Social Media Policies for Business

White Paper

APSCo

SITEFORUM
Social Networking for Business

Osborne Clarke

Social Media Policies for Business

Summary

- **Social media usage is currently largely unregulated** and while this remains the case businesses need to find a way of protecting their business and their employees whilst making the most of the opportunities social media undoubtedly offers

- **Improper use of social media can result in serious damage** to your business as well as the possibility of legal dispute. Key risk areas include loss of valuable business assets, reputational damage and regulatory breaches. .

- **Recruitment businesses can protect their information** by implementing clear social media policies so that everyone knows where they stand.

- **Applying clear policies and monitoring the use and performance of social media will help minimise the risks** to your business and improve your chances of enforceable legal protection. Where employees ignore and breach policy and contractual protections, employers should consider taking appropriate action to safeguard their business interests

- **Social media can offer great opportunities for businesses** to develop their own solutions to engage with candidates and clients, offering brand building, more focussed content and communication, data ownership and control and reduced reputational risk. For many, the ideal solution could be to develop your own branded online community which has appropriate automated links to major social media sites.

Social Media Policies for Business

1. Introduction

The recruitment industry increasingly relies on social media for networking, news and information but such opportunity has grown in the absence of clear regulation exposing recruiters to challenges around protecting business assets and value. The time has come for industry to respond to these changes.

Government has been understandably reticent about regulating social media and we want to show how trade associations like APSCo, can take a lead, self-regulate and provide support to businesses, large and small, in addressing this challenging and dynamic environment. This White Paper is designed to help business leaders develop informed social media policy.

2. Background

The communications revolution gathers pace - never before have so many people communicated so much so often.

Generation Y and Generation Z will automatically use instant messaging rather than email, text messaging rather than voice calling and share personal data about their lives in a page on a social network.

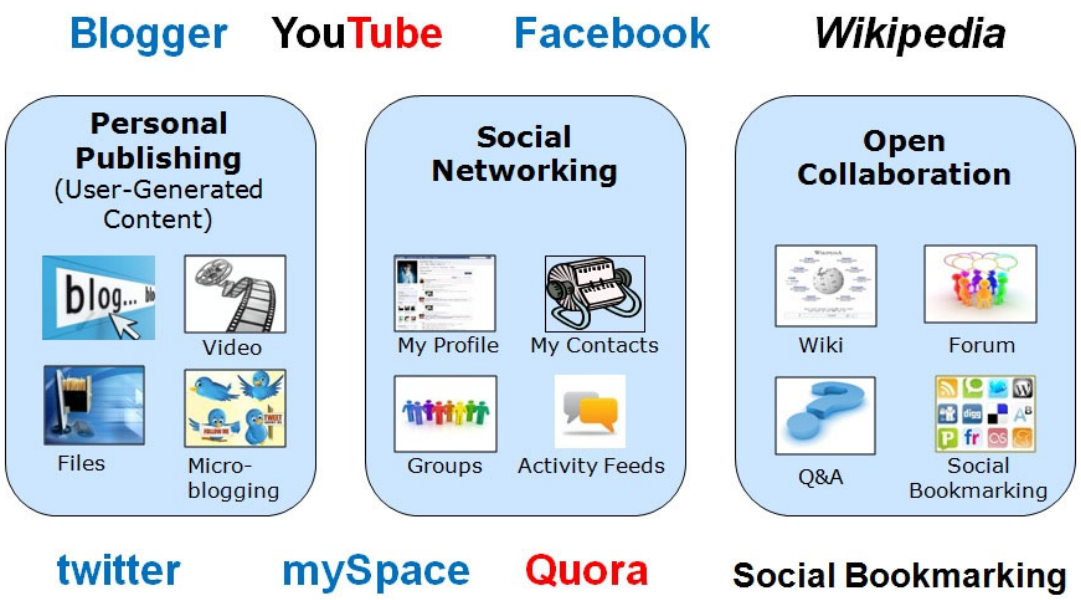
Even today, the volumes of information are staggering: 900,000 blog posts, 50 million tweets and more than 60 million Facebook updates every day.

Like it or not, the business world is well and truly online and inextricably linked with this communications revolution. All this can be considered progress, but the rules of engagement in this brave new world are far from clear.

Good business management requires clear strategies for successful online engagement, with clear guidelines and policies to manage potential risk to companies and their employees.

3. Social Media Platforms

The 3 main components of social media to consider are:



Personal Publishing. Essentially the start of the interactive web experience as blog services became freely available. Individuals were able to push their own content out to a potentially unlimited audience. Since supplemented by micro-blogging services such as Twitter and Facebook postings where people can post snippets of information including links to their Twitter Followers, Facebook Friends or network connections on sites like LinkedIn or Xing. On some platforms this is extended to include the ability to publish documents to targeted groups or the whole community.

Although the direction of communication is principally a broadcast from the author, interactivity is enabled via comments from other readers and sometimes the facility to rate an item. Content may be shared more widely via a variety of social mechanisms including bookmarking services.

Social Networking. For many this term is synonymous with LinkedIn which has become the industry standard in many parts of the world. For leisure and consumer purposes this space is dominated by Facebook. Users connect with others via their social profiles and are able to establish a unique personal network to which they can send updates and from which they can observe activities of their contacts/friends. It is a people-centred environment rather than content-centred and this "social" model is already being viewed as a central component for more effective working inside organizations as well as for keeping in touch with contacts.

Open Collaboration. Possibly the most exciting aspect of social media has been the ability for groups to work together more effectively and co-create IP for the good of the wider community. In stark contrast to the owned documents of the Microsoft era, tools like forums, wikis and more recently Q&A environments have opened up communal collaboration. The most widely used examples of these are LinkedIn Groups and Facebook Groups which can be quite close-knit communities - although successful groups can quickly become large communities in their own right.

4. Areas needing protection

There are a number of areas for recruiter to consider regarding managing business risk.

Business value. A substantial part of most recruitment businesses is derived from their client and candidate contacts. Ensuring that protection is in place to retain ownership of contacts that employees create using social media within the course of their employment is now of paramount importance. Failure to do so may lead to the business losing significant value if an employee leaves and takes these contacts with them. Perhaps more importantly, a potential buyer may consider lowering its asking price for the business if efforts to protect contact ownership are regarded as inadequate.

Brand & Reputation. It is important that business policy and strategy is properly represented online so that all communications and responses are aligned with the business and legal or other issues are avoided. This can be particularly challenging in fast-moving and/or high-profile scenarios, where even quite small incidents can quickly mushroom into major PR incidents.

Staff Identities. Recruitment businesses typically rely on consultants to take on customer facing roles and need to be aware that they are potentially investing a lot of power and responsibility in these people. They may become targets for talent acquisition by other businesses or, for negative communications from disgruntled customers or employees. Social profiles and activity may even be used as a source of intelligence by competitors e.g. monitoring their contacts and activities, not just in their official capacity. Since all online activity is easily accessible, travel plans, meetings, personal preferences and even social connections can all be examined. In the recent UK phone hacking scandal, government members' Facebook friends were queried as proof of potential collaboration/influence.

Regulatory issues. Recruitment businesses whose staff deal with customers via social media may be conducting regulated business in a non-protected environment: Is sensitive personal data being collected and stored for the employer on a networking site? This could be contrary to data protection law. What about sales activity via social networking sites, where such activity is subject to strict regulation such as recruitment and financial services? Allowing employees to operate via new media, outside the normal IT systems of the employer may place employers in serious breach of various regulatory regimes.

Confidential Information. In many situations advice or expertise may be shared and care must be taken to avoid inappropriate sharing of commercially sensitive or confidential information. Informal communications online can be seen by infinitely more people and again are easily accessible in the future. Safeguards must be in place to ensure all employees have clear knowledge of what can and can't be discussed online, whether or not they have customer facing responsibilities.

Intellectual Property. Social media communications may also include images and media materials which have been created by the business. IP owners should assume these will be widely shared. Consequently steps should be taken to implement appropriate branding and disclaimers to cover as many potential usages as possible. Re-use can have many advantages but this needs to be protected by appropriate copyright and brand protection.

5. The need for social media policies in the work place

Best practice advice says: Businesses of all sizes should have a properly drafted policy covering the use of their computer systems and technology, whether they are used on business premises or by employees at home or when travelling for business. The policy should include a specific, express waiver by employees to any right to privacy in information contained on the computer. The policy should also eliminate any expectation that information or communications are confidential to the employee and acknowledging the employer's right to access their computers at any time to review and monitor the contents. However, employers should restrict this access to occasions when there are valid business reasons for doing so, such as when there is a reasonable suspicion of work-related misconduct by the employee or regulated activity which the employer has a duty to monitor.

Employers should also consider clearly stating that all computers are company property and should not be used in any disruptive or offensive ways, such as communicating sexually explicit content, ethnic or racial slurs, or to discriminate, bully

or harass others. Employees should be notified that their employer deems all computer content permanent and subject to retrieval and review at any time.

Recruiters also need to ensure that temps and contractors comply with their clients' computer and system usage policies.

6. Understanding public social media platforms

"*If you are not paying for something, you're not the customer; you're the product being sold.*"

Andrew Lewis under the alias Blue_beetle on the web site MetaFilter.

So what about privacy? This has largely been covered by the use of "Opt In" controls which require the user to confirm they have read and understood the terms of the service before they are able to use it. Unfortunately these are now so complex and numerous that most users have neither the time nor expertise to give these the consideration they require and deserve.

The terms and conditions or a platform's usage policy can and do change quite regularly and, of course, the user has no recourse other than to stop using the service. In many industries including recruitment, the user would have to consider what impact could this have on their business.

Businesses should not assume that service and/or pricing will remain constant – these are still relatively immature business models, so substantial changes may be ahead. It is unlikely that legislation would be introduced to limit change, which means that the clearest route to resisting such change could be on the grounds that the platform's actions are anti-competitive or in restraint of trade.

Another consideration for every social platform is that they can be abused by third parties in a variety of legal and illegal ways. Programs can replicate user behaviour and, armed with a valid user account, quickly and efficiently access all available contact accounts and harvest their data. Businesses cannot assume that online services provide any guarantee of security:

"***That profile, that picture, that browsing habit or that buying pattern makes this generation the easiest and more importantly the quickest, target for fraudulent misuse of identity since the practice began***." *Computer Fraud and Security November 2011*

Individuals and business leaders must understand and accept that it is an imperative for any online service to be able to supply their services and cover their costs while making a profit for their shareholders. We can benefit from these services but we should not presume they are mature, stable or secure. Whilst money may not have changed hands, your participation in the service represents a level of investment and "caveat emptor" still applies.

7. Where Next? Beyond LinkedIn

Many companies have started to look beyond the major social platforms to see how they can exploit these new communications tools to drive more value but with less risk and commercial trade-off.

Social platforms offer opportunities for businesses to develop their own custom solutions. A number of large employers have implemented networks for internal staff collaboration with surprisingly effective results. A recent Gallup poll showed that by using social business tools, employee satisfaction was increased. This equated to improvement in a number of KPIs including: productivity (+50%) , employee retention (+50%) and customer loyalty (+56%).

Large employers are also now replacing job sites with recruitment portals which they can use to build relationships with a significant group of potential applicants. Some organizations have built alumni networks to stay in touch with talent who can generate referrals and may consider re-employment in the future.

One solution is to develop your own branded online social presence which is seamlessly linked to the appropriate major social media sites giving you the best of both worlds. Specifically your owned presence builds your brand and can host more focused content and communication whilst retaining control and reducing risks.

Example social community for recruiters

Social technologies have created new process models in a number of business areas:

Social Sales. Engagement (communication and interaction) technologies such as customer communities, virtual tradeshows and online chat (all used by HR.com) create new channels for selling to individuals.

Social Marketing. Using social media (especially personal publishing), to build brand recognition and product familiarity through regular messaging and conversations in key related areas.

Social Customer Service and CRM. Using social channels to listen to customer feedback and respond in real-time. Also using online collaboration to allow customers and/or staff to communicate and create useful knowledge bases which allow faster access and self-service.

Social Recruitment. The recruitment industry has been transformed by online access to professional profiles and LinkedIn. In addition to highlighting potential candidates, social sites are regularly searched to provide background and/or reference checks. There is also evidence now of attempts by social networking sites to monetise recruitment, disintermediating traditional recruitment companies.

8. Who is responsible for social media policy and implementation?

Where use of social media is being encouraged as a lucrative route to market business leaders must take responsibility for protecting all personal and business reputations and data affected by their activity.

Business managers should not assume this is covered elsewhere and although HR and/or marketing may have developed some guidelines there is very little external regulation or guidance about the use of social media at work and/or its impact on businesses. Ultimately HR, marketing, legal and IT groups are all likely to have some influence in the creation of a social media policy and its successful implementation.

9. Ways you can protect your business's value

Businesses which actively encourage social networking as an integral and important selling tool need to develop and implement their own social media policy. This policy should protecting the business's own reputation and data and also the reputation and associated data of their staff, clients and candidates as well third party contacts such as suppliers.

The recruitment industry has embraced the use of social media as an effective tool to directly and indirectly expand its sales, brand and reputation. This means that the online network of personal “relationships” developed and information gathered by just one recruitment consultant can be potentially huge and the personal and commercial sensitivity of information gained and exchanged unprecedented. However, there often experience a distinct lack of clarity as to how best to protect this valuable information. The industry needs to invest time and thought into educating its business leaders and staff in the art of online brand management, as well as internet recruitment. Having an effective and well implemented social media policy as well as recruitment- business specific restrictive covenants has now become critical to each recruitment business's future profitability and potential sale value. Recent cases have shown that the English courts are now more likely than ever before to recognise a recruitment business's interest in protecting its contacts and confidential information and we know that the prospect of successfully protecting information can be dramatically improved by having clear and well implemented social media policies and restrictive covenants in place. It seems that the courts now recognise that recruitment businesses need to invest in compliance but are unlikely to do so unless they have a reliable way of protecting their business assets.

A policy should focus not only on the protection of a business’s own IP and client relationships but also protect against unwanted use of confidential or personal data by identifying what sort of information may be commercially or personally sensitive. It should also put safeguards in place to regulate the communication of such information from a business to an actual or potential client, candidate or third party supplier using social media.

Businesses which promote the use of social media by their staff may be considered as having a moral responsibility to protect such staff from the very medium they have encouraged them to make part of their daily business routine. Clear procedures will allow staff to easily identify and guard against seemingly innocent online activity, which could have serious implications for both staff and the businesses which employ or use them.

A social media policy should also make clear the extent to which computer use, including the use of social media, is monitored to ensure compliance with regulatory obligations such as data protection law or industry specific regulation such

as the Conduct of Employment Agencies and Employment Businesses Regulations 2003 . This policy should be drafted carefully to ensure that the policy regarding monitoring is itself legitimate.

An additional consideration regarding social media is whether there is a business or reputational opportunity to provide guidance and best-practice from a customer facing perspective? For example, recruiters could consider adopting industry standards to make life easier for candidates e.g. transferrable profiles (i-Profile) and could also consider the steps they can take to educate candidates such as explaining that CVs submitted to job boards are likely to be widely circulated or providing recommendations on the use of Facebook privacy settings. A working group might produce recommended candidate guidelines for the positive use of social media and how to avoid becoming visible for all the wrong reasons.

10. Understanding key risks

By understanding how their employees' use of social media can affect their business, employers can take steps to minimise the potential risk this practice may present. Employers need to be aware of what issues social media can present in the work place, which may include some of the following points identified as being key risks:

Reputational issues. Negative or critical commentary about a business by a member of staff which is made during or out of work time can have a negative impact on the reputation of the business. If a member of staff can be identified as working for a particular business, their perceived or actual behaviour through social media may bring the business into disrepute.

Defamatory postings. Content posted by employees which has the purpose of demeaning a client or competitor could result in the injured party bringing a defamation claim against the employer. At the click of a button, publicity can be gained for all the wrong reasons leaving both employer and employee in the firing line.

Cyber-bullying. Like other forms of bullying, this can include employees posting abusive content about their colleagues, as well as social exclusion and non-cooperation. Cyber-bullying can lead to an employment tribunal claim against the perpetrator's employer if the tribunal decides that the employer was responsible for the individual's actions. Employers may be liable if they do not take steps to prevent behaviour which constitutes discrimination, harassment or victimisation in the workplace.

Loss of business value. Businesses whose value lies in the information they gather in relation to client contacts are at risk of losing some of this value where they fail to take steps to protect the ownership of contacts which are built by an employee in the course of their employment. Networking sites such as LinkedIn present employees with the opportunity to maintain their client contacts externally and exploit their employer's client information for their own benefit if they leave and go into competition.

Misuse of client/personal information. If confidential information is disclosed through social media then this could put an organisation in breach of their confidentiality obligations in other contracts. Personal data, which includes anything which on its own or together with other information identifies an individual, is subject to strict processing requirements under the Data Protection Act 1998 and other local equivalents. Any personal data communicated through social media will be subject to restrictions imposed by regulation.

Monitoring use of social media during work time. Employers should make clear their policy on non-work related internet use. Employers that do allow non-work related access should consider whether they want to outline what amounts to acceptable use, the types of websites that employees may access and the length of time that they may spend on the internet in a non-work capacity. Employers may need to monitor their use of such sites to establish whether or not employees are complying with various regulatory obligations and/or any social media policy. The scope of any monitoring must comply with a range of legislation including the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

11. What should a social media policy cover?

The absence of clear rules surrounding employee use of social media can cause problems for employers needing to take action against misuse. If an employee is dismissed due to their use of social media and there is no clear policy in place, there is a risk that the employee may bring a claim for unfair dismissal against the employer. This is why it is essential that a carefully worded social media policy is teamed up with the employer's disciplinary policy. Given the importance and implications of these policies for recruitment businesses they should be reviewed by specialist advisors with experience of advising recruitment businesses.

A social media policy should set out:

- the risks (to the employer and employee) attached to posting negative content on social networking sites;
- what is, and what is not, acceptable in terms of references to the employer on social media sites;
- staff requirement to back-up online contacts and member lists from any LinkedIn Group(s) by requiring them to submit such information to central storage on a regular basis;
- that the employer will take disciplinary action against employees who use social media in a way that is potentially damaging to the business;
- rules on accessing social media during working time;
- that cyber-bullying amounts to harassment under the harassment policy;
- measures that an employer will take to protect confidential information relating to clients; and
- rules and guidance relating to employees' use of social media to promote the business in the course of their work, including ownership of data.

It is important to consider how "confidential information" is defined within the employees' contract of employment and whether this covers client contact data. Restrictions should also be imposed on an employee during and for a limited period following their employment to prevent them from using confidential information at a competitor or to set up in competition with their employer. These clauses require specialist advice from an advisor with experience of providing enforceable legal protection for recruitment business assets.

12. Call for Action

For recruiters this involves asking:

- What do we believe is the market norm in our sector and where do we want to be in comparison? Who do we want to reach and why?
- What are our candidates' and clients' current levels of social media activity?
- Are our communications skills and resources good enough to deal with this type of engagement?
- Who in the organisation needs to be involved in this?
- What are our measures for success?

Be ahead of the game. Relationship management has never been so possible and so valuable. Social media can offer great opportunities for businesses to develop their own solutions to engage with candidates and clients, offering brand building, more focussed content and communication, data ownership and control and reduced reputational risk. For many, the ideal solution could be to develop your own branded online community which has appropriate automated links to major social media sites.

Next steps should be the implementation of a Social Media Policy and to start this today, contact the partners in this white paper for details on how to achieve the right results.

With input from Osborne Clarke