eBook: An Employer's Guide to Managing Social Media Risks in the Workplace

Sydney Level 4, 179 Elizabeth Street, Sydney NSW 2000 T: +61 2 9299 6105 F: +61 2 9299 2805

Perth Suite 20, 7 The Esplanade, Mount Pleasant, WA 6153 T: +61 8 9288 1826 F: +61 8 9288 1827

Melbourne Suite 203, 35 Whitehorse Road, Balwyn, VIC 3103 T: +61 3 8582 0980

contactus@complispace.com.au www.complispace.com.au CompliSpace Pty Ltd ABN 24 099 302 655

About the Author

James Field is the Managing Director and founder of CompliSpace. He is a highly experienced business executive and legal and corporate governance practitioner, with over 25 years experience in the design and implementation of enterprise corporate governance programs across a wide range of industry sectors.

James has held senior executive positions in a range of publicly listed and private companies and applies his hands-on executive experiences to assist CompliSpace clients to develop lasting governance solutions that work.

James has been a qualified legal practitioner since 1986. He is a Fellow of the Chartered Secretaries of Australia and a member of the Australian Compliance Institute, the Australian Institute of Company Directors and the Australian Human Resources Institute. James is also an approved AUSTRAC External Auditor.

About CompliSpace

CompliSpace is a leading provider of tailored corporate Governance, Risk and Compliance (GRC), Human Resources and Workplace Safety services to organisations across Australia. Our focus is on assisting clients to implement sustainable solutions using cost-effective enabling technologies.

CompliSpace delivers industry specific web-based policies, procedures and workflow management tools that can be quickly tailored and configured to suit an organisation's needs. These are kept up-to-date with key legal and regulatory changes by our team of subject matter experts, to provide a platform for sustainable growth in the ever-changing governance landscape.

For more information visit www.complispace.com.au or call 02 9299 6105.

Table of Contents

Introduction

The use of social media is growing rapidly around the world. Take a moment to absorb these statistics. Every minute of every day:

- 100,000 tweets are sent
- 684,478 pieces of content are shared on Facebook
- 48 hours of video are uploaded to YouTube
- 47,000 apps are downloaded from the App Store
- 3,600 photos are shared on Instagram
- 571 websites are created (source: AllTwitter)

> "40% of people spend more time socialising online than they do face-to-face."
>
> (source: AllTwitter)

With the increasing prominence of social media in our everyday lives, it's of no surprise that social media is significantly impacting day-to-day business operations, as well as workplace relations. The key question is: How can employers effectively manage their social media risks?

Whether an organisation embraces social media, or tries to ignore it, the one thing that is certain is that it is only a matter of time before social media will impact your business. As an employer you need to understand the potential risks to your business posed by social media, carefully consider potential consequences, and take steps to manage these risks.

This eBook is designed to help employers understand and manage their social media risks. It provides examples of potential risks with suggested responses and, importantly, explains why a social media policy will only be effective if it is part of a coordinated and properly documented human resources and general management strategy.

Chapter 1: What Are Your Risks?

The use of social media is growing rapidly around the world. Combined with the use of new smart phone technology, social media is, for many people, blurring the lines between their work and private lives in ways that are legally complex and difficult to control.

"As an employer, it's only a matter of time before you will have to deal with a social media incident."

The law, as always, lags behind the complexity of the commercial situation that employers now find themselves having to deal with. Some scenarios to think about:

- An employee associated or identified with your organisation announces to their social network, which includes many work colleagues, "*Work sucks, I can't stand it anymore.*"
- You decide not to employ a candidate because, using Facebook to do background checks, you discover comments made which you consider offensive to your religious beliefs.
- A senior manager, with authorised access to your corporate Twitter account, leaves her phone on a table at a party without PIN security. One of her friends, after having too much to drink, thinks it's funny to publish a derogatory tweet on her account (which turns out to be the company account) causing a backlash against the company.

The list goes on. In fact the possibilities are nearly endless. As an employer, if you have not already thought about your social media risks you are likely to have a nasty surprise coming your way, maybe not tomorrow, or next week, but it's only a matter of time before you will have to deal with a social media incident.

The following table provides a sample of social media risks that employers may face, with suggested mitigating responses. As you go through this list, ask yourself this question: *"What is the likelihood of this happening in my organisation and how would it affect my business if this was to occur?"*

The bottom line is that social media is here to stay and employers who ignore it, and the implications that it has for their organisations, are simply sticking their collective heads in the sand.

Social Media Risk	How Do You Mitigate Your Risk?
Failure to engage in social media marketing for fear of negative exposure (this may be a missed opportunity and a real risk).	• Social Media Strategy • Social Media Policy • Internal Communications Strategy
In trying to defend your organisation in an online forum, a staff member makes a comment that offends other users and leads to complaints and reputational damage.	• Social Media Policy • Staff Training • Discipline & Termination Procedures
A disgruntled client/customer starts to post negative comments across social media sites and industry forums.	• Complaints Handling Program • Social Media Policy • Staff Training
An employee, whose Facebook page identifies him/her as working at your organisation posts on his/her facebook page, which is visible to work colleagues, "Work sucks, I can't stand it anymore."	• Social Media Policy • Staff Training • Discipline & Termination Procedures
An employee fails to secure their smartphone, or tablet computer. This is then accessed by an unauthorised third party who posts derogatory comments on your organisation's Twitter account.	• Information Security Policy • Staff Training • Discipline & Termination Procedures
An employee sets up a LinkedIn group in her own name, which she managers in work time to attract customers. The group attracts thousands of members. The employee takes the group with her when she leaves to go to a competitor.	• Employment Contract covering intellectual property ownership and restraint of trade provisions • Confidentiality Agreement • Social Media Policy
An employee posts confidential information to a social media site (either deliberately or inadvertently).	• Employment Contract • Confidentiality Agreement • Social Media Policy • Staff Training • Discipline & Termination Procedures.

Chapter 2: Managing Your Social Media Risks

So the burning question is "How do employers manage their social media risks?" Draft a social media policy, we hear you say... If only life was so easy! The concept of a standalone "social media policy" is actually a misnomer.

> "If you are serious about managing social media risks, you must get serious about developing a coordinated corporate governance and human resources management strategy."

It's clear from the sample of risks provided in the previous chapter that implementing a social media policy will not mitigate an employer's risk on its own. To be effective a social media policy must be part of a coordinated and properly documented corporate governance and human resources management strategy. As the types of social media risks vary, so do the strategies for mitigating these risks.

Let's take this concept a little further. Take a simple example – an employee posts a negative comment about your company, and a manager, on their Facebook page. In this situation, the employer's first line of defence may be a well drafted **Employment Contract** which includes a non-disparagement clause and highlights the types of behaviours which may lead to summary dismissal.

The employer's position could then be further strengthened by having:

- A clearly defined **Internal Grievance Procedures Policy** (which the employee didn't use);
- A **Social Media – Personal Usage Policy** which refers back to the employment contract and reiterates the fact that posting negative comments about the organisation and work colleagues is not acceptable behaviour;
- An **Internal Training Program** which covers personal use of social media;
- Robust **Record Keeping Procedures** to evidence staff training in the organisation's policies and the employee's knowledge of these policies; and
- **Discipline and Termination Procedures** to ensure that when the social media event occurs, management is well-versed to manage the situation following principles of substantive and procedural fairness.

Other documents, programs, policies and procedures which may come into play include, but certainly are not limited to:

- Anti-Bullying & Harassment and Anti-Discrimination Policies;
- Staff Performance & Development Review Programs;
- Recruitment & Selection Procedures;
- Privacy Policies;
- Information Security Policies;
- Email and Internet Usage Policies;
- Confidentiality Agreements; and
- Complaint Handling Programs designed to efficiently capture and resolve customer complaints before they hit social media forums.

If you are serious about managing social media risks in your organisation, you must get serious about developing a coordinated corporate governance and human resources management strategy, that not only includes documented policies and procedures, but also an internal training program and robust record keeping procedures.

Chapter 3: Two Social Media Policies, Not One?

Once you actually sit down to draft a Social Media Policy one of the first things you will notice is that you are most likely going to have to draft two policies, not one.

The obvious policy that all businesses will need is a Social Media Personal Usage Policy which provides guidelines to staff when they use their own personal social media accounts.

Secondly, if your organisation has a social media presence, it will need to develop a Social Media Business Usage Policy. The purpose of this policy is to set guidelines with respect to the administration and/or publication of content on your organisation's own social media platforms. This is designed to promote your brand, but also protect it from reputational damage, breach of copyright and other pitfalls.

The policies will have a number of things in common. For example, they should both provide a broad definition of "social media", which should be left open to include new forms of social media that will undoubtedly emerge in the future. They should cross-reference each other and they should also be accompanied by a training course which will be used to effectively communicate the content of the respective policies to staff.

Chapter 4: Designing A Business Usage Policy

How you design your Business Usage Policy will, of course, depend on the social media platforms your organisation uses and its views as to the level of control it wants with respect to material published on its branded social media sites.

One simple way to encourage all staff to contribute to social media publications, while maintaining control, is to establish simple procedures for staff to submit their publication ideas, while simultaneously only allowing authorised staff to actually publish content on your branded social media sites. Put simply, staff are prohibited from publishing content unless they are specifically authorised to do so.

The first dilemma you will come up against is that each form of social media has different attributes which potentially require different authoring and publication skills. For example, publications on Twitter tend to be high volume and conversational. Blogs, on the other hand, tend to be published less frequently, require a higher level of authoring skill, and will often provide advice or opinion.

To accommodate these variances, individual authorisations will need to be tied to particular forms of social media e.g. one staff member may be authorised to publish on Twitter only, while another may be authorised to only publish blogs.

As boring as it seems, a good old fashioned register of authorisations will most likely be required to ensure that your organisation maintains control of its branded social media sites.

Finally, your organisation will need to design a training program for staff that must be undertaken before they are authorised to publish content on your social media platforms. This training will cover issues such as online brand promotion and protection, style guidelines, privacy and confidentiality, as well as guidelines for conducting online conversations and/or responding to comments. You would also be well advised to test each individual's understanding of the training, in case there is any dispute arising as to what is, or is not, appropriate online behaviour.

Chapter 5: Designing a Personal Usage Policy

Your organisation's Social Media Personal Usage Policy will set out your expectations of staff members (and potentially contractors) when using their own social media accounts. This is to be enforced where their identity can be linked back to your organisation – or where their published content makes reference, or implies information about your organisation, its products or services, its staff, directors, or other stakeholders, extending as far as competitors.

As previously explained, the concept of a standalone "Social Media Policy" is a misnomer. The overall design of your organisation's Social Media Personal Usage Policy will be dependent on the overall quality of your corporate governance and human resources infrastructure.

For example, in an organisation with a robust corporate governance and human resources infrastructure its Social Media Personal Usage Policy will most likely reference key documents, such as the employment contract, as well as other key policies and procedures, including:

- Equal Opportunity and Anti-Discrimination, Harassment Policies
- Bullying and Violence Policies
- Email and Internet Usage Policies
- Information Security Policies
- Internal Grievance Procedures
- Counselling and Discipline Procedures
- Complaint Handling Procedures

By referencing other key documents and policies the Social Media Personal Usage Policy can be greatly simplified and focus on its key deliverable, which is to set out guidelines for what staff can and can not do.

Chapter 6: The Do's and Don'ts

There are a lot of opinions out in cyberspace as to what people should do, or should not do, in relation to social media in the workplace. Given this is an evolving space, Do's and Don'ts commentary tends to fall into the following two categories:

- **Increasing Followers/Subscribers** – For example, in some 'do's and don'ts lists' it is emphatically stated **"Don't"** excessively link back to your own website. Others say things like **"Do"** post frequently.

- **Social Media Policy Drafting** – For example, some commentators suggest not developing a Social Media Policy without first understanding relevant state and federal laws. Others suggest you ensure that all staff are trained appropriately.

Employers may do well to go further than this and consider providing their staff with guidance on the **Do's and Don'ts** of social media within their own organisations. Here are some ideas to get you started.

Things Staff Should Do

When using personal social media accounts, staff should ensure they:

- **Do** safeguard their own social media accounts with the highest security settings available so as to minimise the risk of unauthorised third party access;

- **Do** think about their personal reputation, their employer's reputation, and the reputation of their colleagues;

- **Do** ensure their posts are not in breach of their employment contract, or may potentially constitute behaviour which may breach the duties outlined under their employment contract;

- **Do** respect the privacy of their fellow staff members, the management and directors;

- **Do** respect the privacy and confidence of other key stakeholders, such as clients/customers, contractors, suppliers, investors, business partners, and other individuals or organisations associated with their employer;

- **Do** have regard to other relevant human resources policies published by their employer, such as Anti-Discrimination, Harassment, Bullying and Violence etc;
- **Do** remember that their comments are public and can easily be reported or passed on by another person;
- **Do** be prepared to defend their comments (to their boss, their colleagues, their family, their friends);
- **Do** be transparent, particularly if commenting on any matters related to their employer, or their work in general (e.g. use their own name, declare their interests);
- **Do** make it clear that any views they express are their own and not those of their employer if commenting on any matters related to their employer, or their work in general, which can be linked back to their employer.

Things Staff Shouldn't Do

When using personal social media accounts, staff should ensure that they:

- **Do not** disclose any information they have gained through their employment that is commercially confidential;
- **Do not** engage in any activity that reflects poorly on their employer;
- **Do not** post negative comments with respect to any fellow staff members, directors, clients/customers, suppliers, or others associated with their employer (including competition);
- **Do not** post material that is obscene, defamatory, threatening, discriminatory or hateful to another person or entity where they are in anyway associated with their employer;
- **Do not** use their employer's logos, trademarks or other intellectual property.

Summary

Social media is here to stay and with it the challenges for employers who are serious about managing the risks it brings to their business. Drafting a standalone social media policy is not enough. To be effective a social media policy must be part of a coordinated and properly documented corporate governance and human resources management strategy.

As an emerging area of technology, the law, and human resources practice, how employers use social media tools in their business, while effectively managing their employees' personal use of such tools, will continue to be legally complex and difficult to control.

In summary, if you are serious about managing social media risks in your organisation, you must get serious about developing a coordinated corporate governance and human resources management strategy that not only includes documented policies and procedures, but also an internal training program and robust record-keeping procedures.

How Can CompliSpace Help?

CompliSpace is a leading provider of tailored Corporate Governance, Risk and Compliance (GRC), Human Resources and Workplace Safety services to organisations across Australia. Our focus is on assisting clients to implement sustainable solutions utilising cost effective enabling technologies.

Through our human resources content module we deliver a series of enhanced social media policies and online training courses. These are part of a comprehensive suite of online human resources programs, policies and procedures which cover, amongst other things, general conditions of employment, employee leave entitlements, remuneration and benefits, discrimination and harassment and staff performance management procedures.

Our corporate governance content modules include ISO 31000 Enterprise Risk Management, AS 3806 Compliance, ISO 10002 Complaints Handling, AS/NZ 5050 Business Continuity, AS 8001 Fraud & Corruption and AS 8004 Whistleblower programs.

These are not template documents, but rather policies and procedures that are specifically designed to be tailored to the needs of your organisation and integrated with other online content modules. For more information please visit www.complispace.com.au or contact us on +61 2 9299 6105 or contactus@complispace.com.au