<CFS/NESE>

Short abstract (c.25 words):

In this article we examine the potential misuse of social media by employees, the relevant UK legislation, and approaches to limiting such misuse.

Long abstract (c.120 words):

Social networking applications such as Facebook, Twitter, and YouTube are increasingly being used in various ways by organizations. In this article we examine the potential misuse of social media by employees, the UK legislation relevant to such misuse, and also examine approaches by which organizations can attempt to limit such misuse via appropriate guidance for employees.

# Avoiding the misuse of social media by employees

**Mark Taylor, Liverpool John Moores University,**
**John Haggerty, Nottingham Trent University,**
**David Gresty, University of Greenwich,**
**Chris Wren, Liverpool John Moores University,**
**Tom Berry, Liverpool John Moores University**

## Introduction

Social networking applications such as Facebook, Twitter and YouTube are increasingly being used in various ways by organizations. Organizations may adopt the use of social media for a variety of reasons including engaging with customers and clients, and supporting communication between employees.[1,2,3] Although social media can potentially support communication between employees, care needs to be taken that social media is used in a manner appropriate for relevant business purposes, at all times. Due to the 'social' nature of social media, it may be that in certain circumstances, individuals may make comments that they would not make via more 'formal' communication channels such as the corporate email system. The level of privacy provided by the social media, and the manner in which such privacy levels are used is an important factor in the type of misuse that might occur. Although social media can potentially support and enhance communication between employees, as a result of inappropriate use of social media, employees may end up being suspended or dismissed. Therefore it is important that organizations encourage

and guide employees to use social media appropriately typically through the use of a social media policy.

In this article we examine the business, managerial and legal aspects of the misuse of social media by employees. In particular we examine the misuse of social networking applications in terms of discrimination, data protection violations, defamation, and harassment that could potentially occur, the strategies that organizations might adopt to limit such misuse, and the disciplinary actions that might result from misuse of social media. This is an important area of research since social media use is becoming increasingly widespread. However, with increasing use comes the potential for misuse, and employees may not be aware of the potential damage that can be done to careers and reputations purely by materials posted to a social media website. Therefore it is important that employees using social media are aware of how to use such in an appropriate manner and also important that organizations provide appropriate social media guidance and training for employees. The specific topics covered in this article are:

What types of misuse of social media occur in organizations
What UK legislation might apply to such misuse
What strategies can be adopted to limit the misuse of social media by employees

This article discusses the potential misuse of social media by employees and the UK legislation relevant to such misuse in order to inform organizations regarding the possible consequences of such misuse, and the examination of strategies for attempting to limit such misuse.

## Social media in organizations

Social media offers new and different approaches to employee communications. Corporate social networking sites can provide employees and employers with considerable opportunity to share information.[3] Social media can provide employees with information sources both within and beyond organizational boundaries.[4] However, employees may consider that off-duty conduct on social media outside the physical workplace is unrelated to the employer's responsibility with regard to workplace conduct.

### *Misuse of social media in organizations*

Although existing information and communication applications available to employees within an organization such as email, and corporate intranets can provide similar facilities, they typically will not engage employees in quite the same manner as social networking applications. Although organizations might support (or tolerate) social media use by employees, they may not fully appreciate the potential for misuse that social networking applications may provide.[5,6,7] As a general rule, an employee's actions away from the workplace are not connected with the employer and thus should not impact on the employment relationship. However, in the context of social media use by an employee, there could be various possible issues which might determine whether the employer could be entitled to take disciplinary or legal action,

including whether or not an individual reading the content on a personal social media web page would believe that the comments were a reflection of the employer's own beliefs or views and whether the comments might have impacted on others, for example, in terms of promoting certain views or attempting to undermine work colleagues.

The use of social media related to the workplace has been the subject of a number of dismissals from employment and at the centre of the dismissals was the posting of comments via social media sites. A number of UK unfair dismissal hearings are a result of comments and remarks posted on a social media site where the context of communication in many cases, was deemed to be private. Examples from UK Employment Tribunals where social media tools were a factor in the dismissal include the case of Teggart v Teletech UK Limited NITT00704/11 which highlighted that when an employee makes comments on a social media site such as Facebook, even out of working hours about a colleague, they may be dismissed for such.[8] In this case the employee was deemed to have been fairly dismissed. In the case of Whitham v Club 24 Ltd t/a Ventura ET/1810462/10 where an employee made derogatory work related comments via Facebook, the outcome in this particular hearing found for the employee.[9] An employer cannot always seek to dismiss on the grounds of comments made via social media, especially in the absence of policies and procedures regarding their use. In contrast is the case of Crisp v Apple Retail (UK) Ltd ET/1500258/11 in which the dismissal was deemed as fair following the employee making derogatory comments on Facebook about the company's products.[10] In this case there were ample policies produced by the employer regarding electronic communications.

*Discrimination via social media in organizations*

Employees that upload materials via a social networking application that could constitute discrimination of another employee or social group might face disciplinary proceedings, or possible prosecution, if such discrimination infringed anti-discrimination legislation, such as race, gender or disability discrimination legislation.[11] Discrimination could occur through the use of even a single word or phrase, or the inclusion of an image or video that in some way discriminated against a particular social group or individual belonging to a given social group.

*Defamation via social media in organizations*

Employees could be held liable for defamation if they made comments regarding another employee that might damage the reputation of that individual via a social networking application.[12,13] This could lead to disciplinary actions by the employer, or at worst a court case.

*Harassment via social media in organizations*

Previous research has indicated that social media can potentially pose problems relating to cyber stalking and cyber bullying.[14] A teenager became the first person to be convicted under the UK Protection from Harassment Act 1997

where one of the acts constituting the course of conduct in question was bullying pursued via a social networking site.[15,16] Employers and employees can be affected by the widespread use of social media, and the potential challenges and difficulties presented by the use of social media in the workplace.[17,18,19]

*Data protection issues regarding social media in organizations*

Although employees may appreciate the need for data protection with regard to 'corporate' systems such as email, the 'social' view of social networking applications might lead some employees to be less vigilant with regard to the protection of personal data when using such applications.[20] Social networking applications may be used in a 'conversational' manner, with less regard given to the consequences of statements made. Employees may violate the UK Data Protection Act 1998 if they inadvertently upload personal data regarding colleagues (e.g. medical data, social data) via a social networking application. For example, although employees would probably not email other colleagues regarding a particular employee being ill, they might inadvertently post such personal data on a social networking application that might be viewed by work colleagues.

## Strategies for attempting to limit misuse of social media by employees

*Awareness of relevant legislation*

An important issue with regard to avoiding misuse of social media in the workplace is that employees should be aware of relevant legislation. The UK Equality Act 2010 contains legislation relating to discrimination concerning age, disability, gender, pregnancy and maternity, race, religion, and sexual orientation.[11] Clearly any use of social media in the workplace should not involve any materials that could be viewed as being in any way discriminatory. Employees should also be aware of the UK Data Protection Act 1998 with regard to any personal data held by the organization that might be inadvertently disclosed via social media. In addition, sensitivity should be shown regarding circumstances such as relationship breakdowns and bereavement that could be inadvertently disclosed via social media. The UK Defamation Act 2013 could apply if comments made by an employee via social media caused serious harm to the reputation of another person. The UK Defamation Act 2013 introduced a serious harm test to make it more difficult for persons bringing spurious actions, this set a higher bar for an action to proceed for reputational damage. In extreme cases the UK Protection from Harassment Act 1997 might apply if employees harass their colleagues via social media. An important point regarding social media misuse in organizations is that the misuse connected with the organization can occur outside the physical premises, outside normal working hours, and can be done via any computing device whether owned by the organization or not. It is important that organizations provide appropriate specific staff training with regard to relevant legislation, and data protection and equality legislation in particular in order to attempt to limit the damage that could be caused by misuse of social networking applications.

*Social media usage policies*

It is important that organizations have appropriate computer usage policies in place, and ideally social media specific usage policies.[21,22] A social media usage policy for an organization might typically cover the standards of behavior expected from employees regarding the use of social media in a clear and unambiguous manner. This should cover the use of social media by employees both within and outside the place of work. Outside the place of work should include both physically outside the place of work and outside normal working hours, and also cover employees' use of their own personal computing devices for social media. Ideally training for employees regarding the acceptable use of social media should be provided by the organization.

*Use of official organizational social media accounts*

An organization might operate a number of accounts on different social media websites for marketing purposes, and as a communication tool for communicating with clients and customers. There should be guidelines available for setting up such official organizational accounts, and also with regard to updating and monitoring such official accounts. Only authorised staff within the organization should have access to these organizational social media accounts. All information published via the official social media accounts should comply with the organization's confidentiality and data protection policies. In addition copyright legislation should be considered, with any references or sources used cited appropriately. There should also be guidelines available for employees dealing with any negative feedback received via the social media in an appropriate time frame. Any employee who becomes aware of social networking activity via official organizational social media accounts that would be deemed objectionable should report such activity to an appropriate member of the organization's management in a timely manner.

*Guidance for personal use of social media*

Employees with their own personal profile on a social media website should ensure that others cannot access any content from that profile that the individual would not be comfortable for others to view, or that might undermine their position as an employee. When using social media websites for personal purposes, employees should consider changing the privacy settings on their profile so that only people that they have accepted as friends can see their content. In addition it would be practicable to review who is on the 'friends list' on their personal profile.

It should be made clear to employees that personal blogs, Facebook, Twitter, YouTube, or any other social media websites have clear disclaimers that the views expressed by the author (in this case the employee) are theirs alone and do not represent the views of their employer. Disclaimers regarding views expressed by the author not representing the views of their employer have been around with respect to the use of email for some time. Extending disclaimers to social media would be a natural extension of this approach. However, typically disclaimers would be used for 'official' organizational social media accounts, rather than personal social media accounts used by employees for work

purposes. Personal social media accounts used by employees should not contain anything that might suggest that the account owner is acting in an official capacity with regard to their employer. Overall an organization's social media usage policy should provide guidance to attempt to ensure that employees are always respectful towards their employing organization, other employees, and others associated with the employing organization. The social media policy should also remind employees that they are legally liable for anything posted online, at all times, in or out of working hours, and that all actions captured via images, posts or comments online can reflect on the employing organization.

*Reporting social media misuse*

There is the issue of what an employee should do regarding employer related inappropriate material posted via a social media tool. Employees should report such to their line manager within the organization. Relevant staff should record and take copies of such material from the social media website but take care not to do so in a manner that might hamper organizational (or in some cases police) investigations of social media misuse.

**Conclusions**

In this article we have examined the potential misuse of social networking applications in the workplace via a multi-disciplinary literature review of business, managerial and legal literature. In particular, this article examines the main types of potential misuse of social media by employees including discrimination, violations of confidentiality, defamation, and harassment, and the relevant UK legislation that might apply to such types of misuse. In addition we have examined the strategies that organizations might adopt in order to attempt to limit misuse of social media. It is important that organizations have appropriate computer usage policies in place, and ideally specific social media usage policies and provide appropriate staff training in data protection and equality legislation in order to attempt to limit the damage that could be caused by misuse of social networking applications by employees. It is hoped that the examination of the potential concerns relating to the use of social media by employees, including damage to reputations and careers and potential court cases that could occur, the examination of the legal issues associated with misuse of social media, and the examination of strategies for attempting to limit misuse of social media may be of benefit to organizations both in the UK and elsewhere.

## About the authors

*Dr Mark Taylor is a Senior Lecturer in Computing at Liverpool John Moores University. He is a Chartered IT Professional, a Chartered Engineer and a Chartered Scientist.*

*Dr John Haggerty is a Senior Lecturer in Computing at Nottingham Trent University. His research interests include digital forensics, network security, signature matching and mobile computing.*

*David Gresty is a Researcher in the Centre for Computer Security, Audit, Forensics and Education in the University of Greenwich. He has extensive professional experience investigating child protection and the downloading of unlawful material.*

*Dr Tom Berry is the Computer Forensic Programme Leader in the Department of Computer Science at Liverpool John Moores University.*

*Mr Chris Wren is a Senior Lecturer in Computing at Liverpool John Moores University.*

## References

1. Kozinets, R., De Valck, K., Wojnicki, A., Wilner, S. (2010) Networked Narratives: Understanding word-of-mouth marketing in online communities, Journal of Marketing, 74, 2, 71-89.

2. Fagerstrom, A., Ghinea, G. (2010) Web 2.0's Marketing impact on low-involvement consumers, Journal of Interactive Advertising, 10, 2, 67-71.

3. Kaupins, G. Park, S. (2011) Legal and ethical implications of corporate social networks, Employee Responsibilities and Rights Journal, 23, 2, 83-99.

4. Vayrynen, K., Hekkala, R., Liias, T. (2013) Knowledge protection challenges of social media encountered by organizations, Journal of Organizational Computing and Electronic Commerce, 23, 34-55.

5. Ramsay, M. (2010) Social media etiquette: a guide and checklist to the benefits and perils of social marketing, Database Marketing and Customer Strategy Management, 17, 3, 257-261.

6. Clark, L., Roberts, S. (2010) Employee's use of social networking sites: A socially irresponsible practice, Journal of Business Ethics, 95, 507-525.

7. Ruhnka, J., Loopesko, W. (2013) Risk management of email and Internet use in the workplace, Journal of Digital Forensics, Security and Law, 8, 3, 7-19.

8. Teggart v TeleTech UK Ltd (2012) NIIT 00704_11IT 15th March 2012 Industrial Tribunals Northern Ireland

9. Whitham v Club 24 Ltd (t/a Ventura) ET/1810462/10 (2011) UK Employment Tribunals

10. Crisp v Apple Retail (UK) Ltd ET/1500258/11 (2011) UK Employment Tribunals

11. EA (2010) UK Equality Act 2010, http://www.legislation.gov.uk

12. Donaldson, N., Cotton, D. (2011) New media, new risks? In-house lawyer http://www.inhouselawyer.co.uk/index.php/employment/ 9547-new-media-new-risks

13. DA (2013) UK Defamation Act 2013, http://www.legislation.gov.uk

14. Clark, L. (2012) Technology and ethical/moral dilemmas of higher education in the twenty-first century, Campus-Wide Information Systems, 29, 5, 358-367.

15. PHA (1997) UK Protection from Harassment Act 1997, http://www.legislation.gov.uk

16. McMullen, J. (2011) Balancing the right to manage with dignity at work, Perspectives, 15, 1, 3-6.

17. Lakhani, A. (2013) Social networking sites and the legal profession: Balancing benefits with navigating minefields, Computer Law and Security Review, 164-174.

18. Eivazi. K. (2011) Computer use monitoring and privacy at work, Computer Law and Security Review, 27, 5, 516-523.

19. Kierkegaard, S. (2010) Twitter thou doeth? Computer Law and Security Review, 26, 6, 577-594.

20. DPA (1990) UK Data Protection Act 1998, http://www.legislation.gov.uk

21. ACAS (2015) ACAS social media and how to develop a policy http://www.acas.org.uk/index.asp?articleid=3381

22. Lichtenstein, S. (2011) Ethical issues for internet use policy: balancing employer and employee perspectives, International journal of technology management, 54, 2, 288-303.