

THE EMPLOYMENT PRACTICES DATA PROTECTION CODE:

PART 3: MONITORING AT WORK.



CONTENTS

Section 1: About the code.

Section 2: Monitoring Workers

Section 3: Good Practice Recommendations



SECTION 1: ABOUT THE CODE

Our aim:

This Code is intended to help employers comply with the Data Protection Act and to encourage them to adopt good practice. The Code aims to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. It does not impose new legal obligations.

Who is the Code for?

The Employment Practices Data Protection Code deals with the impact of data protection laws on the employment relationship. It covers such issues as the obtaining of information about workers, the retention of records, access to records and disclosure of them. Not every aspect of the Code will be relevant to every organisation - this will vary according to size and the nature of its business. Some of the issues addressed may arise only rarely - particularly for small businesses. Here the Code is intended to serve as a reference document to be called on when necessary.

This part of the Code recommends how your organisation can meet the requirements of the Data Protection Act through the adoption of good practice where you wish to monitor the activities of your workers.

The Benefits of the Code:

The Data Protection Act 1998 places responsibilities on any organisation to process personal information that it holds in a fair and proper way. Failure to do so can ultimately lead to a criminal offence being committed.

The effect of the Act on how an organisation processes information on its workers is generally straightforward. But in some areas it can be complex and difficult to understand, especially if your organisation has only limited experience of dealing with data protection issues. The Code therefore covers the points you need to check, and what action, if any, you may need to take. Following the Code should produce other benefits in terms of relationships with your workers, compliance with other legislation and efficiencies in storing and managing information.

Benefits of the Employment Practices Code:

Following the Code will:

- increase trust in the workplace - there will be transparency about information held on individuals, thus helping to create an open atmosphere where workers have trust and confidence in employment practices.
- encourage good housekeeping - following the Code encourages organisations to dispose of out-of-date information, freeing up both physical and computerised filing systems and making valuable information easier to find.
- protect organisations from legal action – adhering to the Code will help employers to protect themselves from challenges against their data protection practices.
- encourage workers to treat customers' personal data with respect - following the Code will create a general level of awareness of personal data issues, helping to ensure that information about customers is treated properly.
- help organisations to meet other legal requirements - the Code is intended to be consistent with other legislation such as the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA).
- assist global businesses to adopt policies and practices which are consistent with similar legislation in other countries - the Code is produced in the light of EC Directive 95/46/EC and ought to be in line with data

protection law in other European Union member states.

- help to prevent the illicit use of information by workers - informing them of the principles of data protection, and the consequences of not complying with the Act, should discourage them from misusing information held by the organisation.

What is the legal status of the Code?

The Code has been issued by the Information Commissioner under section 51 of the Data Protection Act. This requires him to promote the following of good practice, including compliance with the Act's requirements, by data controllers and empowers him, after consultation, to prepare Codes of Practice giving guidance on good practice.

The basic legal requirement on each employer is to comply with the Act itself. The Code is designed to help. It sets out the Information Commissioner's recommendations as to how the legal requirements of the Act can be met. Employers may have alternative ways of meeting these requirements but if they do nothing they risk breaking the law.

Any enforcement action would be based on a failure to meet the requirements of the Act itself. However, relevant parts of the Code are likely to be cited by the Commissioner in connection with any enforcement action that arises in relation to the processing of personal information in the employment context.

Who does data protection cover in the workplace?

The Code is concerned with information that employers might collect and keep on any individual who might wish to work, work, or have worked for them. In the Code the term 'worker' includes:

- applicants (successful and unsuccessful)
- former applicants (successful and unsuccessful)
- employees (current and former)
- agency staff (current and former)
- casual staff (current and former)
- contract staff (current and former)

Some of this Code will also apply to others in the workplace, such as volunteers and those on work experience placements.

What information is covered by the Code?

It is likely that most information about individuals that is processed by an organisation in the employment context will fall within the scope of the Data Protection Act and therefore within the scope of this Code.

Personal information

The Code is concerned with 'personal information'. That is, information which:

relates to a living person, and

identifies an individual, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession.

All automated and computerised personal information is covered by the Act. It also covers personal information put on paper or microfiche and held in any 'relevant filing system'. In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered. A relevant filing system essentially means any set of information about workers in which it is easy to find a piece of information about a particular individual.

[Note: At the date of publication the case of *Durrant v the Financial Services Authority* is still before the courts. The explanation of 'relevant filing system' is based on the Information Commissioner's previously published advice. This may need to be amended as the case law develops.]

Processing

The Act applies to personal information that is subject to 'processing'. For the purposes of the Act, the term 'processing' applies to a comprehensive range of activities. It includes the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

Examples of personal information likely to be covered by the Act include:

- details of a worker's salary and bank account held on an organisation's computer system or in a manual filing system
- an e-mail about an incident involving a named worker
- a supervisor's notebook containing sections on several named workers
- a supervisor's notebook containing information on only one individual but where there is an intention to put that information in that person's file
- a set of completed application forms

Examples of information unlikely to be covered by the Act include:

- information on the entire workforce's salary structure, given by grade, where individuals are not named and are not identifiable
- a report on the comparative success of different recruitment campaigns where no details regarding individuals are held
- a report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals
- manual files that contain some information about workers but are not stored in an organised way, such as a pile of papers left in a basement

In practice, therefore, nearly all employment-related useable information held about individuals will be covered by the Code.

Sensitive personal information:**What are sensitive data?**

Sensitive data are information concerning an individual's;

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence, or
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Sensitive data found in a worker's record might typically be about their;

- physical or mental health - as a part of sickness records
- disabilities - to facilitate adaptations in the workplace
- racial origin - to ensure equality of opportunity
- trade union membership - to enable deduction of subscriptions from payroll

In the context of monitoring, typical circumstances in which sensitive personal information might be held include;

- health information in e-mails sent by a worker to his or her manager, a personnel department or an occupational health advisor
- trade union membership revealed by internet access logs which show that a worker routinely accesses a particular trade union website
- information about a worker's political opinions or religious beliefs obtained by intercepting and recording a private conversation.

The Act sets out a series of conditions, at least one of which has to apply before an employer can collect, store, use, disclose or otherwise process sensitive data.

See Supporting Guidance page 23 which explains more about the conditions for processing sensitive data

What responsibilities do workers have under the Act?

Workers – as well as employers - have responsibilities for data protection under the Act. Line managers have responsibility for the type of personal information they collect and how they use it. No-one at any level should disclose personal information outside the organisation's procedures, or use personal information held on others for their own purposes. Anyone disclosing personal information without the authority of the organisation may commit a criminal offence, unless there is some other legal justification, for example under 'whistle-blowing' legislation.

Of course, applicants for jobs ought to provide accurate information and may breach other laws if they do not. However, the Act does not create any new legal obligation for them to do so.

Managing Data Protection Page 21 explains more about allocating responsibility.

Other Parts of the Code:

The Employment Practices Data Protection Code has three additional parts,

- **recruitment and selection** – is about job applications and pre-employment vetting.
- **employment records** – is about collecting, storing, disclosing and deleting records
- **medical information** – is about occupational health, medical testing, drug and genetic screening

Each part of the Code has been designed to stand alone. Which parts of the Code you choose to use will depend on the relevance to your organisation of each area covered.

Ask the Information Commissioner for copies of any parts you require or for any further information.

See Supporting Guide, page 39, for contact details or view our website: www.informationcommissioner.gov.uk



SECTION 2: MONITORING WORKERS.

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 information. In other cases, for example in the context of financial services, the employer may be under legal or regulatory obligations which it can only realistically fulfil if it undertakes 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 for evidence 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 to 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 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, Page 47, 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.

Impact Assessments

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 wrongdoing?
- 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, Page 19 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, Page 32 which explains more about rights to access.

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 Supporting Guidance Page 27 for a chart to help assess the degree of intrusiveness involved in monitoring the content of various types of communication

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 data. 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 Supporting Guidance page 28, for more details on The Lawful Business Practice Regulations



SECTION 3: GOOD PRACTICE RECOMMENDATIONS.


There are seven sub-sections in this section of the Code:

- 1. Managing data protection**
- 2. The general approach to monitoring**
- 3. Monitoring electronic communications**
- 4. Video and audio monitoring**
- 5. Covert monitoring**
- 6. In-vehicle monitoring**
- 7. Monitoring through information from third parties**

The good practice recommendations may be relevant to either large or small employers, but they primarily address activities that are likely to be undertaken by those involved with systematic monitoring. As such they are most likely to be relevant to larger organisations. However, how far they are applicable and what is needed to achieve them will, of course, depend very much on the nature and size of each organisation.

Supporting guidance, aimed mainly at those in larger organisations who are responsible for ensuring that employment policies and practices comply with data protection law, includes more detailed notes and examples. These notes and examples, do not form part of this Code.

For Supporting Guidance go to: www.informationcommissioner.gov.uk

A decorative graphic element consisting of a stylized, light blue, curved shape resembling a '9' or a swirl, positioned to the left of the section header.

3.1 Managing data protection

Data protection compliance should be seen as an integral part of employment practice. It is important to develop a culture in which respect for private life, data protection, security and confidentiality of personal information is seen as the norm.

- 3.1.1** Identify the person within the organisation responsible for ensuring that employment policies and procedures comply with the Act and for ensuring that they continue to do so. Put in place a mechanism for checking that procedures are followed in practice

Key points and possible actions

- The nature and size of the organisation will influence where responsibility should rest.
- Ensure the person responsible reads all relevant parts of the Code.
- Check employment policies and procedures, including unwritten practices, against the relevant parts of the Code.
- Eliminate areas of non-compliance.
- Inform those who need to know why certain procedures have changed.
- Introduce a mechanism for checking that procedures are followed in practice, for example, occasional audits and spot checks and/or a requirement for managers to sign a compliance statement.

- 3.1.2** Ensure that business areas and individual line managers who process information about workers understand their own responsibility for data protection compliance and if necessary amend their working practices in the light of this.

Key points and possible actions

- Prepare a briefing to departmental heads and line managers about their responsibilities.

- 3.1.3** Assess what personal information about workers is in existence and who is responsible for it.

Key points and possible actions

- Use the various parts of this Code as the framework to assess what personal information your organisation keeps and where responsibility for it lies.
- Remember that personal information may be held in different departments as well as within the personnel/human resource function.

- 3.1.4** Eliminate the collection of personal information that is irrelevant or excessive to the employment relationship. If sensitive data are collected ensure that a sensitive data condition is satisfied.

Key points and possible actions

- Consider each type of personal information that is held and decide whether any information could be deleted or not collected in the first place.
- Check that the collection and use of any sensitive personal data satisfies at least one of the sensitive data conditions.

See Supporting Guidance Page 23 which explains more about the conditions for processing sensitive data.

- 3.1.5** Ensure that all workers are aware how they can be criminally liable if they knowingly or recklessly disclose personal information outside their employer's policies and procedures. Make serious breaches of data protection rules a disciplinary matter.

Key points and possible actions

- Prepare a guide explaining to workers the consequences of their actions in this area.
- Make sure that the serious infringement of data protection rules is clearly indicated as a disciplinary matter.
- Ensure that the guide is brought to the attention of new workers.
- Ensure that workers can ask questions about the guide.

3.1.6 Ensure that your organisation has a valid notification in the register of data controllers that relates to the processing of personal information about workers, unless it is exempt from notification.

Key points and possible actions

- Consult the Data Protection Register website - www.dpr.gov.uk - to check the notification status of your organisation.
- Check whether your organisation is exempt from notification using the website.
- Check whether all your processing of information about workers is correctly described there – unless your organisation is exempt.
- Allocate responsibility for checking and updating this information on a regular basis, for example every 6 months.

3.1.7 Consult workers, and/or trade unions or other representatives, about the development and implementation of employment practices and procedures that involve the processing of personal information about workers.

Key points and possible actions

- Consultation is not currently mandatory under employment law, but should help to ensure that processing of personal information is fair.
- When formulating new employment practices and procedures, assess the impact on collection and use of personal data.



3.2 The general approach to monitoring.

CORE PRINCIPLES

- **It will usually be intrusive to monitor your workers.**
- **Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment.**
- **If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.**
- **Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified.**
- **In any event, workers' awareness will influence their expectations.**

3.2.1 Identify who within the organisation can authorise the monitoring of workers and ensure they are aware of the employer's responsibilities under the Act.

Key points and possible actions

- There are non-compliance risks if line managers introduce monitoring arrangements without due authority.
- Those who monitor workers, or who can authorise such monitoring, should be briefed on the Act and this Code.

3.2.2 Before monitoring, identify clearly the purpose(s) behind the monitoring and the specific benefits it is likely to bring. Determine – preferably using an impact assessment - whether the likely benefits justify any adverse impact.

Key points and possible actions

- Identify the monitoring that currently takes place in your organisation.
- Identify any monitoring that you plan to implement.
- Consider conducting an impact assessment on either current or planned monitoring based on the guidance on page 15.

3.2.3 If monitoring is to be used to enforce the organisation's rules and standards make sure that the rules and standards are clearly set out in a policy which also refers to the nature and extent of any associated monitoring. Ensure workers are aware of the policy.

Key points and possible actions

- Identify which of your organisation's rules and standards are enforced partly or wholly through the use of monitoring.
- Ensure that these rules and standards are set out in policies that are clearly communicated to workers.

3.2.4 Tell workers what monitoring is taking place and why, and keep them aware of this, unless covert monitoring is justified.

Key points and possible actions

- Ensure that workers are aware of the nature and extent of any monitoring.
- Set up a system (for example by using the workers handbook or via an intranet) to ensure workers remain aware that monitoring is being conducted.
- Tell workers when significant changes are introduced.

- 3.2.5** If sensitive data are collected in the course of monitoring, ensure that a sensitive data condition is satisfied.

Key points and possible actions

- If monitoring workers' performance or conduct results in the collection of information on such matters as health, racial origin, trade union activities or sex life, check that at least one of the sensitive data conditions is met.

See Supporting Guidance Page 23 which explains more about the conditions for processing sensitive data.

- 3.2.6** Keep to a minimum those who have access to personal information obtained through monitoring. Subject them to confidentiality and security requirements and ensure that they are properly trained where the nature of the information requires this.

Key points and possible actions

- Assess whether the organisation could reduce the number of staff involved in monitoring workers.
- Consider whether monitoring is more appropriately carried out by security or personnel functions rather than by line managers.
- Ensure that the training for workers who may come across personal information whilst monitoring makes them aware of data protection obligations

- 3.2.7** Do not use personal information collected through monitoring for purposes other than those for which the monitoring was introduced unless:

(a) it is clearly in the individual's interest to do so; or

(b) it reveals activity that no employer could reasonably be expected to ignore.

Key points and possible actions

- Ensure that only senior management can authorise the use of personal information obtained through monitoring for new or different purposes.
- Ensure that they are familiar with the Act and the relevant parts of this Code.

3.2.8 If information gathered from monitoring might have an adverse impact on workers, present them with the information and allow them to make representations before taking action.

Key points and possible actions

- Equipment or systems malfunction can cause information collected through monitoring to be misleading or inaccurate. Information can also be misinterpreted or even deliberately falsified.
- Ensure that, within or alongside disciplinary or grievance procedures, workers can see, and if necessary explain or challenge, the results of any monitoring.

3.2.9 Ensure that the right of access of workers to information about them which is kept for, or obtained through, monitoring is not compromised. Monitoring systems must be capable of meeting this and other data protection requirements.

Key points and possible actions

- Assess whether monitoring systems collect information in a way that enables you to respond readily to access requests.
- If they do not, ensure that a mechanism that will allow you to do so is built into the system.
- Check that any electronic monitoring system, bought 'off-the-shelf', has the capability to enable you to meet access requests.

3.2.10 Do not monitor workers just because a customer for your products or services imposes a condition requiring you to do so, unless you can satisfy yourself that the condition is justified.

Key points and possible actions

- Monitoring is not justified simply because it is a condition of business. Such a condition cannot over-ride the employer's obligations to comply with the Act.
- Consider carrying out an impact assessment to assess whether meeting any external stipulation means that your organisation is in breach of the Act. If so, cease monitoring on this basis

A decorative graphic element consisting of a stylized, light blue, curved shape resembling a '6' or a similar character, positioned to the left of the section header.

3.3 Monitoring electronic communications.

This sub-section deals with the monitoring of telephone, fax, e-mail, voice-mail, internet access and other forms of electronic communication.

- 3.3.1** If you wish to monitor electronic communications, establish a policy on their use and communicate it to workers – see ‘Policy for the use of electronic communications’ below.

Key points and possible actions

- If your organisation does not have a policy on the use of electronic communications, decide whether you should establish one.
- Review any existing policy to ensure that it reflects data protection principles
- Review any existing policies and actual practices to ensure that they are not out of line, e.g. whether private calls are banned in the policy but generally accepted in practice.
- Check that workers are aware of the policy and if not bring it to their attention.

Policy for the use of electronic communications.

Employers should consider integrating the following data protection features into a policy for the use of electronic communications:-

- Set out clearly to workers the circumstances in which they may or may not use the employer's telephone systems (including mobile phones), the e-mail system and internet access for private communications.
- Make clear the extent and type of private use that is allowed, for example restrictions on overseas phone calls or limits on the size and/or type of e-mail attachments that they can send or receive.
- In the case of internet access, specify clearly any restrictions on material that can be viewed or copied. A simple ban on 'offensive material' is unlikely to be sufficiently clear for people to know what is and is not allowed. Employers may wish to consider giving examples of the sort of material that is considered offensive, for example material containing racist terminology or nudity.
- Advise workers about the general need to exercise care, about any relevant rules, and about what personal information they are allowed to include in particular types of communication.
- Make clear what alternatives can be used, e.g. the confidentiality of communications with the company doctor can only be ensured if they are sent by internal post, rather than by e-mail, and are suitably marked.
- Lay down clear rules for private use of the employer's communication equipment when used from home or away from the workplace, e.g. the use of facilities that enable external dialling into company networks
- Explain the purposes for which any monitoring is conducted, the extent of the monitoring and the means used.
- Outline how the policy is enforced and penalties which exist for a breach of policy.

There may, of course, be other matters that an employer also wants to address in its policy.

- 3.3.2** Ensure that where monitoring involves the interception of a communication it is not outlawed by the Regulation of Investigatory Powers Act 2000.

Key points and possible actions

- Interception occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. It does not include access to stored e-mails that have been opened.
- The intended recipient may be the business, but it could be a specified individual.
- Check whether any interception is allowed under the Lawful Business Practice Regulations.
- Take any necessary action to bring such monitoring in line with RIPA and these Regulations.

See Supporting Guidance Page 28 for more information about the Lawful Business Practice Regulations.

- 3.3.3** Consider - preferably using an impact assessment - whether any monitoring of electronic communications can be limited to that necessary to ensure the security of the system and whether it can be automated.

Key points and possible actions

- Automated systems can be used to provide protection from intrusion, malicious code such as viruses and Trojans, and to prevent password misuse. Such systems may be less intrusive than monitoring of communications to or from workers.

- 3.3.4** If telephone calls or voice-mails are, or are likely to be, monitored, consider - preferably using an impact assessment – whether the benefits justify the adverse impact . If so, inform workers about the nature and extent of such monitoring.

Key points and possible actions

- If telephone calls or voice-mails are monitored, or will be monitored in the future, consider carrying out an impact assessment.
- If voice-mails need to be checked for business calls when workers are away, make sure they know this may happen and that it may be unavoidable that some personal messages are heard.
- In other cases, assess whether it is essential to monitor the content of calls and consider the use of itemised call records instead.
- Ensure that workers are aware of the nature and extent of telephone monitoring.

3.3.5 Ensure that those making calls to, or receiving calls from, workers are aware of any monitoring and the purpose behind it, unless this is obvious.

Key points and possible actions

- Consider the use of recorded messages, informing external callers that calls may be monitored.
- If this is not feasible, encourage workers to tell callers that their conversations may be monitored.

3.3.6 Ensure that workers are aware of the extent to which you receive information about the use of telephone lines in their homes, or mobile phones provided for their personal use, for which your business pays partly or fully. Do not make use of information about private calls for monitoring, unless they reveal activity that no employer could reasonably be expected to ignore.

Key points and possible actions

- Remember that expectations of privacy are likely to be significantly greater at home than in the workplace.
- If any workers using mobiles or home telephone lines, for which you pay, are currently subjected to monitoring ensure that they are aware of the nature and the reasons for monitoring.

3.3.7 If e-mails and / or internet access are, or are likely to be, monitored, consider, preferably using an impact assessment, whether the benefits justify the adverse impact. If so, inform workers about the nature and extent of all e-mail and internet access monitoring.

Key points and possible actions

- If e-mails and/or internet access are presently monitored, or will be monitored in the future, consider carrying out an impact assessment.
- Check that workers are aware of the nature and extent of e-mail and internet access monitoring

3.3.8 Wherever possible avoid opening e-mails, especially ones that clearly show they are private or personal.

Key points and possible actions

- Ensure that e-mail monitoring is confined to address / heading unless it is essential for a valid and defined reason to examine content.
- Encourage workers to mark any personal e-mails as such and encourage them to tell those who write to them to do the same.
- If workers are allowed to access personal e-mail accounts from the workplace, such e-mails should only be monitored in exceptional circumstances.

3.3.9 Where practicable, and unless this is obvious, ensure that those sending e-mails to workers, as well as workers themselves, are aware of any monitoring and the purpose behind it.

Key points and possible actions

- It may be practicable – for example when soliciting e-mail job applications – to provide information about the nature and extent of monitoring.
- In some cases, those sending e-mails to a work-place address will be aware that monitoring takes place without the need for specific information.

3.3.10 If it is necessary to check the e-mail accounts of workers in their absence, make sure that they are aware that this will happen.

Key points and possible actions

- If e-mail accounts need to be checked in the absence of workers, make sure they know this will happen.
- Encourage the use of a marking system to help protect private or personal communications.
- Avoid, where possible, opening e-mails that clearly show they are private or personal communications.

3.3.11 Inform workers of the extent to which information about their internet access and e-mails is retained in the system and for how long.

Key points and possible actions

- Check whether workers are currently aware of the retention period of e-mail and internet usage.
- If it is not already in place, set up a system (e.g. displaying information online or in a communication pack) that informs workers of retention periods.



3.4. Video and audio monitoring.

Some – though not all - of the data protection issues that arise when carrying out video monitoring in public places will arise in the workplace. Employers carrying out video monitoring of workers will therefore find the guidance in the Information Commissioner's CCTV Code useful. Audio monitoring means the recording of face-to-face conversations, not recording telephone calls.

See www.informationcommissioner.gov.uk and search for the CCTV Code of Practice.

- 3.4.1** If video or audio monitoring is (or is likely) to be used, consider - preferably using an impact assessment – whether the benefits justify the adverse impact.

Key points and possible actions

- Where possible, any video or audio monitoring should be targeted at areas of particular risk and confined to areas where expectations of privacy are low.
- Continuous video or audio monitoring of particular individuals is only likely to be justified in rare circumstances

- 3.4.2** Give workers a clear notification that video or audio monitoring is being carried out and where and why it is being carried out.

Key points and possible actions

- Unless covert monitoring is justified, ensure that workers are informed of the extent and nature of any monitoring that is taking place and the reasons for it.

- 3.4.3** Ensure that people other than workers, such as visitors or customers, who may inadvertently be caught by monitoring, are made aware of its operation and why it is being carried out.

Key points and possible actions

- Ensure that there are adequate notices, or other means, to inform such people about the monitoring and its purpose(s).

A decorative graphic element consisting of a stylized, light blue, curved shape resembling a '6' or a similar character, positioned to the left of the section header.

3.5. Covert monitoring.

Covert monitoring means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place. This sub-section is largely directed at covert video or audio monitoring, but will also be relevant where electronic communications are monitored when workers would not expect it.

- 3.5.1** Senior management should normally authorise any covert monitoring. They should satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection.

Key points and possible actions

- Covert monitoring should not normally be considered. It will be rare for covert monitoring of workers to be justified. It should therefore only be used in exceptional circumstances.

- 3.5.2** Ensure that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe and that the covert monitoring does not continue after the investigation is complete

Key points and possible actions

- Deploy covert monitoring only as part of a specific investigation and cease once the investigation has been completed

- 3.5.3** Do not use covert audio or video monitoring in areas which workers would genuinely and reasonably expect to be private.

Key points and possible actions

- If embarking on covert monitoring with audio or video equipment, ensure that this is not used in places such as toilets or private offices.
- There may be exceptions to this in cases of suspicion of serious crime but there should be an intention to involve the police.

3.5.4 If a private investigator is employed to collect information on workers covertly make sure there is a contract in place that requires the private investigator to only collect information in a way that satisfies the employer's obligations under the Act.

Key points and possible actions

- Check any arrangements for employing private investigators to ensure your contracts with them impose requirements on the investigator to only collect and use information on workers in accordance with your instructions and to keep the information secure.

3.5.5 Ensure that information obtained through covert monitoring is used only for the prevention or detection of criminal activity or equivalent malpractice. Disregard and, where feasible, delete other information collected in the course of monitoring unless it reveals information that no employer could reasonably be expected to ignore.

Key points and possible actions

- In a covert monitoring exercise, limit the number of people involved in the investigation.
- Prior to the investigation, set up clear rules limiting the disclosure and access to information obtained.
- If information is revealed in the course of covert monitoring that is tangential to the original investigation, delete it from the records unless it concerns other criminal activity or equivalent malpractice.



3.6. In-vehicle monitoring

Devices can record or transmit information such as the location of a vehicle, the distance it has covered and information about the user's driving habits. Monitoring of vehicle movements, where the vehicle is allocated to a specific driver, and information about the performance of the vehicle can therefore be linked to a specific individual, will fall within the scope of the Data Protection Act.

- 3.6.1** If in-vehicle monitoring is or will be used, consider - preferably using an impact assessment – whether the benefits justify the adverse impact.

Key points and possible actions

- Where private use of a vehicle is allowed, monitoring its movements when used privately, without the freely given consent of the user, will rarely be justified.
- If the vehicle is for both private and business use, it ought to be possible to provide a 'privacy button' or similar arrangement to enable the monitoring to be disabled.
- Where an employer is under a legal obligation to monitor the use of vehicles, even if used privately, for example by fitting a tacograph to a lorry, then the legal obligation will take precedence

- 3.6.2** Set out a policy that states what private use can be made of vehicles provided by, or on behalf of, the employer, and any conditions attached to use.

Key points and possible actions

- Make sure, either in the policy or separately, that details of the nature and extent of monitoring are set out.
- Check that workers using vehicles are aware of the policy.



3.7 Monitoring through information from third parties.

Employers need to take special care when wishing to make use of information held by third parties, such as credit reference or electoral roll information. This section also applies to information held by employers in a non-employment capacity, such as when a bank monitors its workers' bank accounts. Where an employer wishes to obtain information about a worker's criminal convictions, a disclosure must be obtained via the Criminal Records Bureau.

See Part 1 – Recruitment and Selection, Page 34, for more information about the Criminal Records Bureau.

- 3.7.1** Before undertaking any monitoring which uses information from third parties, ensure – preferably using an impact assessment – that the benefits justify the adverse impact.

Key points and possible actions

- A worker's financial circumstances should not be monitored unless there are firm grounds to conclude that financial difficulties would pose a significant risk to the employer.

- 3.7.2** Tell workers what information sources are to be used to carry out checks on them and why the checks are to be carried out.

Key points and possible actions

- Set up a system to tell workers the nature and extent of any monitoring which uses information from third parties. (This could be via a workers handbook, notice board or on-line.)
- Where a specific check is to be carried out, the workers should be directly informed, unless to do so would be likely to prejudice the prevention or detection of crime.

- 3.7.3** Ensure that, if workers are monitored through the use of information held by a credit reference agency, the agency is aware of the use to which the information is put. Do not use a facility provided to conduct credit checks on customers to monitor or vet workers.

Key points and possible actions

- If your organisation uses a credit reference agency to check customers, make sure this facility is not being used to monitor or vet workers. If such practices are in place, stop them immediately.

- 3.7.4** Take particular care with information about workers which you have as a result of a non-employment relationship with them.

Key points and possible actions

- Check whether your organisation routinely uses information about workers that has been obtained from them because they are also (or have been) your customers, clients or suppliers. If such practices are in place, stop them unless they are justified by a risk you face.

- 3.7.5** Ensure that workers carrying out monitoring which involves information from third parties are properly trained. Put in place rules preventing the disclosure or inappropriate use of information obtained through such monitoring.

Key points and possible actions

- Identify who may carry out monitoring using information from third parties.
- Assess whether the organisation could reduce the number of workers involved in this activity without compromising necessary monitoring.
- Set up instructions or training for workers involved in this monitoring, making them aware of the data protection principles involved.
- Consider placing confidentiality clauses in the contracts of relevant staff.

- 3.7.6** Do not retain all the information obtained through such monitoring. Simply record that a check has taken place and the result of this.

Key points and possible actions

- Review procedures on retaining information. Unless there is a legal or regulatory obligation, check that information is not normally retained for more than 6 months.

If you wish to contact us:

Information Commissioner,

Wycliffe House, Water Lane,

Cheshire, SK9 5AF

Telephone: 01625 545700

Fax: 01625 524510

E-mail: ico.gsi.gov.uk

Website: www.informationcommissioner.gov.uk