part 3–monitoring at work

contents

About Part 3 of the Code

Data protection and monitoring at work

A number of the requirements of the Data Protection Act will come into play whenever an employer wishes to monitor workers. The Act does not prevent an employer from monitoring workers, but such monitoring must be done in a way which is consistent with the Act. Employers – especially in the public sector – must also bear in mind Article 8 of the European Convention on Human Rights which creates a right to respect for private and family life and for correspondence.

How does the Data Protection Act regulate monitoring?

Monitoring is a recognised component of the employment relationship. Most employers will make some checks on the quantity and quality of work produced by their workers. Workers will generally expect this. Many employers carry out monitoring to safeguard workers, as well as to protect their own interests or those of their customers. For example, monitoring may take place to ensure that those in hazardous environments are not being put at risk through the adoption of unsafe working practices. Monitoring arrangements may equally be part of the security mechanisms used to protect personal datapersonal information. In other cases, for example in the context of some financial services, the employer may be under legal or regulatory obligations which it can only realistically fulfil if it undertakes some monitoring. However where monitoring goes beyond one individual simply watching another and involves the manual recording or any automated processing of personal information, it must be done in a way that is both lawful and fair to workers.

Monitoring may, to varying degrees, have an adverse impact on workers. It may intrude into their private lives, undermine respect for their correspondence or interfere with the relationship of mutual trust and confidence that should exist between them and their employer. The extent to which it does this may not always be immediately obvious. It is not always easy to draw a distinction between work-place and private information. For example monitoring e-mail messages from a worker to an occupational health advisor, or messages between workers and their trade union representatives, can give rise to concern.

In broad terms, what the Act requires is that any adverse impact on workers is justified by the benefits to the employer and others. This Code is designed to help employers determine when this might be the case.

What does this part of the Code cover?

This part of the Code applies where activities that are commonly referred to as “monitoring” are taking place or are planned. This means activities that set out to collect information about workers by keeping them under some form of observation, normally with a view to checking their performance or conduct. This could be done either directly, indirectly, perhaps by examining their work output, or by electronic means.

This part of Code is primarily directed at employers – especially larger organisations – using or planning some form of **systematic monitoring**. This is where the employer monitors all workers or particular groups of workers as a matter of routine, perhaps by using an electronic system to scan all e-mail messages or by installing monitoring devices in all company vehicles.

The Act still applies to **occasional monitoring**. This is where the employer introduces monitoring as a short term measure in response to a particular problem or need, for example by keeping a watch on the e-mails sent by a worker suspected of racial harassment or by installing a hidden camera when workers are suspected of drug dealing on the employer’s premises.

This part of the Code deals with both types of monitoring, but it is likely to be of most relevance to employers involved in systematic monitoring, which will generally be larger organisations.

Examples of monitoring

There is no hard-and-fast definition of 'Monitoring' to which this part of the Code applies. Examples of activities addressed in this part of the Code include:

- gathering information through point of sale terminals, to check the efficiency of individual supermarket check-out operators
- recording the activities of workers by means of CCTV cameras, either so that the recordings can be viewed routinely to ensure that health and safety rules are being complied with, or so that they are available to check on workers in the event of a health and safety breach coming to light
- randomly opening up individual workers' e-mails or listening to their voice-mails to look forevidence
  of malpractice
- using automated checking software to collect information about workers, for example to find out whether particular workers are sending or receiving inappropriate e-mails
- examining logs of websites visited to check that individual workers are not downloading pornography
- keeping recordings of telephone calls made to or from a call centre, either to listen to as part of workers training, or simply to have a record to refer to in the event of a customer complaint about a worker
- systematically checking logs of telephone numbers called to detect use of premium-rate lines
- videoing workers outside the workplace, to collect evidence that they are not in fact sick
- obtaining information through credit reference agencies to check that workers are not in financial difficulties.

Outside this part of the Code

There are other activities that this part of the Code does not specifically address. Most employers will keep some business records that contain information about workers but are not collected primarily to keep a watch on their performance or conduct. An example could be records of customer transactions – including paper records, computer records or recordings of telephone calls. This part of the Code is **not** concerned with occasional access to records of this type in the course of an investigation into a specific problem, such as a complaint from a customer.

See Part 2: Employment Records for guidance relating to grievance and disciplinary investigations.

Examples of activities not directly addressed in this part of the Code include;

- looking back through customer records in the event of a complaint, to check that the customer was given the correct advice
- checking a collection of e-mails sent by a particular worker which is stored as a record of transactions, in order to ensure the security of the system or to investigate an allegation of malpractice
- looking back through a log of telephone calls made that is kept for billing purposes, to establish whether a worker suspected of disclosing trade secrets has been contacting a competitor.

Impact assessments

The Data Protection Act does not prevent monitoring. Indeed in some cases monitoring might be necessary to satisfy its requirements. However, any adverse impact of monitoring on individuals must be justified by the benefits to the employer and others. We use the term "impact assessment" to describe the process of deciding whether this is the case.

In all but the most straightforward cases, employers are likely to find it helpful to carry out a formal or informal 'impact assessment' to decide if and how to carry out monitoring. This is the means by which employers can judge whether a monitoring arrangement is a proportionate response to the problem it seeks to address. This
Code does not prejudge the outcome of the impact assessment. Each will necessarily depend on the particular

circumstances of the employer. Nor does the Code attempt to set out for employers the
benefits they might gain from monitoring. What it does do is assist employers in identifying and giving appropriate weight to the other factors they should take into account.

An impact assessment involves;

- identifying clearly the **purpose(s)** behind the monitoring arrangement and the benefits it is likely to deliver
- identifying any likely **adverse impact** of the monitoring arrangement
- considering **alternatives** to monitoring or different ways in which it might be carried out
- taking into account the **obligations** that arise from monitoring
- judging whether monitoring is **justified**.

Adverse impact

Identifying any likely adverse impact means taking into account the consequences of monitoring, not only for workers, but also for others who might be affected by it, such as customers. Consider:

- what intrusion, if any, will there be into the private lives of workers and others, or interference with their private e-mails, telephone calls or other correspondence? Bear in mind that the private lives of workers can, and usually will, extend into the workplace.
- to what extent will workers and others know when either they, or information about them, are being monitored and then be in a position to act to limit any intrusion or other adverse impact on themselves?
- whether information that is confidential, private or otherwise sensitive will be seen by those who do not have a business need to know, e.g. IT workers involved in monitoring e-mail content
- what impact, if any, will there be on the relationship of mutual trust and confidence that should exist between workers and their employer?
- what impact, if any, will there be on other legitimate relationships, e.g. between trades union members and their representatives?
- what impact, if any, will there be on individuals with professional obligations of confidentiality or secrecy, e.g. solicitors or doctors?
- whether the monitoring will be oppressive or demeaning.

Alternatives

Considering alternatives, or different methods of monitoring, means asking questions such as:

- can established or new methods of supervision, effective training and/or clear communication from managers, rather than electronic or other systemic monitoring, deliver acceptable results?
- can the investigation of specific incidents or problems be relied on, for example accessing stored e-mails to follow up an allegation of malpractice, rather than undertaking continuous monitoring?
- can monitoring be limited to workers about whom complaints have been received, or about whom
  there are other grounds to suspect of wrong-doing?
- can monitoring be targeted at areas of highest risk, e.g. can it be directed at a few individuals whose jobs mean they pose a particular risk to the business rather than at everyone?
- can monitoring be automated? If so, will it be less intrusive, e.g. does it mean that private information will be ‘seen’ only by a machine rather than by other workers?
- can spot-checks or audit be undertaken instead of using continuous monitoring? Remember though that continuous automated monitoring could be less intrusive than spot-check or audit that involves human intervention.

Obligations

Taking into account the obligations that arise from monitoring means considering such matters as:

- whether and how workers will be notified about the monitoring arrangements

- how information about workers collected through monitoring will be kept securely and handled in accordance with the Act.

See Part 2 – Employment Records for more information on security requirements.

- the implications of the rights that individuals have to obtain a copy of information about them that has been collected through monitoring.

See Part 2 – Employment Records which explains more about rights to access.

Is monitoring justified?

Making a conscious decision as to whether the current or proposed method of monitoring is justified involves;

- establishing the benefits of the method of monitoring
- considering any alternative method of monitoring
- weighing these benefits against any adverse impact
- placing particular emphasis on the need to be fair to individual workers
- ensuring, particularly where monitoring electronic communications is involved, that any intrusion is no more than absolutely necessary
- bearing in mind that significant intrusion into the private lives of individuals will not normally be justified unless the employer's business is at real risk of serious damage
- taking into account the results of consultation with trade unions or other representatives, if any, or with workers themselves.

See Supplementary Guidance for a chart to help assess the degree of intrusiveness involved in monitoring the content of various types of communication. (Clicking this link opens a new window)

Making an impact assessment need not be a complicated or onerous process. It will often be enough for an employer to make a simple mental evaluation of the risks faced by his or her business and to assess whether the carrying out of monitoring would reduce or eradicate those risks. In other cases the impact assessment will be more complicated, for example where an employer faces a number of different risks of varying degrees of seriousness. In such cases appropriate documentation would be advisable.

Is a worker's consent needed?

There are limitations as to how far consent can be relied on in the employment context to justify the processing of personal information. To be valid, for the purposes of the Data Protection Act, consent must be "freely given", which may not be the case in the employment environment. Once given, consent can be withdrawn. In any case, employers who can justify monitoring on the basis of an impact assessment will not generally need the consent of individual workers.

Are there special rules for electronic communications?

Electronic communications are broadly telephone calls, fax messages, e-mails and internet access. Monitoring can involve the 'interception' of such communications. The Regulation of Investigatory Powers Act, and the Lawful Business Practice Regulations made under it, set out when interception can take place despite the general rule that interception without consent is against the law. It should be remembered that – whilst the Regulations deal only with interception – the Data Protection Act is concerned more generally with the processing of personal information. Therefore when monitoring involves an interception which results in the recording of personal information an employer will need to satisfy both the Regulations and the requirements of the Data Protection Act.

See Supplementary Guidance for more details on The Lawful Business Practice Regulations. (Clicking this link opens a new window)