

Social Media Policy & Your Business

The recent coverage of the press surrounding the threats and insults directed at individuals, such as Cardine Criado-Perez, MP Stella Creasy and the classicist Mary Beard by so called 'trolls' on the internet have rekindled interest in the potential flashpoint of where employees behaviour on the internet potentially brings them into conflict with their employer.

Many of the recent press stories concentrate on the extreme examples of trolling and bad behaviour online. These include cases such as the notorious Reddit troll Violentacrez who was recently 'outed' by an investigator in Texas and subsequently lost his job (and a lot more besides). The tragic suicide of Hannah Smith demonstrates the appalling consequences of some of the abuse handed out by individuals on the internet. In this article we are not seeking to explain what motivates a certain individual to behave the way they do online. We are looking to focus on some of the employment and data protection issues which should concern your business and how you can proactively protect your business reputation.

Obviously the vast majority of employers, are not faced with such extreme and deeply unpleasant behaviour as described above, thank goodness. The problems lies in the defining of where the actions of an employee whilst online, particularly when using social media, become of concern to an employer. Individuals have a right to a private life outside work but many employers would act if an employee were found guilty of shop-lifting or drunk driving so where are the boundaries in terms of internet usage?

Firstly, there is no point attempting to stop all use of social media. You will fail. Given the role of social media in the marketing mix for many

companies, there is a very good argument to be had for viewing an attempt to stop all social media use as being counter productive.

What you need as a business are very clear and sound social media policies. Your employees need to be aware of them and the policies need to be updated on a regular basis to stay up with developments online.

It is impossible to monitor all of your employee's activities online all of the time. Education of the consequences of their actions is the way forward. They need to understand that once a comment is out there on the internet, it's out there permanently. Damaging words hang around. If you feel it is appropriate as an employer, provide a training program that clearly explains what is good and what is not and the possible consequences of getting it wrong to your business and the future employment prospects of the staff member. Training is also a good place to deal with questions about private vs. business use of social media.

This is also the time to address company policy on the sharing of confidential data plus also the wider data protection laws and employment law implications tied into internet use. For example, employees may become privy to personal information about clients or other third parties. It must be made clear to employees that any such information must not be broadcast via social media sites or accounts, whether company or individually owned, without the consent of the relevant individual.

To sum up the objectives for your business in terms of addressing social media use: i) It's not going to go away so don't ignore it, ii) If you incorporate clear policies and training within your corporate culture you create an initial line of defence against a negative online

discrepancy, iii) the continual dissemination of your policies on social media through updates and training, ensures that any employee who does go 'off piste' with their behaviour cannot later claim they didn't know what company policy was.

Along with the key considerations around confidentiality, privacy and defamation, employers must also ensure that they are fully aware of, and comply with, their obligations under the Data Protection Act 1998 (aka as the "**DPA**"). There are implications tied into the recruitment and advertising process on and off line but also employers have an obligation to existing staff. For example, an employer may have employee comments or social media updates they want to use for promotional purposes. In these circumstances, employers should be aware of how their employees' personal data is being used on social networking sites, as well as data relating to clients or third parties. Basically if an employer wishes to use the personal data of one of their employees on their social network site, they should always seek the consent of that person before putting the information online.

After an employee has departed (hopefully on good terms), employers need to be aware of their continuing obligations under the DPA even though the employment relationship has come to an end. These obligations apply equally to information held on social media sites or accounts.

If you were to believe much of the material circulated through the popular press, social media platforms would appear to be a huge risk to individual and business existence and success. In fact, if you proactively address the risks from the outset with new and existing employees and make sure you stay compliant with existing employment and data protection laws, social media will continue to be the excellent marketing tool it should be for your business.

rhw Solicitors LLP are able to advise on data protection, employee rights and wider employment law matters. Ensuring your terms of employment address all the areas that they should, with regard to use of social media and the wider internet is already key and will inevitably become increasingly important. As a business you should take professional advice from employment solicitors.

If you have any concerns or questions connected with any matter raised in this article or any other aspect of employment law, please contact either David Denovan-Smith or Richard Brown at rhw Solicitors LLP.

Phone: 01483 302000 e-mail: guildford@rhw.co.uk