

e-Business Factsheet - Legal

E-mail and the Internet - Employer's Risk



SHEPHERD+WEDDERBURN

As the use of IT systems in the workplace rises, there is an increasing degree of overlap between the fields of IT and employment law, raising new concerns for employers in today's workplace.

Developments in the Workplace

In the past, the employer essentially had dominance over the employee's actions and was only required to pay him for the services he provided. However, with the developments in case law and legislation over the past 10 years, employees have been given enhanced rights in the workplace.

Communications too have come a long way and today, it is hard to imagine an environment without telephones and faxes. However, as digital communications are gaining rapid approval, employers are having to face the fact that as use of the Internet by employees increases, so does the potential for claims of abuse by e-mail.

Liability

As a general principle, an employer can be liable for a wrongful act committed by an employee in the course of his employment, even where the act is performed in an unauthorised way (known as the employer's vicarious liability). In many instances, the employer will not even be aware of the employee's actions, or may even have expressly forbidden them, yet this does not prevent the employer from being liable for paying out to defend or settle a claim.

Sexual, Racial and Disability Discrimination

A growing concern for employers as a consequence of e-mail, is the potential for messages to be sent which are sexist, racist or discriminatory. While hard copy communications can be reviewed carefully by employers prior to being sent out, monitoring e-mails is often a difficult process. Although businesses are implementing e-mail policies, there is still potential for employees to send out offensive e-mails without the employer knowing.

Sexual Harassment

Repeated and unwanted requests for a date, sexual innuendoes or downloading or sending pornographic material to other employees may form sexual discrimination, even though the sender may not consider the material to be offensive and did not intend any harassment by his/her actions.

In the US, Chevron paid \$2.2m in an out of court settlement to female employees who were sent sexually offensive e-mail messages by another employee.

The viewing of pornographic material in the workplace has also been held to constitute sexual harassment. In *Morse v Future Reality Limited*, an employer was required to pay damages to a female employee who resigned. She shared an office with several men who spent much of their day viewing pornographic material on the Internet. Although none of the viewing was directed at her in particular, she won her case of sexual discrimination on the grounds of harassment. Employers on both sides of the Atlantic have been attempting to combat the problem by implementing e-mail and Internet use policies and taking disciplinary action against employees who distribute such material.

Racial and Disability Discrimination

Claims of sexual harassment can be extended equally to the context of racial and disability discrimination. Comments or derogatory words in an e-mail about a person's race or disability could give rise to a claim of discrimination. With the concept of vicarious liability being incorporated into the Sex Discrimination Act 1975, Race Relations Act 1976, as amended by the Race Relations (Amendment) Act 2000, and Disability Discrimination Act 1995, employers need to be aware of how vulnerable they are to being liable for discrimination as a result of their employees' actions.

Defamation via the Internet

In addition the Internet and e-mail lend themselves to the possibility of being used by employees to make defamatory comments. A defamatory comment is one which tends to lower the reputation of the subject in the minds of the community in which it is made public, even if this is only made to one person. Once again, the employer may be liable for the employee's actions. No better evidence of this can be found than in the Norwich Union case where the company paid out £450,000 to a rival firm for employees' defamatory e-mail comments.

In terms of the Internet, this problem could be particularly serious as a message could be displayed in several jurisdictions, giving the aggrieved party scope to forum shop for the jurisdiction with the most onerous laws of defamation in which to make their claim.

There have only been a few cases relating to defamation on the Internet but this is an area which looks ripe for development, so care is required.

Employers' Duties

In order to reduce the potential for liability, employers should and furthermore, are required by law, to provide and maintain a suitable working environment.

However, providing a safe system of work proves more difficult with employees having increased access to the Internet. People feel safe behind their computer screens. As a result, they are often less careful and more abusive in the language they use than they would be in a face to face situation.

To avoid being liable for an employee's actions, employers should, where possible, introduce measures, as described below, to monitor employees' access to e-mail and the Internet.

Employers' Right to Monitor

An extremely contentious issue at present is the employers' right to monitor business communications. The Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations which were made pursuant to this Act came into force in October 2000, increasing the complexity in this area.

In a recent case Barclaycard was cleared of any wrongdoing by an industrial tribunal after monitoring its employees' e-mails. It had sacked a worker after he was found to be using the company's internal system to insult colleagues, divulge confidential information to rivals and even set up cannabis deals.

The Regulations authorise employers to monitor e-mails but do not go as far as authorising blanket monitoring. Employers should be aware that all monitoring of e-mail correspondence and content as well as Internet usage must be undertaken for "lawful business purposes". The term "Lawful business purposes" includes monitoring or keeping a record of communications by an employer to determine whether such communications are relevant to the employer's business. Employees should note that all interception and monitoring of employees' communications should be notified to employees and carried out with their consent. There is an obligation on all employers to maintain a safe place of work free from any form of harassment and accordingly employer monitoring is often essential to identify and ultimately eradicate any form of harassment.

The current regulations fall short of setting anything in stone yet it is common sense that blanket monitoring of e-mails would neither be appropriate nor acceptable. Employers should also ensure that monitoring is carried out in a systematic way to avoid any argument that it is being carried out other than for lawful business purposes.

In addition, the Information Commissioner's Office is in the process of issuing a Code of Practice dealing with the implications of data protection law and the employer/employee relationship. There are four parts to the code, the third of which deals with employer's monitoring of employees. The draft code, in its current form suggests new responsibilities for employers with regard to the monitoring of e-mails by encouraging proportionate monitoring in the form of monitoring traffic as opposed to monitoring content. However, employers must inform their employees that monitoring is being carried out. The final Code will not be legally binding but does provide assistance for employers in interpreting their duties under the Data Protection Act.

An additional piece of relevant legislation is the Human Rights Act which also came into force in October 2000 and which incorporates the European Convention on Human Rights into UK domestic law. This further limits the employer's right to monitor employee communications by protecting the employee's right to privacy. There is a fine line to be drawn between monitoring e-mails to protect the business and invasion of privacy. The implementation of the Convention into UK law means that individuals are able to sue for breach of the Convention in the UK courts. The Act is only directly applicable to public bodies, so courts and tribunals are bound by it. However, this means that the Act would extend indirectly to private employers in any dispute to come before the courts. Employers must therefore be careful that information gathered is not used for other purposes, for example to harass the employee, and all employers should be wary of indiscriminate monitoring.

Internet Access and Use Policies

So what can an employer do to protect himself?

The main recommendation is to formulate and publicise policies setting out the permissible and prohibited uses of the Internet and e-mail.

Ideally the policy should be incorporated into the staff handbook and if possible all contracts of employment should be made subject to its terms.

The policy should encompass, among other things:-

- details of the dangers of e-mail abuse;
- procedures for accessing and using the Internet by employees, including scope of access and time limitations e.g. lunchtime access only;
- details of disciplinary action which will be taken against employees found guilty of transmitting defamatory/obscene/ discriminatory material via the Internet;
- procedures for detecting and avoiding computer viruses and making employees aware of the risks such viruses could cause; and
- a comprehensive statement about the monitoring being carried out and the extent to which it is being done.

This legal briefing gives a summary of the law at the date the briefing was written on. Specific legal advice should always be sought in relation to particular matters.

For further information

- contact Joanna Boag-Thomson of Shepherd+ Wedderburn on
Tel 0141 566 8570
Fax 0141 565 1222
e-mail Joanna.bt@shepwedd.co.uk
- visit our website on <http://www.shepwedd.co.uk>

Scottish Enterprise
150 Broomielaw
Atlantic Quay
Glasgow G2 8LU
Network Helpline: 0845 607 8787
Email: network.helpline@scotent.co.uk
www.scottish-enterprise.com/ebusiness

Scottish Enterprise e-Business initiatives
are delivered in partnership with



SE2873/April03

