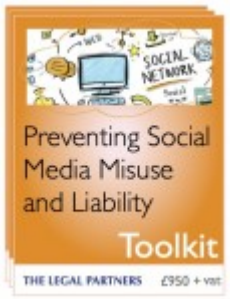
How to avoid Social Media misuse and protect from liability

Exposure through Social Media is rapidly becoming part and parcel of an organisation's day to day operation. Even if your business isn't actively on Social Media platforms such as Twitter, Facebook or messaging Apps such as WeChat or WhatsApp, your employees most likely will be.
Most employers get into trouble over, or on social media because they haven't put policies in place and they haven't set expectations with staff of what is good and bad behavior online.
Below we've put together a 5 point summary of the risks involved and the steps you need to take to avoid Social Media misuse and protect your business from liability.
It provides an overview of the law in this area. Please talk to us for a complete understanding of how it may affect your particular circumstances.

No excuses, just security. Purchase our Social Media Toolkit today.

We've created a Toolkit to Using Social Media at work, its designed to help you put together these policies and controls – and stick to them – to avoid social media misuse and so protect your business and your employees from liability.



Our Social Media Legal Toolkit is a simple way to keep your business out of trouble and to prevent any litigation from social media misuse by employees. It includes:
Social Media Policy
+
IT & Systems usage Policy
+
1 hour of our advice or training with your staff to clearly spell out what they must, must not do,

For a fixed price of £950+vat you are ready to protect your business.
Purchase your Toolkit today, email us directly or call on 0203 755 5288.

Avoid social media misuse by staff and protect from liability.

If your staff use :
Social Media (personal and business)
email and
the internet at work,
If they send work related emails or discuss the workplace on the internet & on Social Media,

you do need to take action to protect the business from social media misuse.

This article will help you:

1. manage employees use of email, the internet or Social Media – where use is excessive, inappropriate and/or leads to loss of productivity

2. protect your business against liability for employees actions on Social Media sites

3. monitor employees use of social networks without infringing their privacy
4. protect the business when an employee/s leaves. Remember the HMV case when the company's redudnacy programme was leaked as it was happening on twitter (link) by a social media manager at the company.

Use Social Media and IT & Systems Policies in your Staff Handbook

It is vital to:

1. conduct a Risk Assessment. This will identify:

Positive use eg Sales and Marketing, Recruitment, Competitor tracking, Training, Research; the business will want to allow certain staff to use the internet/Social Media for these activities.

Negative Uses – reputational risks of employees eg posting derogatory comments on Facebook. Your business can be liable for the acts of your employees on Social Media unless you have taken reasonable steps to prevent such action. The Social Media Policy is one way of demonstrating this. Another example is through training.

Permitted Personal Use – using Social Media privately in work time when in the office, (e.g during the lunch break) or similarly when working from home during work time.

Who owns the contact information on Social Media eg Linked in?

2. Include policies on the use of

IT & Systems, and

Social Media usage

in your Staff Handbook to state what is permitted and what is not permitted usage.
Be clear that if Social Media usage is permitted during lunch time specify that that is the 1 hour period during the employee's lunch break. Employers have lost cases at Employment Tribunal when they do not clearly specify what these permitted hours are.
3. In your Disciplinary Policies, state that breaches of the IT & Systems policy and/or Social Media policies will be treated as Misconduct or Gross Misconduct depending on the severity. The Apple Retail Store case below, illustrates how important this is.
These polices allow you to set and send clear expectations of acceptable & unacceptable behaviour around use of Social Media to your teams.

4. Have regular training on how to use Social Media well, for example:

using twitter correctly

how to engage with contacts using Linked in

how to make postings on Facebook public or private within the group

how to organize contacts in google + groups

hangouts and the privacy settings

Help your staff understand their digital footprint. A digital footprint is the trail of everything someone has posted, commented on, downloaded, and reviewed on line. This trail of content remains in the public domain, and could affect them and the company they work for. To understand more about digital footprint, read http://www.internetsociety.org/your-digital-footprint-matters

For those who have grown up with social media, and other workers whose familiarity with social media might lead them to sleepwalk through it without understanding the implications, this video courtesy of safeinternetbanking.be can be a useful starting point and wake up call.

Examples of social media misuse and litigation are now very common and becoming more so. Take two key cases that made the headlines in recent years. A former Wetherspoons employee lost her case (her dismissal by Wetherspoons was held to be fair) because, whilst at work and during work time, she posted derogatory remarks about customers on her facebook account. Her privacy settings were not set appropriately and the customers saw these remarks.This was in beach of Wetherspoon's carefully worded Social Media policy.

In the Crisp v Apple Retail case, Apple Retail defended the case and won because employee Mr Crisp had received a clear, well communicated Social Media policy and training from Apple on what was acceptable and unacceptable online, so his defence failed. Mr Crisp's right to freedom of expression under the European Convention on Human Rights was overridden by the harm he had caused Apple by his derogatory comments on FB.

5. Monitor what is happening in Social Media channels.

This is important because if someone, including employees, are badmouthing your company online, you want to know what's being said about and who is saying it.

Check your company's ditigal footprint regularly using social media monitoring sites, or google alerts. Google alerts allows you to set up multiple alerts. Set these up independently, one for your name, another for the company name, for the brand, for any key products or employees, another for important keywords etc.Make sure there is someone in the business to monitor these and gather the reports from the results. Plan who will see the reports, what action is taken if something negative is found; follow though.

According to research undertaken by recruitment firm MyJobGroup.co.uk 40% of UK employees surveyed admit to criticising their employer on social networking sites like Facebook and Twitter. When it comes to Social Media usage, your policy will only be as effective as the follow-up & enforcement you practice.

6. If a potential issues crops up, it is vital to collect the evidence as part of any investigatory phase of a disciplinary procedure. It can sometimes be difficult to find the alleged derogatory posting on platforms such as Facebook, Twitter, so always take a screen grab/screen print, save it and print a colour copy of the offending posting(s).

Employers have the right to monitor email and Social Media accounts -under the Regulation of Investigatory Powers Act 2000 (RIPA) – for legitimate purposes eg to investigate wrongdoing. Always refer in the Social Media policy that this may happen.

On the subject of emails, there is a great deal employees can do to protect the company from misuse of emails. Read this article for practical suggestions to minimize risks and liability from email misuse.

Social media needs to be carefully considered in your risk management program.

For more advice or to purchase your Social Media Toolkit, email us or call on 0203 755 5288.