**The internet is a widely used means of obtaining information, banking, paying bills, ordering goods and communicating. Its use by employees needs to be controlled otherwise their productive time could be reduced, says Terry Corbitt.**

# Managing employees' **internet surfing**

All organisations should implement an internet acceptable use policy (AUP) and this should be written into contracts of employment. The AUP should set out what is acceptable to the organisation and to what extent the internet can be used by employees for personal purposes. The AUP satisfies legal requirements for employers to notify employees before monitoring their communications. It protects the employer against claims of false dismissal and if a case should come to court, the employer has evidence that would be inadmissible without such notification of company policy.

**'Having an internet acceptable use policy (AUP) is essential'**

A survey by Croner, a leading provider of business information and advice, has revealed that more than half of UK employers could be losing money by not monitoring employees' use of the internet at work. 15% of the human resource professionals polled by Croner say that they do not have an AUP while 38% who do have an AUP say that they do not strictly enforce it and trust employees to stick to its guidelines. Only 42% said that they strictly monitor their AUP and take disciplinary action against employees who break their rules. The other 5% responded that they currently do not have access to the internet.

Richard Smith, human resources expert at Croner, warned employers that by not having a strictly enforced internet acceptable use policy and simply trusting employees to stick to it, they are encouraging a culture of secret surfing.

He went on to say, "Internet access is now common in our workplaces and has become an essential part of the way we work. However, it offers a host of distractions, from visiting popular sites such as e-Bay and Amazon, doing internet banking and buying the weekly groceries to catching up on emails or planning a holiday. While the survey showed that most organisations have some sort of internet policy, if it is not enforced then it may as well not exist. Having an AUP for the use of the internet is just as essential as guidelines for personal phone calls and should be stated in the contract of employment."

Mr Smith is advising employers to take a realistic approach to AUPs rather than banning all websites unrelated to work. He said, "Using the internet to pay a bill at lunchtime or surfing over a sandwich is unlikely to impact on productivity. In fact allocating employees time to complete chores or catch up on personal interests could even boost concentration and morale, helping them to begin the afternoon focused and refreshed."

Some of the employers surveyed allow access to certain restricted websites, such as banks and supermarkets, over a specified lunch period, while others choose to monitor employees' surfing behaviour via their IT department, which can report a problem which can then be dealt with accordingly. Employers can stop employees

*Companies should implement a sensible internet policy for employees*

viewing pornographic and illegal websites through a filtering system, which will automatically deny access to certain websites.

Mr Smith concluded, "To control secret surfing the AUP should be clearly communicated to all employees. If an amount of free surf time is allocated, this should be explained and the consequences of breaking the rules clearly stated. Then if an employee disregards the policy the employer is justified in taking disciplinary action. Secret surfing could be eliminated by employers blocking access to all websites unrelated to work, or by closely monitoring and assessing employees surfing time.

"However this 'big brother' approach is impractical and time consuming and generally not necessary if a reasonable, common sense policy is in place which gives a degree of personal internet time so surfing does not have to be done in secret."

**Code of practice for employers**

When the Data Protection Act 1998 was first implemented, the then data protection commissioner, Elizabeth France, promised a code of practice for employers, the object of which was to protect the privacy of employees. Richard Thomas, the information commissioner at the Data Protection Commission, has addressed the whole question of employee monitoring. In June 2003 he introduced a code of practice called The Employment Practices Data Protection Code, the third part of which, 'Monitoring at Work' sets out the restrictions on employers when monitoring their employees and the information held about them.

The full details of this are available from the Data Registrars' office, either by post or from their website, this covers a wide range of surveillance activities including opening emails or voicemail, checking internet usage and recording with CCTV cameras.

The Code sets out how employers should comply with the Data Protection Act and encourages respect for Article 8 of the Human Rights Act, which creates a right to respect for personal correspondence. The code of practice is designed to introduce tighter control over the use of employee records in three key areas:

• Employee surveillance involving collection of data to monitor performance or detect problems by interception of email and voicemail, checking internet usage and using CCTV for monitoring;
• Automated processing eg CV scanning, aptitude and psychometric testing and the extent to which employment decisions might be taken by automatic means;
• Collection of new and sensitive information eg genetic tests or results of alcohol or drug testing.

Mr Thomas said, "In reality there are few circumstances in which covert monitoring is justified. Monitoring in the workplace can be intrusive, whether examining emails, recording phone calls or installing CCTV cameras. Employees are entitled to expect that their personal lives remain private and that they have a degree of privacy in the work environment. Only in exceptional circumstances will it be appropriate for employers to monitor their employees without their knowledge". Breaches of the Code of Practice are now likely to be cited in employment tribunals.

The CBI felt that the Information Commissioner had not gone far enough to address business concerns. John Cridland, CBI Deputy Director General, said, "It is crucial for business to know where monitoring ends and unwarranted intrusion begins. "

The Code of Practice will be reviewed regularly to ensure it remains up to date in the light of changes in the law, developments in the interpretation of data protection and legislation, increased availability and use of technology evolution of good employment practice.

Visit *www.informationcommissioner.*gov.uk for more information and to download the Employment Practices Data Protection Code.