay v United Kingdom\textsuperscript{14}. The case concerned the dismissal of a probation officer because of his links to a business involved in sadomasochistic activities. He argued that this breached his Article 8 right. In this case it was found the dismissal was justified because of the individual’s job, which involved working with sex offenders. However, absent that justification, one can imagine a different result being reached. Similar considerations would apply if an employer wanted to dismiss an employee as a result of information it discovered about them on a social media (or other internet) site.

In a similar vein, the dismissal of the employee in *Gosden v Lifeline Project Ltd*\textsuperscript{15} who had forwarded an offensive email from his home computer, outside working hours, was found to be fair. Mr Gosden worked with drug users in prison. The email, which contained sexist and racist material, was forwarded to a colleague who also worked in the prison and was headed with the words "It is your duty to pass this on!"

In reaching its decision that the dismissal was fair, the Tribunal considered whether Mr Gosden’s right to privacy had been infringed. However, whilst the email had been outside work hours and from outside the workplace, the fact that it had been sent to a colleague with an instruction to forward it effectively meant that Mr Gosden relinquished his to privacy.

So, in appropriate circumstances, employers can take a legitimate interest in what an employer does outside the workplace.

*Employers may need to do more monitoring*

In view of the spread of social media/other means of communication, employers may feel the need to undertake more monitoring of their employees’ activities. This will be acceptable in principle provided it is done in an appropriate manner.

Monitoring will of course involve the processing of personal data for the purposes of the Data Protection Act 1998 (the “DP Act”). Amongst other things, the DP Act requires data to be processed fairly and lawfully, that data retained should be adequate, relevant and not excessive, and that it

\textsuperscript{13} List and Others v. Hesley Hall Limited [2001] UKHL 22 (3 May 2001)
\textsuperscript{14} 2009 IRLR 139
\textsuperscript{15} ET/2802731/2009
should be subject to adequate technical/organisation measures to protect against unauthorised processing and accidental loss/destruction/damage.

The principles in the DP Act are expanded on in Part 3 of the (non-binding) Employment Practices Data Protection Code. Amongst other things, the Code advises that monitoring should be done in a way which is proportionate to the perceived risk, that employers should undertake an impact assessment before undertaking monitoring and consider alternatives, that they should provide full information to employees about what monitoring they are doing and should have in place technical/security measures to protect any data obtained as a result.

An employee’s Article 8 rights may also apply to protect an employee against proportionate, but not excessive, monitoring of them.

5. Portability of Data

As the use of sites such as “LinkedIn” (www.linkedin.com) becomes more widespread, employers may find it harder to control their client lists and ultimately to protect their business from departing employees set on poaching clients. In a recent study in the US, six out of ten employees admitted that they had taken company data (such as client lists) on their departure.

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. In businesses where client confidentiality is key (for example in the legal profession) this is clearly problematic. When an employee leaves his employment, he can quickly update the website to show that he has moved and inform all of his contacts that he has done so. This obviously makes it much easier for employees to attempt to poach clients following the termination of their employment, so to what extent can employers protect themselves?

Are client lists confidential?

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), Hays applied for an order for pre-action disclosure against a former employee, Ions, to establish whether he had migrated details of business contacts from the Hays client list to LinkedIn. Ions argued that Hays encouraged him to use LinkedIn so it had, in effect, consented to this migration. The High Court held that Hays had reasonable grounds for considering that it might have a claim against Ions in relation to the transfer of confidential information to his LinkedIn account and it ordered pre-action disclosure against Ions. It is unclear how the matter progressed as no further hearings have been reported (suggesting the parties may have settled the matter). However the court was willing to entertain the possibility that Ions had potentially misused Hays’ confidential information by migrating details from the database onto LinkedIn.

If the contacts are only located on LinkedIn, however, and have not been migrated from a confidential database, it is difficult to see how an employer could argue that they are confidential, given that when a connection is made with another contact on LinkedIn, that individual can view the employee’s full list of connections. In a situation like this, it may be easier for an employer to rely on some of the other remedies/protections set out below.

16 See McGowan v Scottish Water EATS/0007/04
17 See Mills v Mid Sussex District Council, ET, unreported
A protected database?

The client list may amount to a “database” 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) 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, say, Outlook or LinkedIn over a period of time will be sufficient.

In Pennwell Publishing (UK) Limited v Ornstein (2007), Ornstein was a trade journalist who, when he joined Pennwell, had his own Excel spread sheet containing contacts from his previous employment. He added these contacts to Pennwell’s Outlook list and did not maintain any separate list. On his departure, the question was whether Pennwell owned the list and could prevent him from taking it elsewhere. The High Court held that when Ornstein put his own list of contacts into Pennwell’s Outlook list, he had created a new database which belonged to the employer; therefore he could not take his contacts with him. If he had maintained a separate list of pre-existing contacts on his own computer he would have been able to take these contacts.

However, Ornstein did not try to argue that the contacts in Outlook were not a “database” under the Regulations. A different outcome may have resulted if such an argument had been put forward, given that there may not have been a “substantial investment” in the creation of the Outlook list.

Importance of having an IT policy…

In the Pennwell case, the Judge recommended that employers should put in place an E-mail/IT policy requiring employees to keep any personal contacts separate from their business contacts within Outlook.

Certainly, a comprehensive IT policy which incorporates policies on the use of email contacts lists and LinkedIn/similar sites is a useful tool. The employer could also consider going through lists of contacts on, for example, LinkedIn on termination and requiring the employee to delete any contacts which are client contacts. There is a question as to the employee’s right to privacy here, particularly if they have private contacts to whom they are connected on LinkedIn, as well as client contacts. Also, it is doubtful how effective this would be, as it is very easy for the employee to reconnect with the client contact shortly afterwards.

…and restrictive covenants

For this reason, where a business genuinely requires protection from ex-employees on termination, the best solution for employers may well be to include a non-dealing restrictive covenant in the employee’s contract of employment. This would prevent the employee from having any dealings whatsoever with a client for a period following termination, including for example making connections with them on LinkedIn and attempting to solicit business from them. It would also prevent them from speaking to a client if the client contacted them unsolicited.

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 and how quickly a client contact will go “stale”.

6. **Health and safety considerations**

Technology is changing the way employees work. Whilst there are considerable benefits to this as described above, there are also countervailing matters for employers to consider –

- home-working may lead to isolation, which may increase an employee’s risk of suffering from stress and depression;
- a culture of constant availability could also increase the risk of stress claims;
- even spending too many hours in front of a computer screen can increase the risks of depression and insomnia;\(^{19}\);
- excessive computer use is also linked to an increased risk of repetitive strain injury;
- and this risk may be greater where employees are working from home in a workstation that has not been adequately set up;
- it is even being suggested that internet addiction is a mental health condition\(^ {20}\).

Quite apart from an employer’s legal obligations, stress-related absences have a huge cost for employers\(^ {21}\). But employers also have legal obligations in relation to their employee’s health and safety.

**An employer’s health and safety duties**

Under the Health and Safety at Work Act 1974, an employer is responsible for an employee’s welfare, health and safety, "so far as is reasonably practicable. Employers also have a duty to conduct a suitable and sufficient risk assessment of all the work activities carried out by their employees, including homeworkers, to identify hazards and assess the degree of risk. An employer’s duties in these regards will extend to the employee’s mental health.

Employers also have a common law duty to take reasonable care for the health and safety of employees in the workplace. This requires employers to take reasonable care to prevent reasonably foreseeable injuries. Again, this obligation will extend to the prevention of psychological injuries.

The Court of Appeal has given guidance on an employer’s duties when dealing with stress-related illnesses\(^ {22}\) – the Court said that employers will need to be vigilant, looking for the tell-tale signs, although unless they are aware of any particular vulnerability, are entitled to assume that an employee can cope with the "normal pressures" of the job. The Court also said that warning signs from employees are particularly significant.

So employers will need to be alert for signs that employees are over-worked, stressed, isolated or similar because of their working arrangements. They also need to ensure that they undertake health and safety assessments and give proper guidance to reduce the risk of physical/repetitive strain injuries.

**Disability discrimination**

Employers should also be aware that employees with more serious medical conditions may well be deemed disabled for the purposes of the Equality Act and therefore protected accordingly.

---

\(^{19}\) [http://www.dailymail.co.uk/health/article-153281/Why-using-cause-depression.html](http://www.dailymail.co.uk/health/article-153281/Why-using-cause-depression.html)


\(^{22}\) Sutherland v Hatton; Somerset County Council v Barber; Sandwell Metropolitan Borough Council v Jones; Baker Refractories Ltd v Bishop [2002] EWCA Civ 76
An employer will have a disabled within the meaning of the Equality Act if they have a physical or mental impairment that has a substantial and long term adverse effect on their ability to carry out normal day-to-day activities. Long term means the impairment has lasted at least 12 months, is likely to last 12 months or is likely to last for the rest of the person’s life.

Conditions such as depression and RSI can certainly be a disability for these purposes if they are serious enough.

Where an employee is disabled for the purposes of the Equality Act, the employer, will amongst other things, have a duty to make reasonable adjustments in certain circumstances in respect of them. Reasonable adjustments may include allocating some of the disabled person’s duties to another person, transferring them to another role, altering their hours or place of work and providing additional training or support and so on. A failure to comply with the reasonable adjustments duty can lead to expensive claims from employees.

Would a condition such as internet addiction ever amount to a disability? We are not there yet, but it is certainly not impossible to imagine a Tribunal reaching that conclusion; it appears that courts in the United States have already been grappling with this issue.¹²³

What is clear is that any dismissal of an employee will only be justified if it is appropriate and proportionate in the circumstances. Therefore, the two employees in Grant & Ross v Mitie Property Services UK Limited²⁴ were able to claim that their dismissal for using the internet at work was unfair. The employer’s policy was that employees were allowed to access the internet outside “core working times”. The employees said that they only used the internet when there was no work to do. The Employment Tribunal found that the employer’s rules about when employees could access the internet were unclear.

7. **Prevention is better than cure**

All of the risks described above can be managed, provided employers take a proportionate approach to dealing with employers, have appropriate guidance and take proactive steps in managing their employees’ health.

Employers should therefore have guidance on use of social media. Amongst other things, this will need to: specify to what extent employees can access such sites, and when; make clear that employees should not disparage customers, suppliers, employees etc on such sites; make clear that employees should not disclose confidential information etc; and make clear that employees should not hold themselves out as speaking on behalf of the company unless authorised to do so.

Employers should also have policies on monitoring (so that employees are aware of when, how and why this takes place) and guidance on safe work practices.

For further information, please contact Christopher Middleton, Employment Partner, Kemp Little LLP

---


²⁴ Unreported