

# **THE EMPLOYMENT PRACTICES DATA PROTECTION CODE**

## **Monitoring at work: an employer's guide**

# CONTENTS

|   |                              |
|---|------------------------------|
| ABOUT THE CODE .....  | 3                            |
| SECTION 1: BACKGROUND INFORMATION. ERROR! BOOKMARK NOT DEFINED. |                              |
| SECTION 2: THE CODE.....  | <del>1311</del> 13           |
| 1 MANAGING DATA PROTECTION .....                                | ERROR! BOOKMARK NOT DEFINED. |
| 2 MONITORING - GENERAL CONSIDERATIONS .....                     | <del>1715</del> 17           |
| 3 COVERT MONITORING .....                                       | <del>2018</del> 20           |
| 4 MONITORING ELECTRONIC COMMUNICATIONS.....                     | <del>2321</del> 23           |
| 5 VIDEO AND AUDIO MONITORING .....                              | <del>2724</del> 27           |
| 6 IN-VEHICLE MONITORING.....                                    | <del>2926</del> 29           |
| 7 MONITORING PRIVATE INFORMATION .....                          | <del>3128</del> 31           |
| SECTION 3: FURTHER INFORMATION .....                            | <del>3330</del> 33           |

## ABOUT THE CODE

### Who is the Code for?

The Employment Practices Data Protection Code is written primarily for businesses where the employment of staff constitutes a significant activity. Much of the Code, though, will be applicable to any employer. Not every aspect of the code will be relevant to every organisation. This will vary depending on the size and the type of business that is conducted. Particularly for small businesses, some of the issues addressed may arise only rarely. Here the Code is intended to serve as a reference document to be called on when necessary. This part of the Code explains how your organisation can follow the Data Protection Act in the context of recruitment and selection.

### Why should you use it?

The Data Protection Act 1998, on which this Code is based, places responsibilities on any organisation to process personal data 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 its information on 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 clearly states what you need to check, and what action, if any, you need to take. Implementing it should produce other benefits in terms of the organisation's relationship with workers, compliance with other legislation and efficiencies in storing and managing data.

### What is the legal status of the Code?

The legal requirement on employers is to comply with the Act itself. The benchmarks in the Code are however designed to bring about compliance with the Act. They develop and apply the Act in the context of employment practices. They are 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 benchmarks in the Code would be cited by the Commissioner in connection with any enforcement action that arises in relation to the processing of personal data in employment
- disregard for the data protection requirements that particular benchmarks are designed to help organisations meet is likely to mean that an employer will not comply with the Act.

### Other parts of the Code

The Employment Practices Data Protection Code has three additional parts,

- [recruitment and selection – which concerns processing records, checking the accuracy of applications and pre-employment vetting](#)
- **employment records** – is about collecting, storing, disclosing and deleting records

~~● monitoring at work~~ is about monitoring workers' use of telephone or email systems and vehicles

● **medical information** – is about occupational health, medical testing, drug and genetic screening

Each part of the Code has been designed to stand alone and therefore much of the background information is the same. 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 Useful Addresses page 36 for contact details or contact the website [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)**

## Five sections

This booklet is divided into five sections

- Section 1: Background – which answers questions about the Data Protection Act 1998 and The Employment Practices Data Protection Code.
- Section 2: The Code – which gives benchmarks for organisations to meet in the area of recruitment and selection.
- Section 3: Further Information – which provides more information on some aspects of the Code and gives useful addresses.
- Section 4: Frequently asked questions – which sets out several frequently asked questions and their answers.
- Section 5: Checklists – which are designed to help organisations put the Code's provisions into practice.

Throughout this booklet you will see signposts  These indicate where you can go to get further information on certain subjects.

## Our aim

The aim of the Code is to strike a balance between a worker's legitimate right to respect for his or her private life and an employer's legitimate need to run its business.

## SECTION 1: BACKGROUND INFORMATION

### The Data Protection Act 1998: key questions

#### What does the Data Protection Act 1998 cover?

The Data Protection Act 1998 came into force on 1 March 2000. It regulates the use of personal data and gives effect in UK law to the European Directive on data protection (95/46/EC).

The Act covers some manual records, such as those recorded on paper or media such as microfiche, as well as computerised records and is concerned with the processing of “personal data”, that is, data relating to identifiable living individuals. It works in two ways;

- giving individuals (data subjects) certain rights
- requiring those who decide how and why personal data are processed (data controllers) to be open about their use of those data and to comply with the data protection principles in their information-handling practices.

#### What are the responsibilities of data controllers under the Act?

Most data controllers will need to notify the Commissioner of their processing of personal data. Notification is the process by which data controllers inform the Information Commissioner of certain details about the processing of personal data they carry out. These details are then included on a public register. Data controllers or workers can inspect this register at any time by visiting the data protection register website. There are some exemptions from the requirement to notify. These exemptions are likely to apply to smaller businesses that have relatively simple data processing operations. All data controllers are required to comply with the data protection principles even where they are exempt from the requirement to notify.



**Access the website [www.dpr.gov.uk](http://www.dpr.gov.uk) or contact the Information Commissioner for a copy of the *Notification Handbook* to find out more about notification and exemptions. See Useful Addresses page [36-00](#) for contact details.**

#### What are the data protection principles?

There are eight data protection principles that are central to the Act. In brief, they say that personal data must be

1. processed fairly and lawfully
2. processed for limited purposes and not in any manner incompatible with those purposes
3. adequate, relevant and not excessive
4. accurate
5. not kept for longer than is necessary
6. processed in line with data subjects' rights

7. secure
8. not transferred to countries that don't protect personal data adequately.

### **What are the rights of data subjects under the Act?**

The Act grants workers the right to have a copy of the information that an organisation holds about them. It allows them to apply to the courts to obtain an order requiring a data controller to correct inaccurate data held about them, and to seek compensation where damage and distress have been caused as a result of any breach of the Act. Workers may also object to the processing of personal data about them. In some circumstances they can stop employers keeping information about them or using the information in particular ways.

### **Are there any exemptions from the Act?**

Yes. There are some limited exemptions, for example to ensure that applying the Act does not prejudice the detection of crime or the apprehension of offenders. Where exemptions are likely to be relevant, they are referred to in the Code.

### **Who is legally liable for implementing the Act in my organisation?**

Under the Act this is the "Data Controller". Who this is will vary depending on the nature of your organisation. For example, in the case of limited companies, the company itself is the Data Controller. However, in the case of sole traders and partnerships, accountability rests with the owners of the business. With government departments the Data Controller is the Secretary of State. In the case of other public organisations, it is usually the organisation itself that is liable. Often organisations allocate data protection responsibility to an individual or department but this does not transfer legal liability onto individual workers or make them Data Controllers.



**Benchmark 1 page [1400](#) explains more about allocating responsibility.**

## What can happen if our organisation doesn't comply with the Act?

### *Enforcement*

If the Commissioner considers that breaches of the principles have occurred, enforcement action can be taken against an organisation. This will require changes to bring about compliance, for example the deletion of records or the redesigning of an application form. The organisation may appeal to the independent Information Tribunal. However, if the Tribunal upholds the Commissioner's enforcement action, and the organisation continues to break the principles, this is a criminal offence.

### *Prosecution.*

Other criminal offences include a failure to notify when not exempt and a failure to keep a notification up to date. There are also offences of unlawfully obtaining personal data and unlawfully selling the data. If a criminal offence has been committed the Commissioner can and does prosecute. Company directors or people in an equivalent position can be prosecuted where an offence is due to their negligence or connivance.

### *Assessment of Processing.*

A worker or any other person affected may ask the Commissioner to assess whether an organisation's processing of personal data is being done in compliance with the Act. This is often how a breach comes to light. The Commissioner is required to make an assessment when requested to do so. The Commissioner can serve an Information Notice on a data controller where she needs information to determine whether the data protection principles are being complied with.

### *Compensation.*

Compensation can be awarded through the courts to an individual if damage has been caused by an organisation not meeting a requirement of the Act. If damage is proved, then the court may also order compensation for any associated distress.

## What is the role of the Information Commissioner?

The Commissioner is an independent, supervisory authority appointed by the Queen. Her first duty is to promote the following of good practice. To do this she issues codes of practice, provides information, responds to enquiries, checks whether organisations are complying with the Act and serves enforcement notices to require organisations to comply with the law.



See Useful Addresses page [3600](#) for contact details.

## Where can our organisation find out more about the Act?

If you require more information about the Act, contact the Information Commissioner where you can obtain a leaflet called *The Data Protection Act: A Brief Guide for Data Controllers* or, for a more detailed examination, a booklet called *Legal Guidance*.



See Useful Addresses page [36-00](#) for contact details.



---

## The Employment Practices Code: key questions

### What is this Code of Practice for?

The Code is intended to assist employers in complying with the Act and to establish good practice for handling personal data in the workplace. The Code covers such issues as the obtaining of information about workers, the retention of records, access to records and disclosure of them.

### Who does data protection cover in the workplace?

The Code is concerned with data 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 "workers" is used to cover all these individuals. As such it includes;

- Applicants (successful and unsuccessful)
- Former applicants (successful and unsuccessful)
- Employees (current and former)
- Agency workers (current and former)
- Casual workers (current and former)
- Contract workers (current and former)

Some benchmarks will also apply to others in the workplace such as volunteers and those on work experience placements.

### What data are covered by the Code?

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

#### *Personal data*

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

- relates to a living person, and
- identifies an individual either on its own or together with other information that is in the organisation's possession or that is likely to come into its possession.

All automated and computerised personal data are covered by the Act. It also covers personal data 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 worker.

#### *Processing*

The Act applies to personal data that are 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 data, their keeping and use, accessing and disclosing them through to their final destruction.

**Examples of personal data likely to be covered by the Act**

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

**Examples of information unlikely to be covered by the Act**

- 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 useable information held about individual workers will be covered by the Code.

**Sensitive personal data*****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 workers' 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.

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. In the context of monitoring typical circumstances in which sensitive personal data 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 in internet access logs which show that a worker routinely accesses a particular trade union website
- various categories of information caught by the recording of workers' private conversations



See *Further Information Page 00* which explains more about the sensitive data rules.

### What happens when a worker wishes to access information?

The Act allows for any individual to make a 'subject access request' to any organisation that he or she believes is processing his or her personal data. This request must be in writing, for example by letter or email. Once an organisation receives such a request it must respond promptly, or at the most within 40 calendar days. It must produce copies of the information it holds in an intelligible form. The organisation can charge up to £10 for doing this.

The 40 day period starts once the organisation has received the fee together with any information it needs to verify the identity of the individual making the request and to locate the information that the individual seeks.

There are some exemptions that allow organisations to withhold information. These exemptions can apply in areas such as criminal investigation, management planning such as promotion and transfer plans, and negotiations. The exemptions, though, are limited in their application even within these areas. Care must also be taken in deciding whether or not to release information identifying 'third parties' i.e. people, other than the individual who has made the subject access request.



See *Part 2 – Employment Records page 00* for more information on access rights and exemptions.

### What are workers' responsibilities under the Act?

Workers do have some responsibilities for data protection under the Act. Line managers have responsibility for the type of personal data they collect and how they use them. No workers should disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes. A worker disclosing personal data 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.



---

**Benchmark 1 page [14-00](#) explains more about allocating responsibility.**

## SECTION 2: THE CODE

### The role of data protection in monitoring at work

This part of the Code is intended to explain to employers how to approach monitoring and what benchmarks ought to be met. Some forms of monitoring are a recognised component of the employer-worker relationship. Most employers will make some checks on the quantity and quality of work produced by workers. Most workers will expect this. However, the collection, processing and storage of any personal data arising from monitoring must be done in a way that is both lawful and fair to workers.

For the purposes of this Code “monitoring” is used to describe two types of practice. These are;<sup>1</sup>

- the collection of information about workers wholly or mainly as a means of checking their performance, compliance with legal requirements, company rules etc
- the use of information collected for other purposes to actively monitor their ~~watch workers in order to check their~~ performance, compliance with legal requirements, company rules etc.<sup>2</sup>

Examples of activities covered by this part of the Code;

- gathering information through Point Of Sale terminals to check the efficiency of individual supermarket check-out operators
- watching workers by means of CCTV cameras
- randomly checking individual workers’ e-mails to look for evidence of harassment of other workers
- listening to recordings of telephone calls made by workers in a financial call centre to see whether regulatory requirements are being met
- systematically checking logs of telephone numbers called to look for excessive private use
- setting up an arrangement whereby all e-mails sent or received by a worker suspected of disclosing trade secrets are routinely read
- examining logs of websites visited to check that individual workers are not downloading pornography
- obtaining information through credit reference agencies to check that workers are not in financial difficulties.

Examples of activities not covered by this part of the Code;

- looking back through customer records in the event of a complaint to check that the worker dealing with the customer gave correct advice

<sup>1</sup> ~~As you can see, I think this definition must be put up front.~~

<sup>2</sup> ~~Don't understand the second part of the definition – I think we should talk about this because I was not sure what meant so could not try to redraft it.~~

- checking a collection of e-mails sent by a particular worker and stored as a record of transactions or to ensure the security of the system when that worker has been accused of racial harassment involving the use of e-mail
- 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.

~~Note that those~~ These last activities, however, still come within the general scope of the Act and this Code. ~~They are not though activities~~ but are not specifically addressed in this section on monitoring.

~~Employers monitor workers for different reasons. In some cases this will be because they may need to check whether workers are complying with legal or regulatory requirements. In other cases, the employer may be monitoring adherence to its own rules or performance benchmarks and if this is the case, employers should have a genuine and legitimate business requirement to do so. However, in both instances the method of monitoring should comply with the benchmarks in this Code.<sup>3</sup>~~

The Information Commissioner recognises the decision regarding whether to carry out monitoring may involve the striking of a balance between intrusion on the one hand and risk to the business on the other. How this balance should be struck will depend on the circumstances of each case, therefore this Code cannot give hard and fast rules that are applicable in all cases. It is intended to assist employers in identifying factors to be taken into account when deciding whether or not to carry out monitoring and in giving weight to those factors.

## The Code at a glance

The Code consists of a set of benchmarks. In each of the following pages, the benchmarks are dealt with in detail, with notes and examples given as further explanation to each individual benchmark.

---


<sup>3</sup>~~Think this now overlaps with definition and so best to remove it.~~

# 1 MANAGING DATA PROTECTION

Managing data protection is concerned with how your organisation sets up methods to protect personal data about workers. This covers allocating responsibility, establishing what personal data are processed, ensuring employment practices are compliant with the Act and checking whether your organisation needs to notify the Information Commissioner about any data held. These benchmarks appear in all parts of the Code as many of them will be relevant to every employer. How far they are applicable and what is needed to achieve them will, of course, depend very much on the size and nature of the organisation.

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 data are seen as the norm.

## The benchmarks

|  |
|--|
|   |
| 1. <i>Establish a person within the organisation responsible for ensuring employment practices 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.</i>          |
| 2. <i>Ensure that business areas and individual line managers that process information about workers understand their own responsibility for data protection compliance and if necessary amend their working practices in the light of this.</i>                             |
| 3. <i>Assess what personal data about workers are in existence and who is responsible for them.</i>  |
| 4. <i>Eliminate the collection of personal data that are irrelevant or excessive to the employment relationship. If sensitive data are collected ensure that a sensitive data condition is satisfied.</i>  |
| 5. <i>Ensure that workers are aware of the extent to which they can be criminally liable if they knowingly or recklessly disclose personal data outside their employer's policies and procedures. Make serious breaches of data protection rules a disciplinary offence.</i> |
| 6. <i>Allocate responsibility for checking that your organisation has a valid notification in the register of data controllers that relates to the processing of personal data about workers, unless it is exempt from notification.</i>                                     |
| 7. <i>Consult trade unions or other workers' representatives, if any, or workers themselves over the development and implementation of employment practices and procedures that involve the processing of workers' data.</i>   |



Access the website [www.dpr.gov.uk](http://www.dpr.gov.uk) where you can view the register or contact the Information Commissioner for a copy of the *Notification Handbook* to find out more about notification. See Useful Addresses page [3600](#) for contact details.

## Notes and examples

1. In a small business the responsibility might simply be with the owner of the business. Where there is a management structure responsibility should be allocated to a senior manager in the personnel or human resources function or someone in a comparable position. Those with overall responsibility must be in a position to feed their knowledge into other areas of the business where information about workers is processed, and to ensure that the organisation has a co-ordinated approach to data protection compliance. Ideally data protection should be seen as an integral part of employment procedures rather than as a stand alone requirement. For example, in the company's written procedure for dealing with selection, there should be a section on how to follow up on references, which should incorporate the relevant benchmarks in this Code. Procedures are only of value if they are current and adhered to. Review and update procedures as necessary and put a mechanism in place to ensure that they are being followed on the ground. This might involve some form of audit or self-certification by managers.
2. It is important to remember that data protection compliance is a multi-disciplinary matter. For example, a company's IT staff may be primarily responsible for keeping computerised personal data secure, whilst a human resources department may be responsible for ensuring that the information requested on a job application form is not excessive, irrelevant or inadequate. All workers, including line managers, have a part to play in securing compliance, for example by ensuring that waste paper bearing personal data is properly disposed of.

An employer is liable to pay compensation for damage suffered by an individual as a result of the actions of a line manager in regards to data protection unless it is clear that the line manager has been acting outside his or her authority. Employers can help protect themselves against claims by training line managers and having clear procedures in place.

3. It may be helpful to assess personal data held on workers using the same categories as are used in the various parts of this Code, i.e. personal data processed in connection with recruitment and selection, employment records, monitoring at work and medical information. Consider who in your organisation will be collecting, using, storing and destroying such information. Only when you have ascertained this will you be able to check that your organisation is complying with the Act.
4. When making your assessment of personal data consider if all the information collected on workers is necessary for the employment relationship. For example, information concerning workers' lives outside work is unlikely to be necessary. However, it might be legitimate to request information about workers' other jobs where there is a justifiable need, for example, in connection with Working Time Regulations, or to request information about their children in connection with an application for parental leave. The collection and use of sensitive data must satisfy a sensitive data condition.



**See further information, page [30-00](#) for conditions to be satisfied**

5. Workers should be broadly aware of the legal duties that the Act places on employers and their own role as workers in meeting them. In particular, workers should be aware of how data protection compliance impinges in practical terms on the way they perform their work. It is also crucial to make workers aware of the possible consequences of their actions in this area, e.g. disciplinary action or personal criminal liability. It is useful to incorporate such information in the general induction process for new workers and to regularly remind existing workers of their obligations.
6. Failing to notify when required to do so or failing to keep a notification up to date is a criminal offence. The person responsible for data protection should ensure that entries concerning workers' data on the Register of data controllers are complete, accurate and up-to-date. This may be a duty that he or she personally undertakes or it may be delegated.
7. Consultation is not in itself a legal requirement. Nevertheless consultation should help ensure processing of personal data is fair to the workers to whom the data relate

## - GENERAL

# CONSIDERATIONS

~~Remember that workers have a right of access to information collected and kept about them in the course of monitoring.<sup>4</sup>~~

These area set of general benchmarks relevant to all monitoring activities.



1. ~~Be clear Identify who within the organisation can sanction authorise the monitoring of workers and the steps they have to go through before doing so. notify them of their responsibilities under the Act.~~
2. Before monitoring, establish the specific business risk or risks which monitoring might address. Assess the impact of monitoring on the privacy, relationship of trust and other legitimate rights of workers and others. Make a realistic assessment of the likely effectiveness of monitoring in reducing or eliminating these risks and tailor the monitoring, if any, to achieving this. Do not introduce monitoring where the impact is not justified by the reduction in risk. Document your assessment.
- ~~2.3.~~ In making this assessment consult trade unions or other workers' representatives, if any, or workers themselves.
4. 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 any associated monitoring. Make workers aware of the policy.
5. Tell workers that monitoring is taking place and why, and periodically remind them of this, unless covert monitoring is justified.
6. If sensitive data are processed in the course of monitoring, ensure that a sensitive data condition is satisfied..
7. 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.
8. Avoid using personal information collected through monitoring for purposes other than those for which the monitoring was introduced unless it is clearly in the worker's interest to do so or it reveals criminal activity or gross misconduct.
9. If the information gathered from monitoring might have an adverse impact on workers, present them with the information and allow them to make representations.
10. Ensure that the right of access of workers to information about them kept for or obtained through monitoring is not compromised. Monitoring equipment must be capable of meeting this and other data protection requirements.

<sup>4</sup>~~Think this is unnecessary because No 5 and 10.~~

1. Monitoring of workers can have serious implications which may go well beyond data protection concerns. There are risks that the Act will be breached if, for example, line managers institute monitoring of their workers without authority and without taking into account the provisions of this Code. Business practices should be designed to ensure that monitoring does not take place without careful consideration of the requirements of the Act and the benchmarks in the Code.
- 
2. Monitoring should be designed to operate in such a way that it does not intrude unnecessarily on the right of workers to expect respect for their private lives and correspondence. In addition, workers have a right to expect a degree of trust from employers, and to be given reasonable freedom to determine their own actions without constantly being watched or listened to. Monitoring should not undermine this relationship.

In making this determination of whether to monitor, consider the following;

- are there other less intrusive methods, whether involving monitoring or not, that might achieve an acceptable reduction in risk?
- can an acceptable reduction of risk be achieved by more closely targeted monitoring on those areas of the business where the risk is greatest?
- are there technical means that can be employed to keep the intrusion involved in the monitoring to a minimum?

~~Risk should be considered realistically. For example, a well-known case in which an insurance company had to pay substantial damages to another business as a result of defamatory material published by an insurance company employee in an internal e-mail is often cited as a justification for routine monitoring of workers' e-mail. However informed commentators question whether routine monitoring of e-mail could in practice have altered events. Another example is the practice of routine monitoring of e-mail to prevent sexual or racial harassment in the workplace. Although targeted monitoring may have a role where there are concrete suspicions of harassment, it is unlikely to be either a practical or effective means of prevention.<sup>5</sup> Risks however, can be reduced significantly by effective training, supervision and clear communication.~~

---

~~2.3. Consultation is not in itself a legal requirement. Nevertheless, consultation should help ensure that processing of personal data is fair to the workers to whom the data relate.~~

4. If monitoring is to be justified on the basis that it is necessary to enforce the organisation's rules and standards, these rules and standards must be known and understood by workers. In some cases the standards may be obvious, for example that it is unacceptable to engage in criminal activity from the workplace, but in others they may not ~~be, particularly for those who are new to the organisation or even new to any form of employment.~~ Rules and standards, for example in relation to acceptable uses of e-mail systems and internet access, should be set out in a policy that is made known to and accessible by all workers affected. The policy should go on to set out the circumstances in which monitoring may take place, the nature of the monitoring, how information obtained through monitoring will be used, and the safeguards that are in place for the workers that are subject to the monitoring.

5. ~~It is a general requirement of the Data Protection Act that where the carrying out of monitoring results in the processing of personal data, those who are subject to it should be made aware that it is being carried out and why it is being carried out. Workers can be made aware of this, for example, through signage in areas subject to monitoring or through information given in a staff handbook. Workers should be reminded of existing monitoring periodically, and where a new monitoring policy is introduced they should be told of this. NEED TO DRAFT SOMETHING RE TRANSPARENCY<sup>6</sup>~~

---

~~<sup>5</sup> Think we do not need the two examples here. Firstly the insurance company one, I think that either we name the company, so that those that do know the case are sure they recognise it or we should not mention it at all. At the moment it is the only case mentioned and so looks out of kilter with the rest of document. We also deal with the issue involved more comprehensively elsewhere and this is the case with the second example so I would omit them here.~~

~~<sup>6</sup>Please include~~



### 3 COVERT MONITORING

This is monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place.

It is the Information Commissioner's view that in normal employment contexts covert monitoring should not be used to obtain information about workers, and that where it is to be used the police should be involved.

#### The benchmarks



1.

2. Only use covert monitoring if specific criminal activity has been identified and a documented assessment *has been made* ~~has been made~~ *concluding* that notifying workers of monitoring would prejudice an investigation.

3. In the case of public authorities, ensure that the monitoring is carried out in accordance with an authorisation granted under the provisions of Part II of the Regulation of Investigatory Powers Act 2000. In the case of private sector businesses ensure that covert monitoring is not carried out unless it has been authorised at a senior level.

4. Ensure that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe

~~4.5.~~ Ensure that if covert monitoring might be occasionally necessary, workers are aware in general terms of the circumstances in which such monitoring might be used and the form it might take.

~~5.6.~~ Avoid using covert audio or video monitoring in areas where it would be especially intrusive such as in cloakrooms or private offices.

~~5.7.~~ Ensure that workers carrying out covert monitoring are properly trained to do so and are given clear guidance.

8. Ensure that information obtained through covert monitoring is used only for the prevention or detection of the criminal activity or the apprehension or prosecution of offenders to which the monitoring was directed. Disregard and, where feasible, delete other information collected in the course of monitoring unless it reveals other criminal activity or gross misconduct.

## Notes and examples

1. To take advantage of covert monitoring an employer must be able to rely on an exemption in the Act. Covert monitoring is only justified if in the particular case openness would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. It is therefore essential that the employer makes a considered and realistic assessment of whether this is the case.
2. Under Part II of the Regulation of Investigatory Powers Act 2002 (RIPA) monitoring that is covert, is undertaken for the purposes of a specific investigation or a specific operation, and is likely to result in the obtaining of private information about any person, is termed “directed surveillance”. If such monitoring extends to residential premises or private vehicles it is likely to be “intrusive surveillance”. Directed surveillance is against the law unless it has been authorised in accordance with a procedure set out in RIPA. This includes an assessment as to whether the surveillance is proportionate to what it seeks to achieve. The procedure for authorisation of intrusive surveillance is more onerous.

Covert monitoring in the workplace will very often fall within the definition of “directed surveillance”. Almost any monitoring whether involving the use of CCTV cameras, telephone systems or computer networks, is likely to result in the obtaining of private information such as might be revealed in a conversation between two workers. Any public authority considering carrying out covert monitoring must satisfy itself that it is operating within the terms of RIPA.

Although private sector businesses are not subject to Part II of RIPA they should bear in mind the discipline it imposes on public authorities undertaking directed surveillance. Covert monitoring should not be embarked on lightly. Private sector businesses should adopt a similar process of authorisation by senior management, following a considered, realistic assessment of proportionality, to that imposed by law on public authorities. Ensure that such assessments are carefully documented.<sup>9</sup>

~~3.~~ A record of how targeting is to be achieved should form part of the assessment.

~~4.~~

4. Covert monitoring is only justified where criminal activity is involved. It is appropriate that the police are informed ~~(although they do not have to sanction or take part in the monitoring)~~<sup>10</sup> if there is sufficient suspicion of criminal activity ~~to justify covert monitoring. This does not mean that the police have to sanction the monitoring or take part in it but it is hard to envisage circumstances where covert monitoring would be justified but it would not be appropriate to at least inform the police.~~

~~5.~~ It is a general requirement of the Data Protection Act that where the carrying out of monitoring results in the processing of personal data, those who are subject to it should be made aware that it is being carried out and why it is being carried out. Workers can be made aware of this, for example, through signage in areas subject to monitoring or through information given in a staff handbook. ~~Although in some cases giving Obviously, giving~~ workers detailed information as to the location of a camera or microphone might prejudice ~~the detection of specific criminal activity, for example, investigations. However,~~ this does not mean that workers ~~need cannot~~ be informed, in general terms, that covert monitoring might ~~be~~ take place and ~~of~~ the circumstances in which this might happen.

6. It is hard to see circumstances where an employer would be justified in installing secret video cameras or other covert monitoring devices in areas where workers would have a high expectation of privacy such as cloakrooms or their own private offices. If in exceptional circumstances such monitoring is justified, for example where there is evidence of drug-dealing on the premises, any monitoring should take place under the direction of the police.

7. Limit the number of staff involved in covert monitoring and ~~make clear who these can be identify clearly who is~~ authorised to be involved. Clear rules should be set down limiting the disclosure of and access to information obtained. Instruct staff processing the results of the monitoring to disregard information unrelated to the

<sup>9</sup> ~~Do we need a reference to RIPA here?~~

<sup>10</sup> ~~Think this does raise questions such as what happens if the police do not sanction monitoring.~~

original purpose, unless it reveals other criminal activity or gross misconduct.

8. ~~If an exemption from the Act is to be relied on in order to allow the obtaining of personal information through covert monitoring, special care must be taken to ensure that any information obtained in this way is not used in a way that is incompatible with the purpose for which the monitoring took place.<sup>14</sup>~~ If, for example, personal information obtained covertly to prevent specific criminal activity in the workplace were to be used for a different or additional purpose, for example to check a worker's time-keeping, this would take the obtaining of personal information beyond the scope of the exemption and a breach of the Act would occur unless workers were told that monitoring was taking place and why it was taking place.

---

~~<sup>14</sup>I think that mentioning exemptions to the Act here is confusing as we have not introduced them elsewhere in this section. I think the Benchmark pretty much stands by itself: do we need this note?~~

## 4 MONITORING COMMUNICATIONS

This includes the monitoring of telephone, e-mail and internet communications.



See *Further Information Page 00* which explains more about how to weigh factors when deciding to monitor communication.

### The benchmarks



#### 4-General

1. Establish and communicate a policy on the use of electronic communications to workers.
2. Ensure that where monitoring involves the interception of a communication it is not outlawed by the Regulation of Investigatory Powers Act 2000.
- 4.3. Apply the approach suggested in this Code in assessing what, if any, monitoring of electronic communications is justified by the risks. Limit the scope of monitoring to what is strictly required to reduce the risk or risks it is intended to address.

#### 5-Telephone monitoring

4. Ensure that the assessment of whether monitoring is justified takes account of the specific circumstances of telephone monitoring.
5. Ensure that those making calls to or receiving calls from the organisation, as well as workers, are aware of any monitoring and the purpose behind it, unless this is obvious.
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 organisation pays partly or fully. Do not make use of information contained in personal calls obtained through monitoring.

#### E-mail and Internet access monitoring

7. Ensure that the assessment of whether monitoring is justified takes account of the specific circumstances of e-mail and/or internet access monitoring.
8. Display a set of conditions concerning e-mail and internet access which workers must accept before being allowed online.
9. If it is necessary to check the e-mail in-boxes of workers in their absence, make sure that they are aware that this will happen.
10. Inform workers of the extent to which information about their internet access and e-mails is retained in the system and for how long this information is retained.
11. Review the results of any monitoring taking account of the possible unintentional access of websites by workers.

## Notes and examples

1. A policy on use of electronic communications should
  - 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
  - explain the purposes for which any monitoring is conducted, the extent of the monitoring and the means used
  - advise employees what personal information they are allowed to include in particular types of communication and the alternatives that should be used, e.g. communications with the company doctor should only be sent by internal mail rather than e-mail.
  - lay down clear rules regarding the personal 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
  - outline how the policy is enforced and penalties which exist for a breach of policy.

Workers will base their expectations of privacy not only on the employer's stated policy but also on its practice. For example, if the employer's policy imposes a ban on private telephone calls but in practice the employer 'turns a blind eye' to a limited number of private calls, the employer will not be able to refer to a complete ban as part of its justification for monitoring.

2. Except in limited circumstances that are unlikely to apply to the monitoring of communications by employers, interception, without the consent of sender and recipient, is against the law unless it is authorised by the Lawful Business Practice Regulations. This is the case for both public and private sector businesses. An 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 therefore includes access to e-mails before they have been opened by the intended recipient, but does not include stored records of e-mails that have been received and opened.



**See Further Information Page 00 which explains more about the circumstances in which the Regulations authorise interception.**

3. Consider the following in assessing whether communications monitoring is justified and in determining its scope.
  - Limit monitoring to that necessary to ensure the security of the system, e.g. protection from intrusion and from viruses, or detection of the misuse of passwords.
  - Rely on established methods of supervision of workers rather than electronic monitoring.
  - Concentrate on the investigation of specific incidents or problems, for example accessing stored e-mails to follow up an allegation of racial harassment involving the use of the e-mail system, rather than undertaking continuous monitoring.
  - Undertake spot checks or audit rather than continuous monitoring.
  - Target monitoring at areas of highest risk.
  - Automate monitoring. This can reduce the extent to which extraneous information is made available to any person other than the parties to a communication. For example, monitoring to protect the security of a computer system can generally be automated. Monitoring to detect references to matters of particular sensitivity, for example the name of a company involved in a merger negotiation, might also be automated. Automated monitoring systems are becoming increasingly sophisticated and their capabilities should be exploited to assist data protection compliance, for example through the ability to target monitoring at suspicious patterns of activity.
4. Do not introduce monitoring or the recording of the content of calls for every situation. Consider whether an acceptable reduction in risk can be achieved by the use of an itemised call record. If the itemised call record is inadequate for this purpose, assess whether it can be used to help ensure that monitoring is strictly limited and targeted. For example, there might be evidence that commercial secrets are being passed to a competitor. By examining itemised call records it might be possible to narrow down those under suspicion and target monitoring accordingly.
5. Monitoring external calls will mean collecting information about those people who make calls to or receive

calls from the organisation as well as ~~on about~~ workers. These ~~others people~~ are ~~just as also~~ entitled to be told that monitoring is taking place and why. Provide this information, where reasonably practicable, through the use of recorded messages on telephone systems. Don't forget that those who might be making personal calls to workers are less likely to expect that their calls may be monitored, or to understand why, than, for example, customers who might expect some recording to take place. If there is no better way of providing information, instruct workers to inform callers that their calls may be recorded and to explain why this is the case.

6. Where employers pay for mobile phones for workers' personal use or for land lines in their homes, they may receive itemised bills directly or via their workers. If bills are received directly, workers should be made aware of the extent of information about private use received by the employer. In either case, information about personal calls should not be used for monitoring. It may be used for billing or in exceptional circumstances ~~perhaps~~ where there is evidence of criminal activity accessed as part of a specific investigation.
7. Consider the following in assessing whether e-mail monitoring is justified and in determining its scope.
  - Use a record of e-mail traffic rather than monitoring the content of messages. If the traffic record alone is not sufficient, ~~consider how far it can be used to ensure any further monitoring is strictly limited and targeted.~~<sup>12</sup> use the traffic record to narrow the scope of content monitoring, for example by only examining the content of messages that are being sent to a rival organisation.
  - Restrict the monitoring of e-mails sent to specific workers to messages that the worker has received and has chosen to retain ~~rather than to delete.~~<sup>13</sup>
  - Do not open e-mails if there is a reason to believe they are personal.
  - Use, as far as is if feasible, an automated monitoring and detection process, that for example detects viruses or limits the size of attachments that can be received
  - Provide facilities that allow messages to be sent that do not bear the employer's 'official' heading. This should reduce the risk of employers' liabilities in respect of personal e-mails sent using the employer's equipment.
  - Set up secure lines of communication, for example for the transmission of sensitive information from the worker to an occupational health advisor or for trade union communications, that will not be subject to monitoring. Some systems can be set up so that messages to and from particular individuals or sections of the organisation are not subject to monitoring or are monitored differently to others
  - Set up a system that allows workers to mark personal communications as such.
  - Provide a separate e-mail account, encryption capability or access to web-based mail services for personal use.
  - Bear in mind that e-mails and associated records can be falsified. Without special measures their value as evidence in court is likely to be limited.

Consider the following in assessing whether internet access monitoring is justified and in determining its scope. If internet monitoring is determined to be necessary, follow this guidance.

- Design monitoring so that it prevents rather than detects misuse, for example by blocking access to inappropriate sites or material by using web-filtering software. (NB: Web filtering systems are becoming increasingly sophisticated and may be able to deliver real protection to employers with little intrusion on workers. For example, products are available that, it is claimed, can undertake complex analysis of images and thereby prevent the display of sexually explicit material.)
  - Record the time spent accessing the Internet rather than the sites visited or the contents viewed
  - Where possible separate private internet access from business access, perhaps by having a different log-on for private use and then limiting the collection of information on private use to the length and time of the session
  - Undertake monitoring on an aggregated basis, for example examining logs of which sites have been accessed from which departments and only focussing on specific workers if it is apparent there is a problem.
8. Use the capabilities of electronic systems to remind workers of their responsibilities. These can be set so that workers cannot proceed to access the internet or e-mail services without acknowledging the acceptance of certain conditions.
  9. The purpose of doing this should be to ensure the business responds properly to its customers and other contacts. Only check e-mail in-boxes, and use personal information obtained in them, for other purposes, if there is reason to believe the intrusion is justified by the risks.

<sup>12</sup> ~~Not sure what this means.~~

<sup>13</sup> ~~Again not sure what this means~~

10. There are a variety of ways in which workers can be told about the retention of information about their e-mail or internet usage. This might be done by giving them an information pack addressing this when they are given access to the office's internet or e-mail systems, or by displaying on-line information on their computer. It is important to ensure that workers are aware of retention issues and, in particular, that they are not misled into believing that information will be either deleted or retained when this is not the case.
11. Websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising or miskeying.

## 5 VIDEO AND AUDIO MONITORING

The Information Commissioner has published [a CCTV Code of Practice](#) which looks at these issues ~~albeit primarily~~ in the context of monitoring places to which the public have access ~~rather than~~ workplaces.



See *Further Information Useful Addresses Page 00* for Information Commission details to obtain a copy.

### The benchmarks

1. *Apply the approach suggested in this Code in assessing what, if any, video and audio monitoring is justified by the risks. Limit the scope of monitoring to what is strictly required to reduce the risk or risks it is intended to address.*
2. *Give workers a clear notification that video or audio monitoring is being carried out and why it is being carried out.*
3. *Ensure that people other than workers, such as visitors or customers, who may inadvertently be captured by monitoring, are made aware of its operation and its purposes.*

---

## Notes and examples

1. Consider the following in assessing whether video and audio monitoring is justified and in determining its scope.
  - Target video and audio monitoring at areas of particular risk, for example where there is a risk to safety or security. Bear in mind that such routine monitoring is only likely to be justified where there are particular safety or security risks that cannot be adequately addressed in other, less intrusive, ways.
  - Confine monitoring to areas where workers' expectations of privacy will in any case be low, for example areas to which the public have access.
  - Treat video and audio capability separately. Cases where both video and audio monitoring are justified are likely to be extremely rare. Video monitoring with an audio capacity is even more intrusive than video monitoring alone.

---

2. Employers carrying out monitoring should make it clear to workers that monitoring is taking place and why it is being carried out. This could be done by ensuring that in areas subject to monitoring, a prominent sign is displayed that identifies the organisation responsible for the monitoring and the purposes of the monitoring, and carries details of who to contact regarding the monitoring.

---

3. Not only workers but also others who might be caught by monitoring should be informed that it is taking place and why it is taking place. Any notification given should identify the organisation responsible for the monitoring, its purposes, and should say who to contact regarding the monitoring.

## 6 IN-VEHICLE MONITORING

Technology increasingly allows for the type of monitoring that takes place in the workplace to be extended to vehicles used by workers off-site, for example to company cars or delivery vehicles. Devices can record or transmit information such as the location of the 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 and so will fall within the scope of the Data Protection Act.

### The benchmarks

- 1. Apply the approach suggested in this Code in assessing what, if any, monitoring of vehicles used by workers is justified by the risks. Limit the scope of monitoring to what is strictly required to reduce the risk or risks it is intended to address.*
- 2. Set out a policy that states what use can be made of vehicles provided by, or on behalf of, the employer, and any conditions attached to use.*
- 3. Avoid using covert monitoring unless the benchmarks set out in this Code are met. If in exceptional circumstances there is a justification for extending covert monitoring to private use of a vehicle, involve the police.*

## Notes and examples

1. Consider the following in assessing whether in-vehicle monitoring is justified and in determining its scope.
  - Information that relates to private use of vehicles, in particular the location of the vehicle, will be the most intrusive.
  - Where private use of vehicles supplied by, or on behalf of, the employer, is allowed, monitoring their movement when used privately, without the freely given consent of the user, will rarely be justified. (Note: this means that if the vehicle is used for both private and business use there needs to be a 'privacy button' or other arrangement that enables the monitoring to be disabled.)
  - Monitoring of vehicles owned by or leased to workers will only be justified where the vehicle is used for business purposes, the worker has freely consented to the installation and use of any monitoring device and the information collected by the employer is strictly necessary for its business purposes, for example reimbursing the worker for the cost of business use.

This approach should be applied even if vehicles are provided by, or on behalf, of the employer, exclusively for business and related use, e.g. home to work journeys.

- 
2. It is important to lay down clear rules as to what private use is or is not allowed of vehicles supplied by, or on behalf of, the employer and the conditions that attach to both private and business use. Workers should be told clearly of any monitoring that takes place and how any information obtained will be used. It should be possible for the user to disable any monitoring of the vehicle's movements when it is being used privately although there may be a facility to override this in exceptional circumstances, e.g. theft.

Ensure workers given access to vehicles are aware of the policy.

- 
3. In some circumstances covert monitoring of the private use of a vehicle would be 'intrusive surveillance' under the terms of RIPA. If not, it would almost certainly be 'directed surveillance'. It is ~~hard to see circumstances where unlikely that~~ an employer would be justified in installing secret video cameras or other covert monitoring devices in a privately used vehicle. If in exceptional circumstances such monitoring is justified, for example where there is evidence of a vehicle being used to carry out criminal activity, any monitoring should take place under the direction of the police.

## 7 MONITORING PRIVATE INFORMATION

This is where employers use information held by third parties, such as credit reference information or the electoral roll, to monitor workers. It can also include information held by employers in a non-personnel capacity such as when a bank monitors its workers' bank accounts.

### The benchmarks

1. *Apply the approach suggested in this Code in assessing what, if any, monitoring of workers' private information is justified by the risks. Limit the scope of monitoring to what is strictly necessary to reduce the risk or risks it is intended to address.*
2. *Tell workers what information sources are to be used to carry out checks on them and for what purposes the checks are to be carried out.*
3. *Ensure that if workers are monitored through the use of information held by a credit reference agency that 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. This could be a criminal offence.*
4. *~~Do not~~ Avoid monitoring workers through information you have as a result of a different relationship with them.*
5. *Ensure that staff carrying out this type of monitoring are properly trained to do so and put in place rules preventing the disclosure or inappropriate use of information obtained in connection with the monitoring.*
6. *~~Do not~~ Avoid retaining all the information obtained in connection with the monitoring but merely record that a check has taken place and the result of this.*

## Notes and examples

1. Consider the following in assessing whether monitoring private information is justified and in determining its scope.
  - The presumption should be that workers are entitled to keep their private lives private. Employers should not intrude into this unless they face a real risk to which the intrusion is a proportionate response.
  - Monitoring should be justified by evidence, ~~not intuition.~~ For example, workers' financial circumstances should not be monitored unless there is evidence that workers in financial difficulties actually pose a significant risk to the employer.
2. Workers can be told about the sources that will be used to carry out checks on them in a variety of ways. General information can be put in a staff handbook, displayed on a notice-board or delivered on-line to workers with access to computer systems. However, where a specific check is to be carried out, ~~for example as part of a data matching exercise,~~<sup>14</sup> the worker should be specifically informed of this unless to do so would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
3. Section 55 of the Act makes it a criminal offence to obtain personal information without the authority of the data controller. Credit reference agencies hold a range of information about individuals. Some can only be used for credit decisions. An employer ~~using a facility provided to assist it in making credit decisions about customers obtaining access to this information~~ for employee monitoring ~~by using a facility provided to assist it in making credit decisions about customers~~ is likely to be obtaining information without the authority of the agency.

Bear in mind that information held by credit reference agencies is based on public records which are not compiled with worker monitoring in mind. They can be incorrect or misleading.

4. Do not monitor workers through information you have as a result of a different relationship with them, e.g. as a customer or client, unless it is based on a condition of employment and the intrusion caused by the monitoring is justified by the risk faced. This is only likely to be so in special cases; for example a bank must not routinely monitor the bank accounts of all workers. If monitoring can be justified it must be targeted at particular individuals and particular information that poses a risk. In this case monitoring to detect serious indebtedness by the most senior workers might be justified on the basis of avoiding potential public embarrassment to the bank. This would not however justify examining the details of payments made by these workers unless criminal activity was suspected.
5. Take steps to ensure the reliability of staff that have access to worker records. This is especially important where particularly sensitive or personal information is likely to come into their hands. This is not simply a matter of carrying out background checks; it also involves training and ensuring that workers understand their responsibilities in respect of confidential or sensitive information. Consider placing confidentiality clauses in the contracts of employment of relevant staff.
6. Once information has been obtained through monitoring and any necessary evaluation of this made, do not retain the information unless there is an overriding reason for doing so. Usually it will be sufficient to record that the evaluation has been carried out and its result. In any event, do not retain the information for more than 6 months.

<sup>14</sup>~~I have deleted this reference as "Data matching" is not a common term.~~

---

## SECTION 3: FURTHER INFORMATION

### Useful addresses

#### Office of the Information Commissioner

Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Telephone: 01625 545745 (for information and other parts of the Code) or

01625 545740 (for notification)

Fax: 01625 524 510

E-mail: [mail@dataprotection.gov.uk](mailto:mail@dataprotection.gov.uk) (for information and requests for other parts of the Code) or

[mail@notification.demon.co.uk](mailto:mail@notification.demon.co.uk) (for notification and to view the register)

Websites: [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk) (for information and to download other parts of the Code) or

[www.dpr.gov.uk](http://www.dpr.gov.uk) (for notification)

#### Chartered Institute of Personnel and Development

CIPD House  
Camp Road  
London  
SW19 4UX

Telephone: 020 8971 9000

Fax: 020 8263 3333

Website: [www.cipd.co.uk](http://www.cipd.co.uk)

#### Commission for Racial Equality

Elliot House  
10-12 Allington Street  
London  
SW1E 5EH

Telephone: 020 7828 7022

Fax: 020 7630 7605

E-mail: [info@cre.gov.uk](mailto:info@cre.gov.uk)

Website: [www.cre.gov.uk](http://www.cre.gov.uk)

## **Disability Rights Commission**

DRC Helpline  
Freepost MID 02164  
Stratford-upon-Avon  
CV37 9BR

Telephone: 08457 622 633  
Fax: 08457 778 878  
Textphone: 08457 622 644  
E-mail: [ddahelp@stra.sitel.co.uk](mailto:ddahelp@stra.sitel.co.uk)  
Website: [www.drc-gb.org](http://www.drc-gb.org)

## **Equal Opportunities Commission**

Customer Contact Point  
Arndale House  
Arndale Centre  
Manchester  
M4 3EQ

Telephone: 0161 833 9244  
Fax: 0161 838 8312  
E-mail: [info@eoc.org.uk](mailto:info@eoc.org.uk)  
Website: [www.eoc.org.uk](http://www.eoc.org.uk)

## **British Benchmarks Institute (BS7799)**

BSI-DISC  
389 Chiswick High Road  
London  
W4 4AL

Telephone: 020 8995 7799  
Fax: 020 8996 6411  
E-mail [c\\_cure@bsi.org.uk](mailto:c_cure@bsi.org.uk)  
Website: [www.bsi.org.uk](http://www.bsi.org.uk)

## **Advisory, Conciliation and Arbitration Service ACAS**

Brandon House  
180 Borough High Street  
London  
SE1 1LW

Telephone: 020 7396 5100  
Website: [www.acas.org.uk/contact\\_us.html](http://www.acas.org.uk/contact_us.html) (contact details of offices throughout the UK)

## Sensitive Personal Data

### *When can sensitive personal data be processed?*

The Act sets out a series of conditions, at least one of which has to be met before an employer can collect, store, use, disclose or otherwise process sensitive personal data. The conditions which are most likely to be relevant to monitoring at work are:-

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

Note: This condition can have quite wide application in the context of monitoring at work. Employers' rights and obligations may be conferred or imposed by statute or common law, which in this context means decisions in relevant legal cases. For example, they will include obligations to;

- ensure the health, safety and welfare at work of worker
- ensure a safe system of work
- ensure a safe working environment
- not discriminate on the grounds of race, sex or disability
- protect customers' property or funds in the employer's possession
- only dismiss workers when it is fair to do so

Thus an employer may be able to collect and use sensitive data in the course of monitoring if the monitoring is necessary to enable it to meet its legal obligations, for example to ensure the safety of workers, or to prevent unlawful discrimination. The collection and use of sensitive personal data must however be 'necessary' for exercising or performing a right of obligation that is conferred or imposed by law. This condition would not, for example, be satisfied if the employer collects sensitive data in the in the course of monitoring to ensure it is not discriminating if it could reasonably ensure this without the use of monitoring or without the use of sensitive data.

- The processing –
- is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- is necessary for the purpose of obtaining legal advice, or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Note: The application of this condition to the use of information obtained through monitoring in the context of tribunal or court proceedings should be obvious. This condition is also relevant once an employment contract is in place and legal rights stem from it. For example, once a contract is in place the employer has a legal right to insist that the worker meets his or her obligations under the contract. To exercise this right the employer must be able to take reasonable steps to monitor the performance of the worker. The processing of sensitive data must be ‘necessary’. The monitoring must be directed at a clear contractual obligation placed on the worker and the monitoring must be the only reasonable way of ensuring the obligation is met.

- The processing –
- is of information in categories relating to racial or ethnic origin, religious or other beliefs or physical or mental health,
- is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment,
- there are safeguards for the data subject.

Note: This condition may have some relevance to monitoring that is designed to prevent discrimination on the grounds of racial origin, religion or disability. Processing must be “necessary” emphasising that monitoring should only be used where discrimination cannot reasonably be prevented by other means.

- The processing is necessary
- for the exercise of any functions conferred on any person by or under an enactment or
- for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Note: This condition will be relevant for a public sector body that has specific legal duties placed on it in relation to the conduct or probity of its workers. It will also be relevant when a public sector body concludes that in order to discharge its wider statutory functions it is necessary for it to monitor workers and in doing so to process sensitive personal data.

The processing is in the substantial public interest, is necessary for the prevention or detection of any unlawful act and must necessarily be carried out without the explicit consent of the data subject being sought, so as not to prejudice those purposes.

Note: This condition will cover situations where monitoring is necessary to detect criminal activity in the workplace and where seeking the consent of the workers involved would amount to a tip off. ‘Unlawful acts’ include not only criminal matters but also acts that breach other statutory or common law

obligations.

The processing is in the substantial public interest, is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or other service and is carried out without the consent of the data subject because the processing-

is necessary in a case where consent cannot be given by the data subject

is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or

must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

Note: This condition will cover the monitoring of calls to confidential counselling, advice or support lines such as those run by some charities, for example The Samaritans.

- The data subject has given explicit consent to the processing

Note: Employers seeking to rely on this condition must bear in mind that:-

- the consent must be explicit. This means the applicant must have been told clearly what personal data are involved and the use that will be made of them. The applicant must have given a positive indication of agreement e.g., a signature.
- the consent must be freely given. This means the applicant must have a real choice whether or not to consent and there must be no significant detriment that arises from not consenting.

The extent to which consent can be relied upon in the context of monitoring is limited because of the need for any consent to be freely given.

## The Lawful Business Practice Regulations

This section provides guidance to employers who wish to monitor electronic communications (e.g., telephone calls, faxes, e-mails, internet access) on how they can meet the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations).<sup>15</sup> The RIPA and LBP Regulations are not straightforward. This guidance is designed to assist employers. It is intended to cover all the main points but is necessarily simplified. It is not a complete statement of the law but employers following it are unlikely to find themselves on the wrong side of the law.

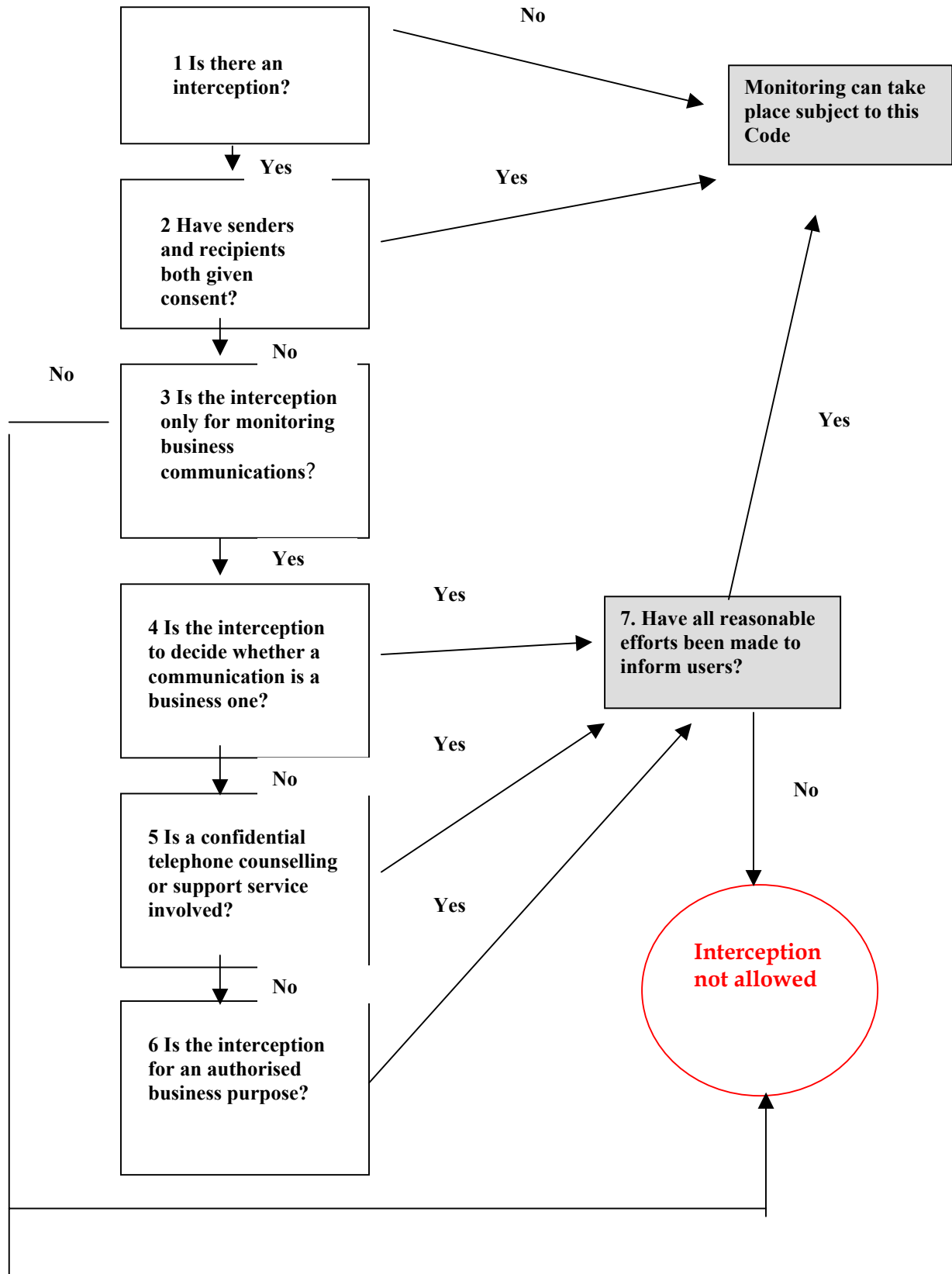
Under RIPA it is against the law for an employer to intercept an electronic communication on its, or anyone else's, system. There are some exceptions. The LBP Regulations contain those exceptions most likely to be relevant. They set out when an employer is authorised to carry out an interception for the purpose of running its business. The exceptions provide considerable scope for employers. It must be remembered though that they are not exemptions from the Data Protection Act.

Except in limited circumstances that are unlikely to apply to the monitoring of communications by employers, for example where interception is authorised under a warrant, if monitoring involves an interception of communications that and it does not come within the exceptions in the LBP Regulations, it is against the law to carry it out. It is irrelevant whether or not the monitoring would satisfy the other provisions of this Code. On the other hand, if the interception does come within the exceptions, the monitoring cannot proceed regardless. The collection, storage, and use of personal information that is involved in the monitoring must still satisfy Data Protection requirements as described in this Code.

---

<sup>15</sup> Is this the correct way of writing these Regulations, including the arrangement of brackets?

The following diagram shows how to check whether the requirements of RIPA and the LBP Regulations are met.



## NOTES

1. Interception takes place if the contents of a communication are made available, during the course of its transmission, to someone other than the sender or intended recipient. Examples of interception include a supervisor listening in to calls in a call centre, an employer opening e-mails stored on its server before they have been opened by the intended recipient, and an automated system that opens e-mails and/or their attachments to check them for viruses. Examples that do not involve interception include an employer accessing a stored collection of e-mails that have been received and opened or deleted by the intended recipient, and an employer accessing a stored collection of sent e-mails.
2. Interception is allowed if the employer has reasonable grounds for believing that both the sender and recipient have consented to the interception. Interception is also allowed in certain other circumstances without the consent of the sender or recipient. However, if an employer is to rely on consent in order to legitimise an interception, there must be some action from which consent can be inferred, for example, saying “yes” when asked or proceeding with a telephone call after hearing a message saying that calls are recorded. Consent must be freely given. Employers may choose to rely on consent to cover the interception of telephone calls or internal e-mails but it is hard to see how consent can readily be obtained from external senders of e-mail. The employer still has a general duty to make all reasonable attempts to inform users of the system that communications may be intercepted.
3. Interception is not allowed by a business unless the interception is solely for monitoring (or recording) communications which:-
  - involve the business entering into transactions or
  - relate in another way to the business or
  - take place in some other way in the course of carrying on the business.

These categories cover a very wide range of business communications but they do not include personal communications by workers unless they relate to the business. Interception will not be allowed if it is carried out wholly or partly to gain access to the contents of personal communications sent to or by workers that do not relate to the business. This does not prevent interception which is carried out only to gain access to the contents of business communications but which may incidentally and unavoidably involve some access to other communications on the system.

4. Interception is allowed if it is to check whether a communication is a business one (as defined in 3 above). For example, an employer is allowed to open e-mails in an absent worker’s inbox if this is necessary to see whether there are business communications that need to be dealt with in the worker’s absence. This does not allow the employer to open e-mails that can be identified as personal without opening them.
5. Interception is allowed if it is to monitor communications to a confidential, free, telephone counselling or support service operated in such a way that users can remain anonymous. This is to enable help-line workers to receive appropriate supervision and support.
6. Interception is allowed if it is part of monitoring (or recording) business communications for one of the following purposes:-
  - to establish the existence of facts (e.g. to collect evidence of transactions such as those involved in telephone banking or to keep records of other communications where the specific facts are important, such as being able to prove that a customer has been given certain advice);

- to check that the business is complying with regulatory or self-regulatory procedures (e.g. to check that workers selling financial services are giving customers the “health warnings” required under financial services regulation);
  - to check the benchmarks that workers are achieving (e.g., to check the quality of e-mail responses sent by workers to customer enquiries);
  - to show the benchmarks that workers ought to achieve (e.g. for staff training);
  - to prevent or detect crime (e.g. to check that workers or others are not involved in defrauding the business);
  - to investigate or detect unauthorised use of the telecommunications system (e.g., to ensure that workers do not breach the employer’s rules on use of the system for business purposes, for example by sending confidential information by e-mail without using encryption if this is not allowed. Note that interception that is targeted at private communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised);
  - to ensure the security of the system and its effective operation (e.g., to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).
7. The requirement is to make reasonable efforts to inform users of the system that an interception may take place. This requirement adds no additional burden to the requirement of the Data Protection Act to provide information to those whose data are processed. Workers will be users but outside callers or senders of e-mail will not be. Where, as will usually be the case, interception involves the collection, storage or use of personal data, the requirements of the Act will come into play.

## Communication: levels of monitoring

The tables below give guidance on the level of monitoring likely to be permissible under the Code.

Level of intrusion

| <b>Pure business communications</b>   |  |
|---|--|
| <p>These are the types of communications that only deal with business matters. Typically they would include letters sent out on a business' headed paper or electronic equivalents. The communication contains no information of a particularly personal or intimate nature.</p>  |  |
| <i>Example</i>  | <i>Guidance on monitoring</i>  |
| <p><b>Example 1:</b> An e-mail from a company accountant to a supplier querying why an invoice has been submitted for goods that have not been supplied.</p> <p><b>Example 2:</b> Work contact details submitted by a health and safety officer to a website so that information about fire safety equipment can be returned.</p> | <p>Disclosure of its contents would be unlikely to cause damage or distress to any worker. To the extent to which it is not obvious, it is sufficient that workers are aware in general terms, that the work they do is likely to be monitored or checked. It is difficult to envisage how such monitoring could be considered to be a disproportionate infringement of privacy.</p> |

| <b>Business communications of a personal nature</b>   |   |
|---|---|
| <p>These are communications taking place in the workplace that are clearly for genuine business reasons but contain information that is of a personal nature. Many 'personnel' type communications will fall into this category and in many instances the worker identified in this type of communication would object to the information made widely available in the workplace.</p> |   |
| <i>Example</i>  | <i>Guidance on monitoring</i>   |
| <p><b>Example 1:</b> A report submitted for e-mail from a worker to a line manager requesting leave of absence from work because of serious sickness in the family.</p> <p><b>Example 2:</b> A report submitted for a disciplinary hearing relating to a worker's alleged misconduct.</p>   | <p>A worker must not be misled into thinking that a communication is private if this is not the case. Those carrying out monitoring should be clear on procedures and fully trained. They have responsibilities to ensure that information obtained through monitoring is kept secure, only used for the purpose for which it was obtained and is deleted once the purpose for carrying out the monitoring is complete.</p> |

| <b>Personal communications</b>  |  |
|---|--|
| <p>This Code makes it clear that there is no obligation under the Act for employers to provide communications equipment for workers' own private use. However, many employers choose to do this. Although employers may provide such facilities, they may face real risks if they do so. For example, a worker might use internet access facilities to download pornography in the workplace. It follows, therefore, that even where personal use of communications systems is allowed, there may be exceptional circumstances where monitoring is necessary.</p> |  |
| <i>Example</i>  | <i>Guidance on monitoring</i>  |
| <p><b>Example 1:</b> A worker's submission to an on-line chat-room where matters unrelated to work are discussed with members of the on-line general public.</p> <p><b>Example 2:</b> An e-mail between two workers complaining to each other about how they are treated by their employer.</p>   | <p>These are circumstances in which workers might reasonably expect that their communications will be private, unless workers have been told clearly that monitoring will take place. Even if workers are told this, it will be intrusive and must be kept to the minimum necessary to address risks. A ban on personal communications does not in itself justify routine monitoring of the content of such communications. Such a ban and the existence of alternative facilities for private communications are relevant factors but the intrusion must still be justified by the risks.</p> |

## **FAQs (note: these to be replaced / supplemented by monitoring-related FAQs)**

### **Aren't paper files exempt from the Data Protection Act – are we OK if we don't computerise them?**

No. Manual data held within a “relevant filing system” are now covered by the Act. This is defined as any set of data which is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible. An example of a relevant filing system would be a personnel file with a worker's name or individual reference number on it, in which it is possible to find information about the worker such as starting date, performance mark at last appraisal, previous employer etc.

### **Isn't there an exemption in the Act for confidential records?**

There is no such general exemption from the right of subject access. There is, however, a special exemption from the right of access to a confidential reference in the hands of the employer who gave it. This exemption does not apply once the reference is in the hands of the employer receiving it although, even then, the employer is entitled to take steps to protect the identity of third parties such as the author of the reference.

### **Do I have to get a person's consent to keep records about him or her?**

Explicit consent to hold personal data relating to workers is not usually required. An employer can usually rely on the last of the conditions laid down in Schedule 2 of the Act which states that personal data may be processed for the purposes of legitimate interests pursued by the data controller.

Employers are much more likely to need the consent of workers if they are processing sensitive personal data rather than non-sensitive personal data. In this case, the consent must be “explicit”. However, even then, sensitive personal data can be processed without explicit consent where the processing is necessary in order to enable the employer to comply with any legal obligation. For example, data about the racial or ethnic origin of workers may be held in order to comply with the law relating to racial discrimination. Similarly, sickness records of workers may be kept in order to enable employers to meet the requirements imposed on them by the law in relation to statutory sick pay.

### **Can we disclose personal data to prospective purchasers of the company?**

The Act doesn't necessarily prevent this. However, if it is not unduly difficult to do so and the prospective purchasers' needs can still be met the information should be anonymised, for example by providing the numbers of workers in each grade rather than their names. If personal information needs to be made available the employer should ensure that the prospective purchaser signs up to conditions on how it will be used. Employers should also ensure that information is returned or destroyed if the sale of the company does not proceed.

### **How can the company be expected to keep accurate records if workers give us inaccurate information?**

Provided that the employer has taken reasonable steps to ensure the accuracy of the information, the data protection principle that requires personal information to be accurate will not be breached.

---

**If the Act forces us to delete information, how are we supposed to protect ourselves against allegations that we have discriminated against someone?**

The Act doesn't require that all information be deleted straight away. However, information that is retained for a particular purpose should not be kept for longer than is necessary for that purpose. Employers should therefore consider carefully what information they hold and why they hold it. A 'risk analysis' approach to the retention of information might be useful.

~~(((Please note that more FAQs may be added)))~~

((These now will be printed on the back cover and will also be available on website and therefore are not part of the Code)))

Following the Code will

- increase trust in the workplace - there will be transparency regarding information held on workers in the organisation, 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 mean that employers will guard themselves from challenges against their data protection practices.
- encourage workers to respect the personal data of customers - following the Code will create a general level of awareness around data protection, helping to improve relations with customers on this issue.
- aid organisations in meeting other legal requirements - the Code is consistent with other pieces of legislation including The Human Rights Act 1998 and The Regulation of Investigatory Powers Act 2000 (RIPA).
- assist global businesses in complying 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 legal requirements in other European Union member states in regards to data protection.
- help to safeguard against illicit use of information by workers - informing employees 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.