

### Introduction

The issue of allowing employees to use social networking sites, such as Facebook and My Space, is one that has caused a lot of apprehension amongst employers. Whilst there are several problems that can arise from allowing access to such sites, this genre of site has also become a cyber networking tool.

### The Issues

With social sites forming a major part of a person's day to day activity, it would be difficult to employ heavy handed tactics in order to completely stop usage altogether. However, giving free reign to an employee is also not the correct approach, as it may have several damaging effects.

The most obvious problem is the amount of time that is wasted, with employees spending working time "networking" with friends online, whilst also uploading video's, photographs and music on to their online accounts. Productivity is impacted, and employee efficiency diminished.

A further and greater problem with using these sites is the information that may be disclosed. Many employees discuss their current work problems with the friends in cyber space, giving intricate details of situations they may be facing, or even work they may be handling. This could potentially cause great damage to an organisation's reputation and, even more damaging, expose potentially sensitive information.

### The Benefits

The question remains whether these dangers justify employers implementing strict policies, in order to avoid these potential pitfalls altogether. However, the importance of such sites should not be dismissed when deciding on their usage.

Whilst the potential dangers are indeed high risk, social networking sites can in fact be beneficial, if used in the correct manner.

Many organisations with national or international offices have found that social networking sites have in fact increased communication between colleagues located at different offices, who would otherwise not communicate. This can foster a greater team spirit, as well as providing a forum to share best practice.

### Developing an IT Policy

The starting point for an employer is to develop an IT policy. Within this, policy guidelines of the internet as a whole can be defined, with more specific rules set on using social networking sites.

Typically an IT policy would include limiting access to networking sites during non-working hours, advising employees whether usage will be monitored, identifying which sites are permitted for use and most importantly, confirming the sensitive or confidential information that should not be put on such sites. Employees should also be aware that making derogatory remarks, which could damage a company's reputation, would not be tolerated.

The policy should also outline any potential disciplinary action that could be taken in the event that the policy is breached. Outlining the potential punishments for breaches focuses the minds of employees granted with internet access.

Where dealing with a breach of the IT policy, employers must make sure that action taken against the offending employee is proportionate to the situation being faced. A harsh or heavy handed approach could cause the organisation greater problems in the longer term, whether internally by way of formal grievances, or externally before an Employment Tribunal. Either way this can cost a significant amount of time and money.

The use of social networking sites is growing and therefore issues in the work place surrounding this are growing in importance. Issues related to this however should be handled carefully as several recent Employment Tribunal cases have shown that if this issue is not handled with care, the potential repercussions could be damaging.

### Can We Help?

If you need help on any issue associated with the employment, performance or conduct of employees, or we can help with introducing an IT Policy on your site, please call us on **0845 603 1610**. Alternatively visit our Website at [www.hrinsight.co.uk](http://www.hrinsight.co.uk).

We look forward to hearing from you!

