

No surfing

Internet access for employees is vital to modern business, but a potential minefield for misuse and litigation. **Claire S Harrington** explains how companies can strike a balance

RESearch PUBLISHED on 9 July 2002, carried out for *Personnel Today* and *WebSense*, highlighted the fact that one quarter of UK companies have dismissed employees for internet misconduct. This statistic emphasises the need for employers to have in place appropriate procedures to monitor, investigate and, if necessary, fairly dismiss employees for inappropriate use of the internet.

Most companies readily accept the internet has become an indispensable business tool allowing them to advertise their capabilities, buy and sell services and communicate with a wider customer base than ever before. However, to remain an aid and not a distraction, there is a clear need to monitor and control employees' internet use. The dilemma faced by employers is how to strike a balance between patrolling use, while continuing to encourage strong and trusting relationships with staff.

Monitoring

The number of UK firms making use of spe-

cial monitoring software has increased over three years from 17 per cent to 45 per cent. An employer may now control access to certain sites and tailor restrictions on computer use to individual employees. Such monitoring is likely to result in increased employee productivity and may also prevent the employer being 'cyberliable' in a range of circumstances.

For example, it is significant that 69 per cent of the dismissals for internet misuse were for employees surfing pornographic websites. This activity has a range of legal consequences for employers. An employer may be held liable for an employee who downloads and distributes offensive material to another employee. Such personal surfing has also been deemed to constitute sex discrimination. In *Morse v Future Reality Ltd* (22 October 1996 Case no 54571/95), the tribunal heard male employees were accessing pornographic sites and downloading images. The tribunal accepted this activity was not directed personally at the female applicant

but it did amount to sex discrimination on the grounds of harassment. The respondents were liable because of their failure to take any action to prevent the discrimination. Using monitoring software to prevent access to such sites would have been an example of such action.

One of the most difficult aspects of any policy is the extent of monitoring and interception. The current legal framework allows an employer to have the 'lawful authority' to monitor communications in a limited number of circumstances (see the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000 No 2699)). These circumstances include investigating or detecting unauthorised use of the system. An employer will also have 'lawful authority' where he has gained the consent of both the sender and recipient of the communication.

The most effective systems of monitoring will be those both known about and consented to by the employee and which interfere minimally with the employees functions.

An excessive and heavy handed approach to monitoring is to be avoided. Not only may an employee regard it as undue interference but it may also amount to a breach of the implied term of the mutual duty of trust and confidence. This, in turn, opens the door to the employee to bring a claim for constructive dismissal. Various unions and the TUC have already warned of the dangers monitoring causes to the employer/employee relationship. The National Secretary from the MSF said:

"The rhetoric of many employers is that their employees are their greatest assets. But they are treating their staff like they are the company's greatest enemy. If an employer doesn't trust you, then why should you trust them?"

However it is not just employees who are objecting to this Big Brother type of monitoring. The Government was widely criticised when it announced plans to extend the number of agencies able to access documents recording an individual's use of the internet and email under the Regulation of Investigatory Powers Act 2000. The issue is seen very much as one of human rights and the need to protect an individual's right to privacy as embodied in the Human Rights Act 1998 ■

Claire S Harrington is a barrister practising from 13 King's Bench Walk

■ Company policy

The starting point for employers is to adopt a policy for internet and computer use generally. An effective policy will have been drafted in consultation with employees and will of course be made known to all employees. The policy should include issues such as:

- The amount of time the employer accepts as reasonable for personal surfing/emailing by employees;
- Details of how the policy will be monitored;
- Details of investigation procedures which will be followed in cases of suspected breaches;
- Examples of conduct which will be regarded as internet misuse; and
- The range of disciplinary sanctions which will be imposed if misuse is discovered, with examples of behaviour attracting each sanction.

This last issue has attracted much comment from the EAT. Complaints of unfair dismissal have been upheld in cases where the employer has failed to make it clear to employees which types of computer misuse will carry which penalties (see *Dunn v IBM United Kingdom Ltd* (1 July 1998 Case no 2305087/97) and *British Telecommunications PLC v Rodrigues* (EAT 20 February 95 845/92)). In the latter case the Tribunal noted that neither the company's disciplinary code nor any other company literature made it clear that incidents of computer misuse would automatically result in summary dismissal. The applicant's complaint that the summary dismissal was unfair was accordingly upheld.