Social media in the workplace – a roadmap for employers

Martin Thomas (consultant and author of the *Financial Times Guide to Social Media Strategy*) & Katee Dias (senior employment lawyer at Goodman Derrick LLP)

The following paper is the summary of a workshop and discussion that took place at the offices of Goodman Derrick LLP on 23rd May 2019.

Recent incidents involving high-profile celebrities in the UK and beyond have served to highlight how the misuse of social media, in and out of the workplace, has created a new set of legal and reputational risks for employers. Broadcaster Danny Baker's tweet following the birth of the royal baby was interpreted as a racial slur and he was fired by the BBC; one of the world's leading rugby union players Israel Folau made homophobic comments on the basis of his fundamentalist Christian principles on Twitter and lost his Rugby Australia contract; Shila Iqbal lost her acting job on Emmerdale when historic tweets were discovered in which she had used racist language; and US film-maker James Gunn was dismissed by Disney for offensive historic tweets commenting on issues such as 9/11 and rape.

These celebrity misdemeanours represent the tip of an ever expanding iceberg. As the number of employee dismissals would testify, criticism of the company, bosses, work colleagues and customers and the sharing of confidential or inappropriate information on social media have become all too common occurrences. Take for example, the UK's largest employer, the National Health Service – according to figures released to The Times by 194 NHS trusts in England under freedom of information laws, 1,200 NHS staff have been reprimanded over their use of social media since 2013 and at least 65 NHS workers have lost their jobs due to their behaviour on social platforms or sharing private patient information. Another study by BMJ Innovations revealed that 97% of NHS staff have shared confidential patient information via non-secure messaging apps without consent.

Senior managers have also found themselves on the wrong side of the regulators by accidentally disclosing sensitive financial information through their tweets and posts. In most cases, these actions have been inadvertent, reflecting the all too common confusion between the private and public domain – people considering their comments as simply private conversations between friends. There is also what psychologists term 'the online disinhibition effect' – people say things on social media that they would never say in other circumstances.

Employers have a (non-legal) duty of care to their employees to ensure they use social media responsibly and safely in the workplace and in particular to highlight the dangers of over-sharing and disinhibited comment. They are unlikely to prevent the (hopefully rare) malicious act and an act of sheer thoughtless stupidity but pointing out the dangers and sharing cautionary tales of incidents in which people have lost their jobs (and risked damage to the reputation of their employers) should help focus minds.

Similarly, senior leadership teams are arguably failing in their corporate governance responsibilities if they do not take social media risk management seriously, which means explaining risks to employees, providing appropriate training for every employee, ensuring that appropriate monitoring systems are in place to identify potential risks and regularly reviewing systems and processes.

Social media and employment law

Even if an employee believes they are using social media in a purely private capacity - and despite the courts' recognition of the right to privacy and freedom of expression (enshrined by the Human Rights Act) - this usually offers little defence in the event of social media behavior that damages the reputation or rights of others or discloses confidential information. As far as the law is concerned, the fact that private comments on social media can be easily shared by others means that individuals can have no real expectation of privacy.

The challenges for employers are exacerbated by the relative lack of case law to guide when and how they should deal with inappropriate social media behaviour. The employment law specialists at Goodman Derrick LLP have pulled together a handful of cases in which an Employment Tribunal adjudicated on an employer's decision to dismiss an employee for misusing social media. These hopefully provide practical illustrations of how employers should respond to such incidents and avoid claims for unfair dismissal.

Trasler v B&Q (2012)

Mr Trasler posted some comments on Facebook while chatting with one of his Facebook friends. His comments were clearly linked to his work and he referred to "doing something he would regret" and "doing some busting but it won't be queues". He had a public profile and around 200 'friends' (of which around 45-50 were colleagues). Mr Trasler was not remorseful about the comments he had made but he had a clean disciplinary record and four years of service with the company. He explained that he had simply had a bad

day and it was his way of relieving stress. His employer acknowledged that nobody really felt threatened by the comments but dismissed him anyway because they believed that the way he had acted was contrary to their social networking policy.

The Tribunal found that Mr Trasler's dismissal was unfair. They said that despite being a technical breach of the employer's policy, it was key that nobody really felt threatened. They concluded that it was inappropriate conduct but did not warrant dismissal. A lesser disciplinary sanction should have been given instead.

Learning from this case: Although there might be a breach of the company's social media policy, an employer needs to assess the seriousness of that breach to determine whether a dismissal is an appropriate disciplinary sanction.

Teggart v Teletech UK (2011, Northern Ireland)

Mr Teggart was a customer service representative and he posted an obscene comment about one of his female colleagues on his Facebook page. The comment was made at home, using his home computer and in non-work time. It was read by some of his Facebook 'friends', which included some work colleagues. The female colleague about whom the comment was made was not a Facebook 'friend' but she heard about the comment and, via Mr Teggart's girlfriend, asked him to remove it. In response Mr Teggart posted a further lewd comment about her. His employer concluded that his behaviour was a breach of their Code of Conduct and Dignity at Work policies which prohibited harassment and unwelcome sexual behaviour. He was therefore dismissed.

Mr Teggart bought an unfair dismissal claim and contended that his human rights had been infringed, in particular his right to a private life.

The Tribunal concluded that Mr Teggart's **dismissal was fair.** They said that the finding of harassment was a reasonable conclusion for his employer to reach in the circumstances. In response to his arguments regarding his human rights, the Tribunal said that as soon as his comments were put on his Facebook page, he had abandoned any right to consider his comment as being 'private' for the purposes of human rights laws.

Learning from this case: Making arguments for privacy on the basis of human rights are unlikely to succeed.

Kurmajic v Sainsbury's Supermarkets (2018)

A Sainsbury's colleague posted a photo on Facebook of an incident that had taken place in the employer's multi-storey car park in which a car got stuck on the ramp. Mr Kurmajic commented on the post and added details of the driver's name, age (86 years old), address and the registration number of his car. He had 422 Facebook 'friends'. When the comment was discovered by his employer, the post was promptly removed. When questioned, Mr Kurmajic explained that he had posted the details because he was concerned about the driver's fitness to drive. When asked if he would do it again, he initially said that he would but then seemingly changed his mind saying "no, next time I would judge differently". Mr Kurmajic was 69 years old and had 12 years' service, a clean disciplinary record and had very recently been awarded the 'colleague of the year' award.

During the disciplinary meeting with his employer, Mr Kurmajic acknowledged that he was aware of the Social Media and Keeping Information Safe policies but explained that he had not studied their contents and he had not received any training about them. He was dismissed for gross misconduct. The colleague who had originally posted the photo received a final written warning, with the employer explaining that, as she had not shared customer information, it justified a lesser sanction.

The Tribunal found that the **dismissal was unfair.** They said that no reasonable employer could have decided on the available evidence that the conduct had brought the brand into disrepute. The Tribunal was influenced by the fact that the content of the policies were not known well to the employee. They explained that if policies exist which, if breached, expose the employee to a risk of dismissal, it is important that they are properly communicated.

Learning from this case: It is important to have good policies in place but also to bring these to the employee's attention. Regular training is sensible. An employer should also keep good records to be able to evidence this.

Gibbons v British Council (2017)

Ms Gibbons was employed by the British Council. The British Council's patron is the Queen and their scope of work is set out in a Royal Charter. A Facebook post was made by a band called the Dub Pistols, commenting on Prince George's birthday and containing obscene language. Ms Gibbons got involved in the Facebook conversation accompanying this post and added a comment about the Prince's privileged background. Ms Gibbons held Republican views.

The comment made by Ms Gibbons was made at her home during private Facebook chat. She had 150 'friends' who she knew well. Her privacy settings were set at their highest level and she had added disclaimer wording to her page, making it clear that it was not work related. Her post fell into the public domain and was widely reported in the media, causing an outcry for her dismissal. The British Council had a Code of Conduct in place emphasising that employees should not act in a way that undermines public trust in the organisation and had also issued social media guidance. Ms Gibbons was a very senior employee, well respected within the organisation and had an unblemished disciplinary record. As a charity, the British Council is required to report serious incidents but it did not feel that this was needed in these circumstances. However, following a disciplinary process, it dismissed Ms Gibbons.

The Tribunal found that the **dismissal was fair**. They held that Ms Gibbons had shown a reckless lack of judgement which was inexcusable for somebody in her senior position. Given that she did not act with attention and due care and caused damage to the integrity and reputation of the British Council, it was reasonable to dismiss her.

Learning from this case: Personal disclaimers and privacy settings provide no solid defence when it comes to making online statements that could be considered to bring the employer into disrepute. It may still be reasonable to dismiss an employee in these circumstances.

Benning v British Airways (2011)

Mr Benning was employed as cabin crew. During a period where strikes were being undertaken, he posted offensive postings on YouTube about strike breakers. This was in breach of a number of the employer's policies including their Dignity at Work and Bullying and Harassment policies. When questioned, he originally said that he did not have a YouTube account. He then went on long term sick leave and refused to participate in further discussions.

Eventually a disciplinary hearing was held at which he produced a letter from his brother which said that it was his brother who had posted the videos. He also produced a letter from his doctor stating that Mr Benning was suffering from depression and that this could have potentially contributed to his actions. Mr Benning had been employed for more than 15 years and had a clean disciplinary record. Nevertheless, the employer dismissed him.

The Tribunal found that the **dismissal was fair**. It was significant that Mr Benning did not show any remorse, he did not put forward the information regarding his brother when he

was first asked and the other postings on his YouTube account were consistent with the video in question. They felt that, on the evidence, it was reasonable to conclude that it was Mr Benning who posted the videos and that dismissal was a reasonable response.

Learning from this case: Whatever social media platform is being used (whether that is Facebook, YouTube, Twitter, LinkedIn, Instagram and the like) the same unfair dismissal principles apply.

Minimising and managing the risks

The problems created by employees' misuse of social media are exacerbated by a lack of planning, poor training and inadequate processes and policies. Conversely, the majority of problems can be avoided, anticipated or dealt with, so long as you have the right policies, training, monitoring and procedures. Unfortunately, many organisations are deficient when it comes to social media risk management. In a recent survey of UK workers, 61.2% either had no idea whether their company had a social media policy, or the company simply did not have one.[1]

Policies

Even where an organisation has a social media policy, it is often inadequate. A good policy includes the following elements:

- An explanation of why it is necessary. The key point to stress here is that the policy should be designed to protect both employer and employee.
- An explanation of how the employer defines social media in both a professional and private capacity.
- The areas in which employees should exercise particular caution. This is an opportunity to educate employees that there is no such thing as an entirely 'private' space in social media: whatever they say in social media might appear in public, even if they believe it is a private conversation.
- The regulations or codes that apply to the use of social media in a particular sector. For example, there are very clear rules governing what employees working in the financial services sector are allowed to say.
- The organisation's core principles when using social media. For example, you might want to ask people to be careful, be respectful of others, be thoughtful (i.e. think before you post or tweet or get involved in an argument), be transparent (always

[1] Pulsar Research for Viking, 2018

mention who you work for if you are tweeting, posting or commenting in a professional capacity).

- What the employer designates as 'inappropriate' use of social media. This will typically include sharing confidential business information, making negative comments about work colleagues or customers and making and sharing offensive remarks that have the potential to damage the reputation of the employer.
- The rules governing access to and the use of official company social media accounts.
- The protections that the employer will provide to the employee. For example, what happens if an employee using social media in a professional capacity experiences abuse from an irate customer or online 'troll'?
- The steps that the organisation will take when monitoring employee social media activity. This may include the provision of a whistleblowing system in which employees can report colleagues guilty of what they consider to be inappropriate use of social media.
- How the policy will be enforced. For example, the employer may demand the right to have any inappropriate material or comments removed.

It is also important to note that employees do not represent the only threat. Freelancers, temps and contractors can also create problems if they misuse social media – for example, inadvertently sharing confidential information about the organisation.

Training

Social media training needs to be comprehensive, documented (so there is proof that people have attended a training session, which could become important in the event of an unfair dismissal claim) and repeated to reflect the all too frequent changes to the social media platforms and what is considered best practice. For example, the growing popularity of WhatsApp to connect internal groups has created a new set of risks for employers. The encrypted nature of WhatsApp messages makes it difficult to screen what is being said and shared but it also possibly encourages employees to take unnecessary risks, especially when it comes to the sharing of sensitive data.

There is a danger that employee training places too much emphasis on risks. Rather than discouraging employees to use social media, smart organisations recognise that there are significant benefits from mobilising employees to become proactive and supportive sharers of appropriate corporate information. An employer's ability to harness the collective

reach of employees' personal social media networks is one of the easiest and fastest ways for any organisation to increase its profile and enhance its reputation with customers, clients, prospects, potential employees and other stakeholders.

Monitoring Social Media

Data protection regulations in most countries require employers to have a good reason to check their employee's social media activities. The employer must demonstrate that the monitoring of social media activities is reasonable, proportionate and 'relevant to the performance of the job.' Employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process the data'.[2]

Procedures

The organisational response to a case of employee misuse of social media should be swift – to hopefully minimise the reputational damage – but follow the correct employment law procedure. In those incidences where action is taken against an employee because of their inappropriate use of social media or for bringing the employer into disrepute, there is always the possibility, as outlined by the earlier cases, where the decision is reviewed by an Employment Tribunal. Typically, these Tribunals judge whether there is a fair reason to justify dismissal and whether the employer followed due process and acted 'reasonably', rather than whether the original tweet or post was appropriate in the circumstances. As an employer, your chances of successfully defending a claim for unfair dismissal will be enhanced if you are able to provide evidence of a comprehensive social media policy, proper training for all employees and a documented process - in one case the employer's case was weakened by the fact that it was unable to prove that an employee who had been dismissed had attended a social media training workshop.

[2] The guidance provided the Article 29 Working Party - an EU independent advisory body on data protection and privacy - may not sound like the most riveting of reads, but its ruling on the monitoring of social media in the workplace has huge implications for every business. It ultimately shapes how the data protection authorities across the EU will choose to apply existing data protection law to the use of social media monitoring. The UK government has agreed to adopt the same approach, so post BREXIT businesses in the UK will find themselves bound by the same legislation. In an effort to find *'the balance between the legitimate interests of employers and the reasonable privacy expectations of employees',* the Working Party put the onus on the employer to demonstrate that the monitoring of social media activities is reasonable, proportionate and *'relevant to the performance of the job'*. It also challenged the assumption that employers can legitimately scrutinise any publicly accessible data - *'employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process the data'*. The ruling is consistent with the direction of travel of EU data protection legislation which prioritises the rights and freedoms of employees above the interests of employers. The members of the Working Party are clearly concerned by the potential use of screening to collection *'information regarding their [employees'] friends, opinions, beliefs, interests, habits, whereabouts, attitudes and behaviours'* and the impact this might have on people's careers and job prospects.

The Financial Times Guide to Social Media Strategy: Boost your business, manage risk and develop your personal brand is published by FT Publishing International. It is available on Amazon here and from all good book stores.

Martin Thomas

martinthomasmarketing@gmail.com
www.linkedin.com/in/martinthomas-marketing
@martinmktg

Katee Dias

kdias@gdlaw.co.uk
www.linkedin.com/in/kdias
@EmpLawHeroes

GOODMAN DERRICK LLP