

# Employee Use of Technology in the Workplace: Corporate Liability for Sexual Harassment Claims

## CONTENTS

Abstract	1
Hostile Work Environment	2
Defence in Sexual Harassment Cases	2
Reducing Potential Liability	3
About the Authors	4

*Abstract: Use of technology in the workplace has grown exponentially over the past few years. We are at a time when literally every employee has access to the Internet and the corporate e-mail system. That access affords employees use of a communications medium that may result in substantial liability for their employers.*

*E-mail and Internet use has already served as "smoking gun" evidence in lawsuits involving breach of contract, discrimination, harassment, fraud, defamation, and many other claims. It has become almost commonplace to find articles on the front pages of the business sections of many newspapers detailing the latest corporate liability stemming from electronic evidence. For example, Norwich Union was reported as paying £450,000 to Western Provident Association for an internal e-mail claiming that WPA was insolvent. In another libel case, British Gas had to pay out more than £200,000. We have written this White Paper to address one particular aspect of that liability: sexual harassment and discrimination claims. The reason for focusing on this particular area of liability is that it is one of the most common sources of claims involving employee use of their employer's Internet and e-mail systems and carries with it some of the greatest liability.*

*For example, in the US, oil giant Chevron paid £1.4m. to four female employees to settle the women's claim that they were being sexually harassed by jokes sent through the company's e-mail system.*

*A few statistics will further highlight the problem:*

- ▷ 1 in 5 men and 1 in 8 women admitted using their work computers to access sexually explicit material online*
- ▷ More than 25% of workers surveyed said they "sometimes" or "often" receive sexually explicit or otherwise improper e-mails*
- ▷ A 2000 study revealed that 1 in 3 companies had terminated employees for abusing Internet access*
- ▷ A survey conducted by Elron Software Inc. found the following: Of the 86% of people who said they send or receive personal e-mail at work, 70% said their e-mail contains "adult content"*
- ▷ Research suggests that staff spend at least 30 minutes a day surfing the web for entertainment material, costing British companies over £2.5m. a year*
- ▷ A recent survey of American porn sites showed that the majority of hits come between the hours of 9 a.m. and 5 p.m., Monday to Friday*

*Many employers have had to take drastic action to address this problem:*

- ▷ Orange sacked 45 workers from three offices for distributing Internet pornography to colleagues*
- ▷ Huddersfield-based Holset Engineering disciplined 40 workers, sacking two, for receiving and distributing sexually-offensive cartoons and jokes*
- ▷ Staff at city solicitors Norton Rose and at the Financial Services Authority were disciplined for forwarding the same saucy e-mail from Miss Claire Swire. Norton Rose' website received so many hits that it crashed.*
- ▷ Focus Management Consultants sacked Ms. Fraxhi, its IT manager, who surfed 150 Internet sites at work. Her claims for sex discrimination and unfair dismissal were dismissed by a Liverpool employment tribunal.*

## HOSTILE WORK ENVIRONMENT

Harassment is defined as unwanted conduct, related to sex, which has the purpose or effect of (a) violating a person's dignity, or (b) creating an intimidating, hostile, degrading, humiliating or offensive work environment. The conduct may affect dignity or create a hostile work environment, or both. The conduct has to be considered from the perception of the complainant. The EC Code of Practice on dignity at work stresses that it is for the individual to decide what is and is not offensive. However, courts and tribunals also have to consider whether the unwanted conduct should reasonably be regarded as violating dignity or creating a hostile work environment.

In most cases of harassment in the workplace, the harassing conduct is committed by a fellow worker rather than by an employer. The employer is still liable for that conduct, as long as it is committed "in the course of the employment". This phrase is given a broad meaning, and has been held to include conduct in a pub after work and at an organized leaving party. Conduct may be in writing, oral or physical.

A common form of corporate liability for harassment is for claims based on a "hostile work environment." The most frequent form of this liability arises when an employee downloads sexually-explicit jokes, graphics, and stories from the Internet and then forwards them around the company by e-mail. There have been instances where employees have downloaded literally hundreds of megabytes of this material and stored them on their employer's computer systems. In addition to potential liability for sexual harassment, the presence of this material on the employer's computer systems may give rise to liability for copyright infringement or criminal offences under the Obscene Publications Act, Computer Misuse Act or Protection from Harassment Act. In addition, these types of materials frequently contain illicit code (e.g., viruses, worms, Trojan horses) that may cause substantial harm to the employer's systems.

Apart from potential liability issues is the very real problem of lost employee productivity as a result of these activities. As indicated by the studies mentioned above, the amount of time spent by employees surfing non-business related sites on the Internet and, in particular, sites with sexually-explicit content is at an all time high. Many businesses now view the loss of employee productivity as so substantial that the use of blocking software and other technological measures to limit access to inappropriate sites has now become the rule, rather than the exception, in business.

An employer may be liable for failing to monitor and prevent inappropriate use of e-mail and the Internet when it has notice of the offensive use. In *Morse v Future Reality Limited*, the employer failed to monitor or prevent male office staff spending a lot of time poring over obscene images on the Internet. The employment tribunal ruled that Ms. Morse was justified in walking out and claiming unfair dismissal and sex discrimination.

## DEFENCE IN SEXUAL HARASSMENT CASES

Even if harassment has occurred in the workplace, the employer can escape liability by showing that he has taken "reasonable steps" to prevent the unwanted conduct from occurring. This is likely to involve:

- ▷ an equal opportunities policy
- ▷ a "harassment" or "dignity at work" policy; and
- ▷ a policy for use of e-mail and Internet

It is not sufficient simply to have written policies. Staff must be trained to understand and implement them; and they must be enforced. Complaints must be dealt with properly in accordance with the policies and disciplinary procedure. A complaints procedure specifically geared towards harassment is recommended, as part of a "dignity at work" policy. A suitable culture ("the way we do things") is just as important as policies. In *Schwenn v. Anheuser-Busch, Inc.*, a US case, an employee received sexually harassing e-mail messages from fellow employees. The employee failed to establish a claim of hostile work environment because, in large part, her employer had an e-mail policy in place and promptly responded to her claims by meeting with employees responsible for sending the inappropriate e-mail to advise them of the company's policy

against such messages. In another US case, *Daniels v. WorldCom*, the employer successfully defended a claim in relation to a racially-harassing e-mail, because it had a written policy against such activity and proof that it responded quickly to claims of harassment.

Another advantage of proper policies is reduced risk of other legal claims, for infringement of copyright, libel, or inadvertent creation of contractual relations. Under the Defamation Act 1996, a person has a defence if he can show that he was not the author or editor, took reasonable care in publication, and had no reason to believe that what he did contributed to the publication. In *Godfrey v Demon Internet Limited*, it was held that this defence was not open to Demon, which failed to delete alleged defamatory material. Immediately a complaint was made. In *Hall v Cognos Limited*, an employer was held liable for a line manager's unauthorized e-mail promising to pay an out-of-time expenses claim. Most of the documentary evidence in many employment tribunal claims comprises internal e-mails.

## REDUCING POTENTIAL LIABILITY

As the cases described above make clear, employers can substantially mitigate potential liability by adopting a three-pronged approach to employee use of technology:

1. Adopt an appropriate technology use policy, together with policies on equal opportunities and dignity at work
2. Conduct training for employees to ensure they understand their rights and obligations regarding these policies and use of corporate computer resources, and
3. Prompt enforcement of policies, including the implementation of appropriate technological measures (e.g., e-mail content monitoring applications and Internet monitoring and blocking programs). The use of technological measures, in particular, has become a key element of many businesses' approach to preventing sexual harassment claims. By using content monitoring technology, these businesses can prevent access and distribution of sexually-explicit materials before they give rise to a harassment claim. Use of such technology would likely have prevented many of the harassment claims filed to date involving employee use of e-mail and the Internet.

To be effective, the technology policy must clearly describe each employee's rights and obligations regarding use of the corporate computer systems. In the context of potential harassment claims, a basic policy should include the following:

- ▶ A statement regarding the employer's position against harassment, including examples of inappropriate uses. For example:

*Material that is harassing, embarrassing, sexually-explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate, including any comments that would offend someone on the basis of race, age, sex, sexual orientation, religion, or political beliefs, national origin, or disability, must not be sent by e-mail or other form of electronic communication, viewed on or downloaded from the Internet or other online service, or displayed on or stored in our computer systems. Users encountering or receiving such material must immediately report the incident to their supervisor. For more information, please see our Dignity at Work Policy.*

- ▶ A strong notice to employees that no one controls the Internet and that having an e-mail account will likely result in the receipt by the employee of spam, including messages with highly offensive, sexually explicit content. A typical disclaimer would read as follows:

*WE ARE NOT RESPONSIBLE FOR MATERIAL VIEWED OR DOWNLOADED BY USERS FROM THE INTERNET. THE INTERNET IS A WORLDWIDE NETWORK OF COMPUTERS THAT CONTAINS MILLIONS OF PAGES OF INFORMATION.*

USERS ARE CAUTIONED THAT MANY OF THESE PAGES INCLUDE OFFENSIVE, SEXUALLY EXPLICIT, AND INAPPROPRIATE MATERIAL. HAVING AN E-MAIL ADDRESS ON THE INTERNET MAY LEAD TO THE RECEIPT OF UNSOLICITED E-MAIL CONTAINING OFFENSIVE CONTENT. USERS ACCESSING THE INTERNET DO SO AT THEIR OWN RISK.

- ▷ A reference to the employer's general equal opportunities and dignity at work policies

*Use of our computer systems, including Internet and e-mail, is subject to the provisions of our equal opportunities and dignity at work policies [title of policies].*

- ▷ A statement communicating that violations of the policy may subject employees to disciplinary action and possible dismissal. For example:

*Violations of this Policy may result in disciplinary action, including dismissal without notice, as well as potential civil and criminal liability.*

- ▷ A statement that the e-mail and Internet systems are the property of the employer and provided for business use; also that the employer reserves the right to access, monitor and disclose all matters sent over the systems or stored on it, at any time without notice.

- ▷ Guidance as to confidential information, intellectual property rights, access (passwords), authority levels in making contractual commitments, and minimizing the risk of viruses.

Given the potential damages and adverse publicity businesses face from harassment claims, employers should not delay in implementing the three-pronged approach outlined above. By taking action now, before a claim arises, businesses can potentially avoid the risks of having to pay compensation and suffering bad publicity. The costs involved in implementing this approach are minimal compared to the potential damages that may result from even a single legal claim. The Centre for Policy studies estimates that a US-style compensation culture now costs British business £6.8bn. a year. There is no longer any reason to delay. Businesses should act immediately to address this problem.

## ABOUT THE AUTHORS

This paper was developed by Michael R. Overly is a partner in the e-Business and Information Technology Group in the Los Angeles office of Foley & Lardner. As an attorney, Certified Information Systems Security Professional (CISSP), and former electrical engineer, his practice focuses on counseling clients regarding technology licensing, information security, electronic commerce, and Internet and multimedia law.

The paper was tailored specifically for the UK market by Geoffrey Bignell, principal in the specialist employment law and human resources practice, Just Employment. He is a solicitor and advocate, frequently representing clients in Employment Tribunals in England and Wales. He writes and broadcasts on employment law, particularly discrimination and harassment.