Internet use may not have been a key feature of the manufacturing sector in the past, but this is changing rapidly. From the supply chain to the shopfloor, IT systems are more prevalent and the internet is fast becoming an vital part of working life. There are still some manufacturing firms that do not use the internet directly for business purposes, but even these organisations tend to provide employees with internet access at break times.

Generally, internet access is regarded as a positive by both employers and employees alike. If correctly used, it can offer a number of benefits, not least the fact that employees can conduct their personal business (such as banking/shopping) from the workplace, without having to take time off work.

While the growing use of the internet is popular, it can sometimes be perceived as a headache by employers and by HR managers. It is easy to see why: research carried out by internet security specialist Clearswift in November last year revealed that more than 50% of employers had to deal with internet misuse by employees.

The most recent problem encountered by employers has been badged ‘cyberslacking’ – where employees spend large amounts of their working day surfing personal websites. Social networking sites, such as Facebook and MySpace, are the latest websites to be blamed for distracting employees from their work, but they are not the only culprits. The internet now offers users the opportunity to shop online, chat online, even watch television online – and this is proving extremely tempting for employees. In a recent case to hit the headlines, one employee of Neath Port Talbot Council was dismissed and two others resigned after it was discovered that each had been spending up to two hours a day browsing on the auction website eBay. And cyberslacking is not the only issue. Other common internet 'offences' include excessive use of email, viewing inappropriate material, such as pornography, and forwarding offensive emails.

With these concerns in mind, it is no surprise that many employers decide to monitor employees’ internet use. Obviously, the purpose of monitoring is to collect information; however, employers must remember that with information comes obligations. The two main pieces of legislation in this area are the Data Protection Act 1998, which regulates how personal information can be used, and the Human Rights Act 1998, which gives every individual a right to respect for their private life. To ensure they stay within the law, employers should ensure that they have comprehensive internet usage policies in place, which clearly state the standard of behaviour that is expected from employees. If internet use is to be monitored, the policy should tell employees about the reasons for monitoring, the type of information that will be obtained and how that information will be used. The policy should make it clear that any breach will be treated as a disciplinary offence. Ideally, employees should be required to sign the policy to indicate that they have read and understood it.

Even the best policies will only be effective if they are enforced correctly, so employers should be proactive in following up any breaches. It is also important to ensure that any disciplinary action taken is applied consistently. Employers cannot fairly expect to discipline some employees for breaches of the policy while turning a blind eye to other similar breaches.

Back in 2002, computer giant Hewlett Packard (HP) was caught out by its inconsistent approach to disciplinary treatment concerning internet use. The problem arose after the company dismissed three employees who had been caught sending explicit emails in breach of its internet and email policy. During the course of its investigations, HP discovered that over 100 other employees had also been abusing the policy, yet none of these were dismissed. The three employees subsequently brought a claim in the Scottish Employment Tribunal for unfair dismissal. HP’s inconsistent approach was one of the main factors which led the Tribunal to hold that the employees had been unfairly dismissed.

The message for other employers to take from this decision is that if a policy is not being taken seriously and employees are breaching it routinely, it is likely to be considered unfair to take action against employees who just happen to ‘get caught’.

Despite the potential pitfalls surrounding the use of the internet, it is possible for employers to manage the risks without damaging employee relations. The key to success is knowing where the risks lie and implementing a clear policy to reduce those risks. Whatever approach employers choose to take, one thing is clear – the internet is here to stay and employers must be prepared to adapt their practices and procedures to meet this challenge.

Sara Sawicki is a partner in the employment law team at Pinsent Masons