Social Media: Legal Issues in Recruitment & Dismissal

Social media presents many opportunities and challenges for charities. Employers across all sectors have dealt with disciplinary issues involving online misconduct. The fundamental legal principles that apply to issues such as misconduct, data protection and competitive behaviour remain the same.

We will look at:

- Using information from social media in recruitment
- Misuse of social media, disciplinary issues and social media policies
- Misconduct and reputational risk v the right to privacy
- Ownership and control of online accounts and followers
- Intellectual property and competition issues

Recruitment

A 2008 Personnel Today survey indicated that while 27% of companies look at personal online profiles in recruitment, charities are unlikely to do so; only 8% of charity respondents in the survey said they would carry out such research. The Information Commissioner's Employment Practices Code gives detailed guidance on the gathering of information during the recruitment process. The Code states that if information will be obtained from sources other than the applicant's application form, individuals should be informed of this and should told of the nature of the additional information sought and the sources which will be used. (Section 1.2.4)

If you wish to consider information they have obtained online in the recruitment process, the applicant should be given an opportunity to respond. Section 1.6.6 of the Code indicates that employers should not place reliance on information collected from possibly unreliable sources and the application should be allowed to make representations about information that will affect the decision to finally appoint.

> *Information Commissioner's Office (www.ico.gov.uk): The Employment Practices Code*
>
> *1.6.4 Only use vetting as a means of obtaining specific information, not as a means of general intelligence gathering. Ensure that the extent and nature of information sought is justified.*
> *1.6.5 Only seek information from sources where it is likely that relevant information will be revealed. Only approach the applicant's family or close associates in exceptional cases.*
> *1.6.6 Do not place reliance on information collected from possibly unreliable sources. Allow the applicant to make representations regarding information that will affect the decision to finally appoint.*

Discrimination claims

Recruiters should be aware that if a prospective candidate can raise an inference of possible discrimination, this shifts the burden of proof to the employer to show that there was another reason (not tainted by discrimination) for the employer's decision. Personal online profiles will often reveal a candidate's age, ethnicity, sexual orientation, beliefs and other information. Reliance on such profiles can increase the risk of discrimination challenges.

Discipline and Dismissal

ACAS Code

ACAS guidance makes it clear that employers should take a common sense approach and should not generally discipline staff for online comments that would not attract sanctions if they were simply verbal. Employers who have a particular concern about their online image and want staff to take additional steps to safeguard it must make this clear.

Employers should consider whether informal action would be sufficient to address the problem, in the same way that such an option would be considered with other alleged misconduct.

The Importance of a Clear Policy

Crisp v Apple Retail (UK) Ltd (ET)

Mr Crisp joined Apple in September 2009 and received extensive training on the use of social media. This covered how he should present himself "in public" on social networks and blogs; the fact that employees may be disciplined for posts or online activity and the fact that activities outside work may adversely affect the company, regardless of whether or not an employee identifies themselves as an Apple employee. The training also emphasised that if an employee was unsure whether online activity – posting comments and photos, blogging etc – breached internal rules, they should ask.

Employers are expressly prohibited from commenting about Apple's products, services or initiatives on personal websites.

In November 2010, one of Mr Crisp's colleagues alerted their store leader to comments made by Mr Crisp on Facebook. One post referred to his "jesusPhone" and complained about problems locating the Royal Courts of Justice and getting a signal. Mr Crisp also complained about an Apple application getting his time zone wrong and waking him up at 3 am as well as general complaints about work. A further post said "Tomorrow's just another day that hopefully I will forget" posted the day before Apple used the tagline "tomorrow is another day that you'll never forget" to advertise the forthcoming availability of Beatles music on iTunes.

Disciplinary proceedings were commenced and Mr Crisp was suspended. He removed the comments as soon as he became aware of the employer's concern. At the investigatory stage, Mr Crisp accepted that some of his comments did relate to Apple products but maintained that his Facebook page was private. Mr Crisp was then invited to a disciplinary meeting; the allegations were that he had brought Apple's name into disrepute by commenting about Apple products and services on Facebook. Mr Crisp argued that other employees had made similar comments and had not been dismissed. He referred to three separate cases where employees had posted about Apple apps not working; performing in a burlesque show and allowing an iPhone to run 3rd party software. The manager conducting the disciplinary hearing considered that while only Mr Crisp's friends could see his Facebook posts, they could have easily been shared by others and that he should have been aware that the comments could have been made public. Mr Crisp was dismissed for bringing the company into disrepute. He appealed and was given a full rehearing. His dismissal was upheld, but on slightly different grounds: breach of Apple's business conduct policy.

At the Tribunal hearing, Apple gave evidence about how similar cases had been dealt with previously. One employee had been dismissed. The two other employees Mr Crisp had referred to had received final written warnings. Both were extremely apologetic in the disciplinary process. The Tribunal held that there was clear evidence that Apple valued its' image (indicated by the detailed employee training on protecting that image and clear

policies) and they were entitled to conclude that any Facebook post was not truly private because any of the employee's friends could have shared the post with others.

Mr Crisp also argued that the decision infringed his privacy and human rights, in particular the right to respect for private and family life and freedom of expression. The Tribunal noted that the employer had not hacked into Mr Crisp's account and he had not been coerced into providing access, rather the comments had been reported by another employee. There was no reasonable expectation of privacy and the employer was entitled to protect its reputation in these circumstances.

The company had failed to provide Mr Crisp with a copy of the disciplinary procedure until 1 hour before the investigation meeting (while on suspension he was not able to access internal procedures). The Tribunal considered that this was a procedural failure but was not significant enough to affect the fairness of the dismissal, particularly in light of the full rehearing at the appeal stage.

Preece v JD Wetherspoon plc (ET)

A manager was dismissed after she made inappropriate comments on Facebook about two customers while at work.

Ms Preece thought that only her close friends would be able to see the comments. However, all of her 646 Facebook friends could see the comments including the daughter of one of the individuals who was the subject of the comments, who subsequently complained to the company. Wetherspoons had a clear policy that prohibited the use of Facebook at work.

The dismissal was held to be fair. The Tribunal commented that while they might have been inclined to give a final warning, they could not substitute their view for the employer's and the decision did fall within the band of reasonable responses open to an employer in those circumstances. It was not relevant that the employee was genuinely mistaken about her privacy settings

Did the online misconduct have an adverse impact on the organisation?

Online comments and posting are intrinsically public. However, employers cannot automatically infer from this that offensive or otherwise adverse online behaviour has brought the organisation into disrepute. Employers must consider the evidence and assess actual impact of the comments on the organisation's reputation.

Gosden v Lifeline Project Ltd (ET)

The Claimant was employed by Lifeline, a charity who worked with HM Prison Service, working with drug users in prison. Lifeline also worked with the wider community. The Claimant, Mr Gosden, sent an email from a personal account (and his home computer) to the personal email account of a Prison Service employee whom he knew as a result of his work. The email was a chain email headed 'it is your duty to pass this on' and contained racist and sexist material, including pornographic images. When the Prison Service employee forwarded the email on, it was sent to Prison Service email accounts and picked up by their firewall.

The Prison Service banned Mr Gosden from working on their premises and the Prison Service employee who forwarded the email was subjected to disciplinary proceedings and took early retirement.

Lifeline dismissed Mr Gosden for gross misconduct, on the basis that he had carried out an act which breached their equal opportunities policy and which may damage the charity's relationship with one its main commissioners. The dismissal was held to be fair. However,

when considering communications that are entirely outside the workplace, employers need to consider the impact carefully. In this case, the email was clearly intended to be circulated widely and the content was extremely offensive.

Taylor v Somerfield (ET)

The Claimant was dismissed for bringing the employer into disrepute after he and two other employees posted a video on YouTube in which an employee (not identifiable but clearly wearing a Somerfield uniform) hit another employee with plastic bags, stuffed with other plastic bags. The video had only had 8 hits and 3 of these were from employer's managers in the course of the investigation process.

There had previously been some local press coverage about clips posted on YouTube showing Somerfield staff knocking cakes onto the floor and throwing things at displays in stores. Following this, managers had been instructed to warn employees that such behaviour would be misconduct but the manager in the Claimant's store did not actually communicate this to staff. The Tribunal also noted that the staff concerned were junior and found that the dismissal was unfair.

Whitham v Club 24 (ET)

The Claimant was a team leader in a call centre which handled calls for external clients, including Volkswagon. After a particularly bad day, she posted on Facebook "I think I work in a nursery and I do not mean working with plants."

Management were told of the comments by colleagues who were the Claimant's friends on Facebook. The Claimant was subsequently dismissed for gross misconduct, despite an otherwise clean disciplinary record. The employer argued that the comments had brought the company into disrepute and there had been a risk of an adverse impact on its' relationship with Volkswagon, although no evidence of actual damage to the relationship was presented.

The Tribunal did not accept that there was any real risk to the company's relationship with its' client. It considered that the comments were trivial in nature and there was no specific reference to Volkswagon.

As with all misconduct cases, it is important to ensure that if an allegation, such as an allegation that an employee has brought the company into disrepute, is upheld, it must be supported with reasonable evidence.

Regardless of whether the alleged misconduct is online or not, the employer must consider all the evidence. Where the employer believes the employee has brought the organisation into disrepute, they must present evidence of this, which can be complaints or other comments from third parties online.

Teggart v TeleTech UK Limited (Northern Ireland Industrial Tribunal – the principles of the law of unfair dismissal are the same in all parts of the UK)

Mr Teggart, a customer service representative in a call centre, posted a number of vulgar comments about a female colleague ("A"), including a comment asking who at TeleTech had A not slept with. The comments were read by other work colleagues although A could not see them. She heard about them from a friend and asked Mr Teggart's girlfriend to get him to remove them. Mr Teggart felt offended by this and posted a further obscene comment about A on his Facebook page.

The comments were reported to the company by a call from someone who claimed to be a customer but who was never interviewed. The service manager spoke to A who said she was distressed about the posts (but no formal statement was taken). Mr Teggart was

suspended pending a disciplinary investigation into alleged harassment of a colleague and actions bringing the company into serious disrepute. He argued that the comments were a joke and were not intended to harass but simply 'create vulgar distaste' for A. Both allegations were capable of amounting to gross misconduct under the company's internal policies.

The Tribunal found that there were deficiencies in the company's disciplinary process. A full investigation was only carried out after the disciplinary hearing. However, the company gave Mr Teggart statements from witnesses prior to his appeal which cured this procedural defect.

The company upheld the allegations of harassment and bringing the company into disrepute and dismissed Mr Teggart. The decision was confirmed on appeal. The Tribunal criticised the second ground of misconduct: bringing the company into serious disrepute. When making the decision to dismiss, the panel had not considered whether the damage to the company's reputation was serious. Only one member of the public appeared to be aware of the comment but there was no statement from that individual.

Mr Teggart argued that his rights under Articles 8, 9 and 10 (the right to respect for private and family life; the right to freedom of belief and religion and the right of freedom of expression respectively) of the European Convention of Human Rights had been breached. The Tribunal held that when Mr Teggart posted the comments on Facebook he had given up any right to consider them to be private. They did not feel that the comments amounted to a protected belief under the Convention; Mr Teggart was alleging that a colleague was promiscuous. In relation to freedom of expression, this right is not unlimited and did not provide a defence where comments amounted to harassment and unlawfully damaged the reputation of another.

Social Media Policies

What should policies cover?

ACAS highlights the following areas to cover in a workplace policy:

- *Network security: to avoid viruses, most organisations will have controls on the downloading of software. Technical security features, such as firewalls, will usually be managed by the IT department.*
- *Acceptable behaviour and use for:*
    - *Internet and emails: what limits are there on personal use of internet and email?*
    - *Smart phones: employers need to update their policies to cover new and evolving ways for accessing social networking tools and to reflect changing employee behaviour and attitudes.*
    - *Social network sites: remind employees of privacy settings. Research has shown that the majority of employees would change what they have written on their social networking sites if they thought their employer could read them. Also cross reference to your bullying and harassment policy.*
    - *Blogging and tweeting: if an employee is representing the company, set appropriate rules for what information they may disclose, the range of opinions they may express and reference relevant legislation on copyright and public interest disclosure.*
    - *Data protection and monitoring: Have you considered alternatives to monitoring and can you justify its use in terms of the negative impact it will have on your*

business? Make sure you consult thoroughly with your employees and their representatives.

- *Business objectives: As well as setting clear rules on behaviour, many employers are integrating the use of social media tools into their business strategy. Social networking can be used internally to promote levels of employee engagement and externally to help promote the organisational brand and reputation.*

- *Disciplinary procedures: Try and apply the same standards in virtual and non-virtual settings. To help you respond reasonably, consider the nature of the comments made and their likely impact on the organisation. Provide examples of what might be classed as 'defamation' and the sanctions you will impose. Also, be clear about confidentiality and what constitutes intellectual property.*

ACAS Advice & Guidance: Social Networking

Key Points for your Policy

- Consider whether you wish to prohibit staff from adding service users or work contacts on Facebook or LinkedIn and expressly cover this in the policy.

- Do specify that the policy covers all online activity, both in and out of working hours and regardless of whether the employer's computers/phones/equipment is used.

- Do warn staff that even if a Facebook post can only be read by a limited group of contacts, those contacts can repost it and it could be made public without prior notice.

- Do emphasise that all activity in and out of work is capable of bringing the organisation into disrepute. The particular risk with social media is that it can create a record of certain behaviour over which the employee has no control.

- Do make it clear that the obligation not to bring the organisation into disrepute by conduct out of work also applies to online conduct.

- Consider whether your staff may comment online about issues relevant to your work. Be clear about whether staff are free to do so without prior notice (i.e. all you require is that they state that they are writing in a personal capacity and not on behalf of their employer or any other partner or associated organisation) or whether this is prohibited. Staff should be encouraged to speak to a specific person (e.g. their manager) if they are unsure about any aspect of the policy.

- Warn staff that any electronic communication or document which includes comments about a particular individual may be disclosable to them if they made a data subject access request under the Data Protection Act.

- Highlight the issue of misuse of intellectual property belonging to third parties.

- If use of social media is one of the tools you use in fundraising, recruitment, campaigning etc, do set out clear guidelines. This can be a separate policy or simply a defined section within your social media policy but you should be clear that this differs from personal use of social media.

    - It is generally advisable to ensure that employees have separate online accounts for work related online activity, to minimise the risk of disputes over ownership of the account if they leave.

- You should guide staff about the type of social media content you expect, when they can, or are expected to, use initiative and comment or respond quickly and when they should seek approval or consult a manager.

- Set out guidance for dealing with online criticism or difficult comments from third parties

- Highlight the risks of claims for defamation or infringement of intellectual property rights and the importance of not disclosing confidential information.

It is good practice to consult with staff about the introduction of new non-contractual policies, although it is not a strict legal requirement. As with all workplace policies, it should be non-contractual to allow the employer to make changes without the need to obtain consent.

It is vital to communicate the policy to all new and existing staff; it will not be safe to rely on a policy to discipline or dismiss employees if it has not been drawn to their attention.

Policies should also be applied in practice as inconsistent treatment of employees in the same or similar situations can render a dismissal unfair.

Ownership of followers and social media accounts

Hays Specialist Recruitment v Mark Ions (1) and Exclusive Human Resources Ltd (2) [2008] EWHC 745 Ch

Mr Ions worked for Hays for approximately 6 years before leaving to set up a competing business (he was open with Hays about his plans). His Hays contract including an obligation not to disclose any confidential information, including client database details and a prohibition on soliciting, canvassing, dealing with or accepting instructions from clients or applicants with whom he dealt or had contact with during his employment for a period of six months thereafter.

In their High Court application for pre action disclosure, Hays alleged that while still in their employment Mr Ions transferred personal information to his own LinkedIn account for use in his new business. Hays employees were encouraged to join LinkedIn and use this for business purposes.

Mr Ions accepted that he had sent LinkedIn connection requests to two applicants who had registered with Hayes and to the HR manager at a company which was an existing Hays client. Hays alleged that Mr Ions had used LinkedIn as a way of transferring confidential Hays data to his personal account via LinkedIn. In pre-action correspondence from Hays' solicitors, they requested a copy of all of Mr Ions' LinkedIn business contacts. Mr Ions' response was that he had deleted the list and could not recreate it from memory. The operators of LinkedIn agreed to preserve the data pending the outcome of the hearing.

Hays relied on the fact that Mr Ions had made a number of searches of their client database which they considered to be suspicious. They also produced double hearsay evidence of comments allegedly made by Mr Ions but this was disregarded by the Court.

However, the Court considered that Mr Ions' actions in adding Hays' contacts to LinkedIn after he had incorporated his new company (but before he left) gave reasonable grounds for the suspicion that the contacts were added with the purpose of competing with Hays. It was irrelevant that the contacts had to accept Mr Ions' invitation for access to their profiles. If the details had been obtained from searches of Hayes' database, there may be misuse of confidential information. This was not merely a case of Mr Ions making contact with

individuals he had worked with via LinkedIn – this was implicit in the fact that he could not recreate the list from memory.

Hays were not entitled to an order for details of all of Mr Ions' LinkedIn contacts as this was not in itself a specific document. This was simply a request for information. The Court was also unwilling to order that Mr Ions disclose his own client database as that would force him to give commercially sensitive information to a competitor. However, Hays were entitled to disclosure of emails sent by Mr Ions' via his LinkedIn account from Hays' computer system and documents relating to the use of contacts downloaded from Hays' system during employment.

Surveillance and Monitoring Employees in the Workplace or Online

Data Protection Requests

Employees, as data subjects, are entitled to access personal data held about them in the same way as third parties.

The ICO Employment Practices Code

> *...The right applies, for example, to sickness records, disciplinary or training records, appraisal or performance review notes, e-mails, word-processed documents, e-mail logs, audit trails, information held in general personnel files and interview notes, whether held as computerised files, or as structured paper records. A fee of up to £10 can be charged by the employer for giving access.*
> *Responding to a subject access request involves:*
>
> *• telling the worker if the organisation keeps any personal information about him or her;*
>
> *• giving the worker a description of the type of information the organisation keeps, the purposes it is used for and the types of organisations which it may be passed on to, if any;*
>
> *• showing the worker all the information the organisation keeps about him or her, explaining any codes or other unintelligible terms used;*
>
> *• providing this information in a hard copy or in readily readable, permanent electronic form unless providing it in that way would involve disproportionate effort or the worker agrees to receive it in some other way;*
>
> *• providing the worker with any additional information the organisation has as to the source of the information kept about him or her.*

Monitoring Online Behaviour – The Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000

Under the Regulation of Investigatory Powers Act (RIPA), the general rule is that interception of public postal systems or public or private telecommunications systems is a criminal offence unless that interception is authorised under the Act.

Even if interception is authorised under RIPA or the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, interception in the employment context is likely to include the processing of personal data. Therefore, the obligations under the DPA will also apply.

It may be the case that interception would be permitted under RIPA but would be in breach of the DPA. However, the fact that the processing of personal data is lawful under the DPA does not provide any excuse for a breach of RIPA.

The ICO Code does not have an exhaustive definition of 'monitoring' but examples include:

> • *gathering information through point of sale terminals, to check the efficiency of individual supermarket check-out operators*
>
> • *recording the activities of workers by means of CCTV cameras, either so that the recordings can be viewed routinely to ensure that health and safety rules are being complied with, or so that they are available to check on workers in the event of a health and safety breach coming to light*
>
> • *randomly opening up individual workers' e-mails or listening to their voice-mails to look for evidence of malpractice*
>
> • *using automated checking software to collect information about workers, for example to find out whether particular workers are sending or receiving inappropriate e-mails*
>
> • *examining logs of websites visited to check that individual workers are not downloading pornography*
>
> • *keeping recordings of telephone calls made to or from a call centre, either to listen to as part of workers training, or simply to have a record to refer to in the event of a customer complaint about a worker*
>
> • *systematically checking logs of telephone numbers called to detect use of premium-rate lines*
>
> • *videoing workers outside the workplace, to collect evidence that they are not in fact sick*
>
> • *obtaining information through credit reference agencies to check that workers are not in financial difficulties.*

Before monitoring can be considered, there should be a clear policy in place. Employers should consider whether there is any less intrusive way of achieving the same result. Where employers wish to prohibit personal use of social media or the internet generally, a clear policy will normally suffice. If there is cause for concern, analysis of email traffic may be enough and is less intrusive then monitoring the content of messages.

Automated monitoring (through antivirus software, malware detection tools, blocking of certain sites and limits on the size of email attachments) are also less intrusive then monitoring.

> *3.2.7 If e-mails and/or internet access are, or are likely to be, monitored, consider, preferably using an impact assessment, whether the benefits justify the adverse impact. If so, inform workers about the nature and extent of all e-mail and internet access monitoring.*
>
> *3.2.8 Wherever possible avoid opening e-mails, especially ones that clearly show they are private or personal.*

3.2.9 Where practicable, and unless this is obvious, ensure that those sending e-mails to workers, as well as workers themselves, are aware of any monitoring and the purpose behind it.

3.2.10 If it is necessary to check the e-mail accounts of workers in their absence, make sure that they are aware that this will happen.

Key points and possible actions
• If e-mails and/or internet access are presently monitored, or will be monitored in the future, consider carrying out an impact assessment.
• Check that workers are aware of the nature and extent of e-mail and internet access monitoring.
• Ensure that e-mail monitoring is confined to address/heading unless it is essential for a valid and defined reason to examine content.
• Encourage workers to mark any personal e-mails as such and encourage them to tell those who write to them to do the same.
• If workers are allowed to access personal e-mail accounts from the workplace, such e-mails should only be monitored in exceptional circumstances.
• It may be practicable – for example when soliciting e-mail job applications – to provide information about the nature and extent of monitoring.
• In some cases, those sending e-mails to a work-place address will be aware that monitoring takes place without the need for specific information.

3.2.11 Inform workers of the extent to which information about their internet access and e-mails is retained in the system and for how long

The Supplementary Guidance to the ICO Code emphasises that accessing a worker's personal emails is particularly intrusive and should be avoided wherever possible. This principle is likely to apply to personal messages sent and received via Facebook and LinkedIn. In the case of Facebook, employees are likely to be able to argue that they have a genuine and legitimate expectation of privacy due to the personal/social nature of the site. Monitoring must be justified by a pressing business need that cannot be met through other less intrusive means. The only example given of a pressing business need in this context is work related criminal activity.

Deborah Nathan

Solicitor
Charity & Social Business Team
Russell Cooke LLP
Deborah.Nathan@russell-cooke.co.uk
0208 394 6437

May 2012

Deborah.nathan@russell-cooke.co.uk

Website: www.russell-cooke.uk