Is it ever OK to monitor your employees' use of electronic communications?

In a nutshell, yes – as long as you have clearly defined policies and a valid business reason for doing so. But read on for more details about a recent case that was brought to the European Court of Human Rights for more clarity.

Employers have used various methods of monitoring employees' internet, telephone, email, instant messaging and social media use from the relatively simple checking of internet history to more complex solutions which record every keystroke by the employee.

This very subject was put under scrutiny in a recent ruling by the European Court of Human Rights in the case of Barbulescu v Romania.

The case — Barbulescu v Romania

A Romanian national, employed as an engineer in charge of sales, was asked by his employer to set up a Yahoo Messenger account in order to respond to client enquiries. He was provided with a clear policy prohibiting all personal use of company facilities, including the internet and computers.

He was informed later by his employer that his Messenger communications had been monitored over a nine day period and he'd been found in breach of the company's policy. After the employee denied the allegation, the employer produced a 45 page transcript of messages that had been sent by the employee to his fiancée and brother. The content of these messages was very personal and the employee was subsequently dismissed.

The employee claimed to the Romanian courts that his correspondence was protected by the Romanian Constitution and that his employer had breached the Romanian Criminal Code. These claims were not upheld as it was deemed that the employer had followed Romanian Labour Code in the approach they adopted in his dismissal, and that the employer had a right to check the messages in order to verify that the employee was only using the account for business purposes.

He then complained to the European Court of Human Rights that his dismissal was in breach of his rights under Article 8 of the European Convention on Human Rights, declaring that the Romanian state had failed to protects his rights on his behalf.

The ruling

The court ruled that, even though Article 8 does protect personal correspondence and private life, the fact that the employer had a clear policy in place meant that the employer was within their rights to monitor the use of work computers to ensure that work was carried out properly and that its policies were being adhered to. Consequently, the employee's rights had not been violated.

Particular importance was placed by the court on the following:

- The employer had a clear policy in place
- The monitoring was limited in scope and proportionate
- When accessing the messages, the employer assumed that they contained only work-related communications

In addition to the above, the employee did not explain clearly why he used the account for personal correspondence and had previously been made aware that a predecessor had already been dismissed for using company facilities for personal use.

What does this mean for me as an employer?

Importantly, what it doesn't mean is that you have free reign to snoop on your employees and everything they do. Even though the Data Protection Act 1988 doesn't stop you from monitoring your employees, under the Regulation of Investigatory Powers Act 2000 (RIPA) it is unlawful to 'intercept' communications unless an exception, listed within the Act, applies. One of these being where the interception is to 'ascertain compliance with regulatory or self-regulatory practices' – ie: ensuring employees adhere to your policy.

What it does mean is that you must have a clear policy in place outlining what you expect from your employees in terms of their use of company facilities, setting out the nature and extent of any monitoring you will be carrying out and what the consequences will be for breaching the policy.

Any monitoring you wish to undertake must have a legitimate business objective and be both reasonable and proportionate.

The Employment Practice Code set out by the Information Commissioner's Office advises employers to get their employees to mark any personal/private correspondence as such. Where this is done, the employer doesn't necessarily need to read the communication to ascertain that the company policy has been breached. If you do subsequently read those message, you run the risk of violating their rights.

This code of practice also recommends that employers carry out an impact assessment to decide if and how to carry out employee monitoring, as follows:

- Clearly identify the purpose behind the monitoring and the benefits of it
- Identify any adverse consequences it could have on your employees
- Consider alternatives
- Judge whether monitoring is justified