CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Companies need clear internet use policy
Authors	Whelan, Darius
Publication date	2004-05-31
Original Citation	Whelan, D. (2004) 'Companies Need Clear Internet Use Policy', The Irish Times, 31 May.
Type of publication	Contribution to newspaper/magazine
Link to publisher's version	http://www.irishtimes.com/opinion/companies-need-clear-internet-use-policy-1.1142796
Rights	© 2004 The Irish Times Limited
Download date	2026-11-04 21:04:13
Item downloaded from	https://hdl.handle.net/10468/2614



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Companies need clear Internet use policy

Darius Whelan

Irish Times, 31 May 2004

The Bank of Ireland chief executive's resignation on Saturday after he accessed websites containing links to adult material highlights the need for employers and employees to be aware of legal issues concerning Internet use at work. This area involves a delicate balance between employers' interests and employees' rights, and care must be taken to draw up a policy which addresses both sides of the equation.

The employers' interests include their general power to determine work tasks and control contract performance, their property interests in computer equipment, and their duty to safeguard employees' health and safety.

The key right of employees at issue is their right to privacy, although their freedom of expression may also be relevant. People are sometimes surprised to hear talk of employees' privacy in the workplace, but employees do not leave their privacy at the front door when they come to work. For example, an employee could receive a phone call from his or her partner about a family matter while at work and it would hardly be expected that the employee should refuse to take the call on a work phone, or that the employer should easily be able to eavesdrop on the conversation. The European Court of Human Rights has confirmed the existence of workplace privacy rights in *Niemietz v Germany* (1992) and *Halford v UK* (1997).

Employees can misuse the Internet in various ways, ranging from brief consultation of sports results websites to commission of criminal offences.

It is now widely known that possession of child pornography is a criminal offence, but it is important that the broad scope of the definition of child pornography be appreciated: it can cover any image of a sexual nature of a person under 17 years of age, and can even extend to cartoons which depict child characters, such as Bart Simpson.

Legislation concerning child pornography contains harsh penalties because most of it involves trade in images of actual abuse of children. It is now being suggested that the use of the term "pornography" is inappropriate, with replacements such as "child abuse images" conveying more accurately the seriousness of the crime.

Adult pornography is in an entirely different legal league, and regarded as far less serious a matter.

Mere viewing of adult pornography is not normally a criminal offence, but there is potential criminal liability at common law for distribution of such images, which could apply to employees who forward e-

mails of this kind to each other, although prosecution is unlikely. In addition, if employees circulate adult pornography to colleagues, this may amount to sexual harassment.
If employers decide to monitor employees' Internet use, this will involve collection of personal data and so the principles in the Data Protection Acts 1988-2003 will apply. This means that, for example, the data must be obtained and processed fairly and the data subject must be informed of the purposes for which data are processed.

Covert monitoring, without advance notice to employees, will rarely be permissible, except perhaps in the context of investigation of criminal offences.

The Data Protection Commissioner has emphasised that a clear statement of workplace policy on Internet and e-mail use is needed. A code of practice has been drawn up by the UK's Information Commissioner and a similar code may be drafted in Ireland in due course. It is also possible that the EU may issue a draft Directive on Employment and Privacy this year.
The absence of a workplace policy on Internet use may prove fatal to any attempt to dismiss an employee for such reasons. This is illustrated by the Employment Appeals Tribunal case of *Mehigan v Dyflin Publications* (2002), where the employee had allegedly received three adult pornographic images by e-mail and forwarded them on to another person.

The tribunal said that it would be heavily influenced by the existence of a written policy reserving the right to dismiss for Internet misuse and that it would be unlikely that dismissal would be permissible otherwise.

A possible exception would be the downloading of "obscene" pornography, a classification which the tribunal did not explain in detail, but presumably might include child abuse images. As the employee in this case had not been notified of a policy against Internet misuse, his dismissal was found to be unfair.

His award of compensation was reduced to €2,000 because he was found to have contributed substantially to his own dismissal.

Many employers already have policies on Internet use in place, as appears to have been the case with Bank of Ireland. Those who have not yet done so would be well advised to prepare a detailed document balancing the employers' interests and employees' rights.
Once a policy exists, it is important to review it annually in light of recent legal developments, and to circulate it to all employees regularly.

Dr Darius Whelan lectures in the Faculty of Law at University College Cork
d.whelan@ucc.ie