



# The Data Protection Code: monitoring at work

Employment, pensions & benefits: briefing 91

## Executive summary

The third part of the Employment Practices Data Protection Code limits the circumstances in which employers can monitor the activities of their staff. In this briefing we look at what amounts to monitoring; the steps employers should take when deciding whether monitoring is justified; and good practice to adopt if monitoring is carried out.

The third part of the Employment Practices Data Protection Code (the Code) was published on 11 June 2003. The Code aims to help employers comply with the Data Protection Act 1998 (the Act) when processing employees' personal data. For further information on the Code as a whole, see our briefing *The Data Protection Code: recruitment and selection*.

Part three focuses on the steps employers must take to comply with the Act when monitoring their staff. After strong lobbying from employer organisations, the Code is noticeably more business-friendly than the original draft produced in 2000. The information commissioner has also produced supplemental guidance to the Code, designed to give large employers 'a better understanding' of the issues raised. Despite this, the Code still places significant limitations on employers' ability to monitor their staff.

The main provisions of the Code and the supplemental guidance are outlined below. The Code states that where electronic communications are intercepted, the provisions of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 will also apply. The requirements of those Regulations are not dealt with in this briefing.

## Monitoring

The Code describes monitoring as 'activities that set out to collect information about workers by keeping them under some sort of observation', whether directly or through the use of electronic systems. Such monitoring

may be routine, adopted for all or some workers as a matter of course, or one-off and introduced in response to a particular problem. Both types of monitoring are covered by the Code if a manual record is made or automated processing is carried out. Reviewing a log of websites visited by employees, accessing employee voicemails and checking email accounts can all amount to monitoring.

However, the Code is only likely to apply if the purpose of monitoring is to check the performance or conduct of employees. The Code does not cover access to records kept in the normal course of business that are accessed only in response to a particular concern or query, such as a customer complaint. This will be of some comfort to employers – for example it should mean that reviewing an employee's email account in response to pending or threatened litigation should not be covered by the Code.

## Impact assessments

If monitoring is carried out to assess conduct or performance, the key to complying with the Act will be to do an impact assessment before any monitoring starts. An impact assessment involves balancing the employer's interests in the proposed monitoring with the possible prejudice to the employee, before deciding whether monitoring is justified. The Code outlines a five-step process, described below.

- Identify the purpose of the monitoring and likely benefits for the business.
- Identify any adverse impact the monitoring will have

– both for employees and for customers. The employer will need to consider how far the monitoring will interfere with the privacy of workers; whether employees will know about the monitoring; the impact of the monitoring on other relationships (such as those between employees and trade union representatives); and whether confidential or other private information will be seen by people without a business need to have access to that material.

- Consider whether the same benefits can be achieved in a different, less intrusive way. For example, it might be possible to use training or supervision to ensure correct use of a particular system rather than monitoring. One-off monitoring in response to a particular incident may be as effective as continuous monitoring. A small group of ‘high risk’ roles could be monitored instead of checking all staff. Automated monitoring may in some cases be less intrusive than that carried out by individuals.
- The employer will have obligations to staff as a result of monitoring. Employees should be notified about the monitoring that is being conducted and will be able to obtain a copy of processed data. These obligations need to be taken into account in the impact assessment.
- Balancing these factors will help the employer to take a decision about whether the proposed monitoring is justified. The Code stresses that fairness to workers is the most important factor. The least intrusive degree of monitoring consistent with business objectives should be adopted. Monitoring that entails a serious intrusion into the private life of staff can only be justified where a business is at serious risk of harm.

The Code indicates that the nature of the impact assessment will vary depending on the type of monitoring to be carried out. Where the risk is obvious and the monitoring proposed fairly limited, a quick and informal assessment may be sufficient. As a general rule, the more intrusive the monitoring proposed, the more important it will be to carry out a careful and properly documented impact assessment.

Assuming that an employer can justify monitoring having carried out an impact assessment, it will not be necessary to obtain the consent of employees.

## Good practice

The Code contains a series of good practice recommendations for employers to adopt in monitoring staff. It sets out principles with supporting action points that replace the benchmarks, accompanying notes and examples used in earlier parts of the Code.

### Managing data protection

This section reflects the benchmarks and notes on managing data protection contained in the first part of the Code. It concentrates on the need to establish proper compliance procedures and to ensure that staff are aware of their data protection obligations and the sanctions that apply if these are not observed.

### General approach to monitoring

The Code proceeds on the basis that that monitoring is intrusive and that workers are entitled to respect for their privacy at work. If monitoring is justified workers should be made aware that it is taking place, unless there are exceptional circumstances.

### Key points/actions

- Those who can authorise monitoring should be identified and they must be familiar with the Act and the Code.
- An impact assessment should be conducted before monitoring staff. At the very least the purpose and advantages of monitoring should be weighed against any adverse impact.
- If monitoring is to be used to enforce disciplinary rules, these must be set out in a policy of which workers are aware. The policy should include details about how monitoring will be used to enforce those standards.
- Workers must be told what monitoring is being carried out and the reasons for it. This includes information about when monitoring will take place, how it will be used and to whom information will be disclosed. A simple statement that emails (for example) may be monitored is insufficient. It is good practice to remind employees about this from time to time. Any significant changes to monitoring must also be notified.
- The number of people who have access to personal information should be limited and they should be

familiar with data protection requirements. Employers should also consider who is the most appropriate person to have access to information – it may be more intrusive for a line manager to have access to personal data than someone in an HR function, for example.

- Information obtained through monitoring should only be used for the original purpose for which monitoring was introduced, unless no employer could reasonably be expected to ignore what has been discovered – such as evidence of gross misconduct, criminal activity or breaches of health and safety.
- Workers should have the chance to comment on any information obtained through monitoring before any action is taken against them. This will usually be a vital part of a disciplinary process anyway.

### **Monitoring electronic communications**

Electronic communications include emails, faxes, telephone calls and internet access. The Code stresses the need for employers to introduce a policy on the use of such systems and make workers aware of the policy. It should include information about the terms on which employees are entitled to make private use of work systems – if at all. Any restrictions on internet access must be clear. For example, it will be insufficient to say that ‘offensive material’ cannot be accessed – an employer will need to be explicit about what is viewed as offensive. Details about what monitoring is carried out and why should also be covered. The sanctions for breach of the policy must also be clear.

The supplemental guidance also points out that the existence of a policy will not in itself determine a worker’s expectation of privacy – the policy must also be enforced consistently.

### **Key points/actions**

- Monitoring of electronic communications should be as limited as possible. Automated monitoring for viruses or unauthorised access may be less intrusive than monitoring actual communications. Web-filtering software could be used to prevent misuse of the internet. It might be sufficient to use an itemised call record, analysis of email traffic or the amount of time spent on the internet in preference to monitoring the content of communications.

- The content of emails should generally not be monitored. Monitoring should be confined to address and header information unless it is essential to monitor content. The supplemental guidance points out that even where an employer does not allow personal use of a system it will not always be necessary to look at email content in enforcing those rules – action could be taken on the basis of header information.
- The benefits of the proposed monitoring must outweigh the adverse impact. Employees must be aware of the monitoring that is being carried out – for example that voicemails and emails are checked in their absence. Employees should be able to protect emails by marking them ‘personal’, and emails marked in this way should be opened only in exceptional circumstances.
- Those emailing or calling employees (ie third parties) must also be aware that monitoring is being carried out – either through the use of recorded messages or by an instruction to staff to tell callers about the extent of monitoring.
- Workers should be told about an employer’s access to information about personal use of business equipment such as mobile phones.
- Staff should know how long information about emails and internet access is kept.

### **Video and audio monitoring**

This section deals with video surveillance of workers such as the use of CCTV, or the recording of conversations between workers (as opposed to telephone conversations). The supplemental guidance says that continuous monitoring will be particularly difficult to justify because of its intrusive nature.

### **Key points/actions**

- As with all monitoring, an impact assessment should be conducted before monitoring starts. Generally the use of CCTV should be restricted to public areas where employees do not expect privacy.
- Workers should be informed of where and why monitoring is being carried out. Simply telling the employees that monitoring may be carried out from time to time is insufficient. The supplemental guidance even suggests staff should be told the location of cameras and microphones. Third parties

who might be caught, such as visitors, should also be informed about monitoring, by notices or other means.

### Covert monitoring

Covert monitoring will only be justified in exceptional circumstances, such as suspected criminal activity or other malpractice, where notifying staff about the monitoring would prejudice the ability of an employer to detect the conduct. The supplemental guidance suggests that covert monitoring may be justified where the suspected activity could reasonably lead to police involvement.

### Key points/actions

- It will usually be appropriate for covert monitoring to be authorised by a senior manager. Covert monitoring should only be used as part of a specific investigation within a limited timeframe. The number of people involved in the investigation should be as limited as possible and clear rules about access to information should be in place.
- Monitoring should not take place in areas where employees reasonably expect privacy – such as private offices. The only exception would be where serious criminal activity is suspected, in which case the police should be involved.
- Information discovered through covert monitoring should not be used other than for the purpose for which it was collected, unless it reveals matters that no employer could reasonably ignore.

### In-vehicle monitoring

The Code applies where vehicles are fitted with devices that monitor information such as distances travelled and location, and this information is collected in relation to a specific driver. Most importantly, an impact assessment should be conducted.

### Key points/actions

- Any conditions attaching to private use of a company vehicle should be clearly set out and workers should be aware of the policy. Information about monitoring that takes place and how any information will be used should be included.
- Monitoring private use of a company vehicle will not generally be permitted. A monitoring device should

be disabled when a vehicle is in private use. An exception arises where the employer is legally required to monitor all usage, as might be the case for vehicles fitted with tachographs.

### Monitoring through third parties

In some cases employers will want to access information about workers held by third parties, such as credit reference agencies, or by the employer in a different capacity from employer, for example as a banker for a member of staff. Again, an impact assessment must be conducted before any such information is accessed and workers should be aware of what checks are being carried out and why.

### What next?

In the short term, the most important action for employers is to review their information technology policies to ensure they reflect the provisions of the Code. The employer should also consider whether existing monitoring is justified under the new principles. Even if such monitoring is justified, in the future it is likely employers will have to be much more explicit with employees about the type of monitoring that is being carried out and why. Failing to do so is likely to result in increasing numbers of complaints to the information commissioner – either on an individual or collective basis.

For further information please contact

Nicholas Squire  
T +44 20 7936 4000  
F +44 20 7832 7001  
E [nicholas.squire@freshfields.com](mailto:nicholas.squire@freshfields.com)

Joanna Broadbent  
T +44 20 7936 4000  
F +44 20 7832 7001  
E [joanna.broadbent@freshfields.com](mailto:joanna.broadbent@freshfields.com)