



MessageLabs<sup>®</sup>

Be certain

# Online Social Networking The Employer's Dilemma

A white paper which considers how relevant UK legislation and employers' policies impact on the use of social networking websites

Jonathan Naylor, Employed Barrister, Shoosmiths

## **Table of Contents**

Introduction	3
Social Networking and the Law	3
Productivity and Damage to Brand	4
Practical Steps for Employers	4

Online social networking presents specific problems because of the nature of the content on such sites.

## Introduction

The majority of employers permit employees to have reasonable personal use of the Internet during working hours. Employers have sought to minimise the risks that this personal use might present by introducing Acceptable Use Policies (“AUP’s”) and monitoring employee use. This bargain between employers and employees is now being tested by the phenomenon of online social networking, in which the popularity of sites such as Facebook, Bebo and MySpace poses a new question for employers; do we trust our employees and allow unrestricted access to such sites, or do we perceive the danger as too great and ban the sites?

This article considers how relevant UK legislation and employers’ policies impact on the use of social networking sites, highlights some of the problem areas that cause employers most concern and provides guidance on how employers can take practical steps to avert the dangers involved.

## The Online Social Networking Phenomenon

IT and HR managers will be well used to the challenges that come with regulating employees’ personal use of the Internet while at work. Having a clear AUP, enforcing it with technical solutions, notifying employees of clear rules on what is acceptable and what is not, balancing the need to monitor with the employees’ reasonable expectations of privacy and weighing the overall benefits of allowing personal usage against the risks of doing so, are all issues with which managers will be familiar.

To some extent, online social networking is still just one example of employees using an employer’s PC to access a website for personal use; all of the above issues apply. However, this particular type of employee use brings a new, sharper edge to these issues and has often meant that employers who would generally encourage a liberal approach to personal use have drawn the line at social networking sites and imposed a ban.

Online social networking presents specific problems because of the nature of the content on such sites. Would an employer normally ask an employee to explain comments made to a friend during a conversation in a pub on a Saturday night? Hardly, and yet such comments made online to the same friend might be monitored by the employer. When recruiting, an employer is unlikely to telephone a candidate’s friend to get more of an understanding of what actually happened on the candidate’s stag do, and yet it is known that some employers have used sites such as Facebook to check on the online “personality” of potential job applicants.

While employers have to tread carefully because of the very personal nature of the information accessed and distributed via these sites, it is understandable that many employers feel the need to monitor employees’ usage. Social networking sites can be both addictive and time-consuming, damaging employee productivity. Employers may be identified and there is always the possibility of derogatory comments or disclosure of commercially sensitive information being made by an employee, which then becomes a permanent feature online.

In the light of these risks, it is hardly surprising that recent surveys suggest at least 43% of employers have banned employees from social networking sites for productivity and security reasons. The electrical retailer, Comet, which normally operates what it describes as a “culture of trust” within the company, has taken the decision to ban staff access to Facebook. It described this as an unusual step, but felt that it had to be explicit about the behaviour to be expected from staff.

## Social Networking and the Law

The same legal principles apply to the use of online social networking as apply to all employee use of the Internet. Employers therefore need to consider the Data Protection Act 1998 (‘DPA’) and particularly the guidance given by the Information Commissioner in Part 3 of The Employment Practices Data Protection Code (‘the Code’), which deals with monitoring at work. Under the Code, employees are entitled to a degree of privacy at work and employers should only monitor in a

## The same legal principles apply to the use of online social networking as apply to all employee use of the Internet.

proportionate way, having first considered which is the least intrusive method of monitoring to achieve the objective required.

Under the Regulation of Investigatory Powers Act 2000 ('RIPA') and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 employers are permitted to monitor or record communications without express employee consent in certain circumstances. Such instances include investigating or detecting unauthorised use of the employer's telecommunications system, establishing the existence of facts or ensuring quality control. In order to undertake such monitoring lawfully, the employer must have taken all reasonable steps to inform the employees concerned that monitoring may take place; this is usually made clear in the AUP.

While the Human Rights Act 1998 ('HRA') only has direct effect against public authorities (such as councils and NHS Trusts) it may be cited by private sector employees as an additional claim should they seek to argue, for example, breach of contract or unfair dismissal. Article 8 of the HRA provides that everyone has the right to respect for private and family life. This is not an absolute right and will always be balanced against the reasonable needs of the business.

### **Productivity and Damage to Brand**

One of the biggest concerns regarding employees' use of online social networking is simply poor productivity; that employees may spend an excessive amount of work time on these sites. However, if this were the only concern, it could be addressed by only permitting access during certain times (e.g. lunch and break times) or alternatively setting a particular amount of time that would be acceptable usage.

A more troublesome concern is the potential for damage to an employer's reputation or brand, if an employee makes derogatory comments about an employer, client or customer. Such comments then become easy to find via an online search and may be available for an unlimited time.

Employers are also concerned about the potential loss of confidential information by an unguarded (or malicious) comment by an employee, then causing the company embarrassment, financial damage or possibly leaving them open to security risks such as identity fraud.

For employers, the temptation to utilise sites such as Facebook and MySpace may also lead them into trouble. Some employers view the scanning of such sites for information on prospective employees as legitimate; others view it as distasteful and intrusive (the equivalent of rummaging through a candidate's personal items). Whatever the view, employers adopting this approach would do well to heed the warning of the TUC's guidance on online social networking. This guidance reminds employers that only a minority of potential staff will have a public profile on a social network, so using information from this source can give either an unfair advantage or disadvantage to certain candidates, as well as leaving the employer open to the accusation of discrimination.

### **Practical Steps for Employers**

Most employers accepted long ago that a total ban on personal use of the Internet by employees was unrealistic and ultimately counter-productive in trying to foster a relationship of trust with staff. However, asking the same question in relation to the growing popularity of social networking sites does not lead so easily to a clear answer.

Employers are within their rights to ban all employee use of social networking websites and indeed many have done so. In some cases, this runs contrary to the employer's normal ethos of permitting reasonable personal use and placing trust in employees to respect this freedom.

The TUC's guidance suggests that a total ban may, in some cases, be an overreaction and proposes instead that what is needed is more education of

## Employers are within their rights to ban all employee use of social networking websites and indeed many have done so.

employees to the risks that may come from inappropriate or careless use of the Internet.

Regardless of the view that a particular employer may take, there are some practical steps that all employers should consider when attempting to deal with this issue:

- Have a clear and comprehensive AUP in place, ensure employees are aware of it and keep it regularly reviewed and updated.
- Enforce the AUP with an appropriate technical solution.
- Ensure the potential impact of any monitoring is assessed and proportionate.
- Amend the AUP to reflect what is permitted regarding social networking sites.
- Ensure any AUP is easily accessible to employees; perhaps by being placed on the company intranet.
- Educate employees about the implications of the social networking sites from a professional and personal point of view. You may wish to offer training to raise employees' awareness of IT security and identity theft issues.

Employers have had to grapple with the issues raised by employee use of the Internet for some years and the rise of online social networking presents another challenge. There is no obvious conclusion here; employers will have to do what they consider to be correct in the light of their business concerns, their employee relations and their business culture. The dilemma posed by the heightened risks surrounding online social networking, whether to trust or restrict employees, does not lead to one "right" answer, but there is certainly a "wrong" answer. Given the ever-growing popularity of such sites and the potential consequences for employers of employee misuse, simply ignoring the issue can only lead to problems for the unwary employer.

Operating at the Internet level, MessageLabs' Web Security Service combines benchmark, constantly updated URL filtering, with real-time anti-virus and anti-spyware scanning. The service combines ease-of-use with the flexibility necessary to allow businesses to devise and implement exactly the right approach to social networking sites for their specific needs.

David Mitchell, Group Product Manager at MessageLabs explains: "Our highly configurable service enables different website blocking and filtering rules to be applied and then monitored right down to user group or even individual employee level. Rules can include a total ban on individual sites or, consistent with a more relaxed approach, enable staff to have access to these sites during certain parts of the day, for example during the lunch break or outside core working hours."

*To find out more about how MessageLabs Services can help your business harness the potential benefits of social networking while protecting you against the risks, visit [www.messagelabs.co.uk/products/](http://www.messagelabs.co.uk/products/)*

**www.messagelabs.co.uk**  
**info@messagelabs.com**

Freephone UK  
0800 917 7733

**Europe**  
**HEADQUARTERS**  
1270 Lansdowne Court  
Gloucester Business Park  
Gloucester, GL3 4AB  
United Kingdom

T +44 (0) 1452 627 627  
F +44 (0) 1452 627 628

**LONDON**  
3rd Floor  
40 Whitfield Street  
London, W1T 2RH  
United Kingdom

T +44 (0) 207 291 1960  
F +44 (0) 207 291 1937

**NETHERLANDS**  
Teleport Towers  
Kingsfordweg 151  
1043 GR  
Amsterdam  
Netherlands

T +31 (0) 20 491 9600  
F +31 (0) 20 491 7354

**BELGIUM / LUXEMBOURG**  
Culliganlaan 1B  
B-1831 Diegem  
Belgium

T +32 (0) 2 403 12 61  
F +32 (0) 2 403 12 12

**DACH**  
FeringasträÙe 9  
85774 Unterföhring  
Munich  
Germany

T +49 (0) 89 189 43 990  
F +49 (0) 89 189 43 999

© MessageLabs 2007  
All rights reserved

**Americas**  
**AMERICAS HEADQUARTERS**  
512 Seventh Avenue  
6th Floor  
New York, NY 10018  
USA

T +1 646 519 8100  
F +1 646 452 6570

**CENTRAL REGION**  
7760 France Avenue South  
Suite 1100  
Bloomington, MN 55435  
USA

T +1 952 886 7541  
F +1 952 886 7498

**Asia Pacific**  
**HONG KONG**  
1601  
Tower II  
89 Queensway  
Admiralty  
Hong Kong

T +852 2111 3650  
F +852 2111 9061

**AUSTRALIA**  
Level 6  
107 Mount Street,  
North Sydney  
NSW 2060  
Australia

T +61 2 8208 7100  
F +61 2 9954 9500

**SINGAPORE**  
Level 14  
Prudential Tower  
30 Cecil Street  
Singapore 049712

T +65 62 32 2855  
F +65 6232 2300