Social media and compliance Part 1: Managing the risk

In the first in a two-part series looking at legal and compliance issues in social media, Ashley Hurst, Partner, and Jack Gilbert, Associate, at Olswang LLP suggest some practical considerations that should be borne in mind when establishing an effective corporate social media compliance framework.

Companies from a wide range of industry sectors are embracing social media like never before. Many are now coming to the view that enabling employees to blog freely and engage with social media networks is crucial in order to be able to exploit the corresponding commercial opportunities increasingly available through social platforms.

Whilst once the reserve of companies on the cutting edge of media and technology, social media is now a ubiquitous feature right across the corporate landscape.

Whether it be thought leadership on blogs, responding to customer complaints on Twitter, creating common interest groups on LinkedIn or setting up company pages on Facebook, many in even the most conservative of industries are beginning to join the social media revolution.

This represents a problem for compliance teams, who may in the past have opted to impose blanket bans on employees using social media at work rather than expose the company to the potential risks that it can bring.

Indeed, particularly for those in regulated industries such as financial services and pharmaceuticals, the thought of giving employees carte blanche to use Twitter and Facebook at work is enough to give many lawyers and compliance officers sleepless nights.

As use of social media becomes ever more prevalent, however, companies are realising that the opportunities to enhance brands and build relationships are just too good to miss.

How, then, can firms embrace these opportunities whilst protecting themselves against this exposure? What are the challenges of formulating an effective compliance framework that is consistent in its application, and flexible enough to deal with the needs of individual teams and departments?

Defining the risk

Examples of social media policies are easy to find, and indeed there are many tools online which allow you to build your own policy simply by ticking a few boxes. However, compliance officers should think very carefully before borrowing ideas from elsewhere.

An effective social media policy is one that has been drafted with the individual needs of the company in mind, and there is no one-size-fits-all solution.

The potential risks of social media will vary greatly from company to company. The first step should therefore be to identify the key risks to the company in question, and agree upon what the social media policy should achieve and what it should protect against.

There are certainly many concerns that will apply across the board.

Will allowing employee access to Twitter increase the risk of hacking by fraudsters? Should the company pre-moderate or post-moderate user comments on the company blog? Can the company be liable for those comments? How, and for how long, should social media communications be retained? Can employees take their Twitter and LinkedIn accounts with them on exit?

Of course, the answers to some of these questions will simply come down to the approach employers may wish to take with regard to internal strategy and issues of employment law, and these are considered in more detail in the next article in this series.

In addition to these, some concerns will be specific to certain companies – and under the watchful eye of industry regulators like the Financial Services Authority, those subject to regulatory regimes require particular thought.

For example, can a financial services company use a tweet as part of a marketing campaign for a new financial product? When will a tweet about a financial product

be considered to be a financial promotion?

What is universal is that the risks must first be identified before an effective policy can be developed. Only then can companies ensure that the policy will be fit for purpose, and can be monitored effectively going forward.

Joined-up thinking – preparing a policy

Most large companies now provide social media policies and/or guidance to their employees, often in the form of lengthy documents. Such documents, though, should not operate in a vacuum.

There is a tendency for social media policies to be drafted by various combinations of the legal, communications and social media teams, and the end result can sometimes be inconsistent with other internal policy documents such as the group communications policy, the employee handbook, the data retention policy and he data security policy.

Consistency across the board is key to avoiding confusion and legal disputes.

A distinction should be made between policy and guidelines, which should each have a clear objective and should not be confused. Whilst a social media policy should lay down rules that employees should abide by when using social media, guidelines should serve to give advice and suggestions as to how employees should go about this task.

These documents should be drafted with on-going effective compliance in mind, and once drafted, communication of the compliance framework and the training of staff are vital to ensure effective compliance.

It is unrealistic to expect employees to take time out of their busy days to read 20 pages of social media guidance.

Companies therefore need to find ways of distilling these documents into key points and must ensure that those charged with monitoring and contributing to social media discussions have had the right training to enable them to make sound judgments in the heat of the moment.

"for those in regulated industries such as financial services and pharmaceuticals, the thought of giving employees carte blanche to use Twitter and Facebook at work is enough to give many lawyers and compliance officers sleepless nights"

And as the world of social media never stops turning, on-going training and monitoring are essential. Old platforms die and new ones take their place at a tremendous pace, and in the process policy requirements will change. The compliance framework should therefore be seen as a living document, and as it evolves this too should be identified and communicated to employees.

Crisis management

One of the biggest risks posed by social media is the speed with which it moves, and companies are often caught out by how quickly mistakes can 'go viral'.

For some companies, problems can escalate to a global level in a matter of hours, and the damage can be considerable. In a report last July by US data security firm Symantec, it was estimated that social media mistakes cost major corporations around the world an average of $4.3 million each in 2010, as a result of PR disasters, lawsuits, regulatory fines, loss of revenue and reductions in share price.

As such, effective crisis response procedures are vital, particularly when external moderation companies are used.

When a crisis breaks, there simply isn't time to spend several hours deciding how bad the problem is, whether to respond, who should respond, and who needs to authorise the response. By the time this is done, it is likely to be too late and the potential costs will be even greater.

10 Step Plan

When devising a social media strategy, companies should therefore also consider implementing the following 10 step plan:

- **Step 1** – Identify key internal stakeholders and form a social media focus group
- **Step 2** – Identify what your organisation wants to achieve through employee use of social media
- **Step 3** – Identify the relevant social media channels
- **Step 4** – Identify the key legal risks for your organisation
- **Step 5** – Collect existing policies which may impact on employee social media
- **Step 6** – Form a clear view of the desirable/acceptable bounds of social media use and draft a strategy document
- **Step 7** – Draft/amend social media policy and guidelines as appropriate
- **Step 8** – Form a crisis team
- **Step 9** – Establish a training plan
- **Step 10** – Build an integrated online communication network for crisis response

(Continued on page 4)

(Continued from page 3)

Care should also be taken to establish whether any industry-specific requirements also apply.

Last year, the US financial services regulator, FINRA, issued a regulatory notice providing social media guidelines to regulated firms. This includes recommendations to retain records of all social media activity, to avoid recommending securities on social media platforms, to obtain approval from compliance departments on blog posts, to establish policies and procedures regulating social media activity, and to provide evidence that such policies are enforced.

In the UK, the Financial Services Authority has so far adopted a fairly light-touch approach to social media and has restricted its guidance to financial promotions, but it is surely only a matter of time before it follows a similar path to FINRA, and there is also potential for other industry regulators to follow suit.

Now is therefore the time to put the compliance framework in place and embrace the opportunities that this new form of communication can provide.

How do social media policies protect employers and what should they cover? To what extent can companies lawfully monitor employees' and job applicants' use of social media? Can anything be done to harness employees' online contacts, and who owns an employee's social media presence on exit? In Part 2 of this series, Melanie Lane and Catherine Taylor, partners at Olswang LLP, will highlight some of the key employment law issues that arise out of the use of social media, and the approaches employers can take to manage the risks.

Ashley Hurst and
Jack Gilbert
Olswang LLP
ashley.hurst@olswang.com
jack.gilbert@olswang.com