AccountancyAge

Staff email and internet: where do you draw the line?

by Anne Hughes, Fox Solicitors

24 May 2012

IN A WORLD where everyone is glued to their smartphones and addicted to Facebook and Twitter, there are still a few people (usually those over 20) who want their personal communications to remain private. There has been much controversy recently over the government's proposals to introduce new laws allowing it to snoop on all electronic communications of UK citizens without a warrant. But how do people feel about their employers snooping on their personal communications?

Accountants play an important role in steering a company's attitude and policy as regards protecting its reputation and confidential information. The risks are changing as technologies develop and employee behaviours change.

You need to assess the risks (and quantify the potential costs), and consider whether they justify the intrusion into an employee's privacy.

Carrying a Blackberry 24/7 means that the line between your work and your private life becomes more blurred, and most of us use work email for personal use. iPads are the latest "must have" executive accessory for work and play, and many people don't think twice about forwarding confidential company documents to their personal email accounts so that they can access them away from their desks.

This helps us cram more working hours into our days, and so has an obvious upside for productivity. But there are downsides too. Sensitive confidential information may be lost or stolen. As staff "tweet" about their day, or post comments on Facebook about their boss's latest antics, their right to freedom of expression and privacy comes into direct conflict with the company's interests to protect its professional reputation.

This has led to a string of employment tribunal cases hitting the news in the past couple of years.

An employer can be far more confident taking action to monitor and investigate employees, and taking disciplinary action, if there are clear written policies in place beforehand, so that everyone knows where they stand. This can save substantial costs in fighting or paying-off legal claims by employees.

Here are some pointers:

• The business should have a clear internet and electronic communications policy for staff, which lays down the ground rules and explains the consequences of failure to comply.
• Staff should be required to be familiar with the policy and warned that a breach of it will be treated as serious misconduct, which could lead to dismissal.
• If employees are expected to work away from the office, they should be provided with a secure way of accessing the confidential information needed to get the job done.
• If you want to monitor an employee's use of emails and internet at work, the Employment Practices Code published on the Information Commissioner's Office's website is essential reading (www.ico.gov.uk). Do not assume that the company has the right to inspect all communications sent and received (and internet content accessed) from the employee's computer and blackberry just because the devices belong to the company. If the company generally allows (or tolerates) employees using their work computers to send personal emails and to access social networking websites for personal use, there may be a legitimate expectation of privacy in respect of those activities.

If it is discovered that an employee has forwarded confidential information to their personal email account, the company will want to make sure that the information has not been misused or leaked. Often, an employer's first step is to carry out an investigation (including a forensic IT investigation and an interview with the employee concerned).

Then, the company may ask the employee to give written undertakings to confirm that the information has not been misused or disclosed to any third parties. The company can then decide whether disciplinary action is appropriate.

If the company believes that there may be company information stored on an employee's personal computer or other device, it may wish to inspect those devices and delete the relevant information. However, most employees will regard this to be a gross intrusion into their privacy; most of us store a huge amount of personal information and photographs on our personal computers, belonging to us and our families.

Any proposed process for inspecting an employee's personal devices must show respect for their privacy and property. Here are some tips on best practice:

• Appoint an independent IT expert, who will inspect the employee's devices only with their consent and under their supervision.
• The scope of the IT expert's job should be very clearly defined and explained to the employee in advance.
• The IT expert should enter into a separate confidentiality agreement with the employee, agreeing not to disclose to any third party information belonging to the employee.
• In return for the employee's co-operation, the company may be willing to indemnify the employee in respect of any damage to their device, software or personal data (including deletion).

This generation of staff has learnt how to multi-task so that we are almost constantly online. It seems that we are still working-out where the dividing line should be, between work and our private lives. The challenge for employers now is to help staff understand when it is appropriate to switch on and off from work, and when to keep them separate.

*Anne Hughes is a senior associate at **Fox Solicitors***