Data protection

The employment practices code

Information Commissioner's Office

Contents

About the code

Our aim

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

Who is the code for?

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

The benefits of the code

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

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

Following the code will:

- increase trust in the workplace – there will be transparency about information held on individuals, thus helping to create an open atmosphere where workers have trust and confidence in employment practices.
- encourage good housekeeping – following the code encourages organisations to dispose of out-of-date information, freeing up both physical and computerised filing systems and making valuable information easier to find.
- protect organisations from legal action – adhering to the code will help employers to protect themselves from challenges against their data protection practices.
- encourage workers to treat customers' personal data with respect – following the code will create a general level of awareness of personal data issues, helping to ensure that information about customers is treated properly.
- help organisations to meet other legal requirements – the code is intended to be consistent with other legislation such as the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA).
- assist global businesses to adopt policies and practices which are consistent with similar legislation in other countries – the code is produced in the light of EC Directive 95/46/EC and ought to be in line with data protection law in other European Union member states.
- help to prevent the illicit use of information by workers – informing them of the principles of data protection, and the consequences of not complying with the Act, should discourage them from misusing information held by the organisation.

What is the legal status of the code?

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

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

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

Who does data protection cover in the workplace?

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

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

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

What information is covered by the code?

Information about individuals, that is kept by an organisation on computer in the employment context, will fall within the scope of the Data Protection Act and therefore, within the scope of this code However, information that is kept in simple manual files will often fall outside the Act. Where information falls outside the Act, this code can do no more than offer advice on good information handling practice.

Personal information

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

- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature, and
- identifies a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession.

This means that automated and computerised personal information kept about workers by employers is covered by the Act. It also covers personal information put on paper or microfiche and held in any 'relevant filing system'. In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered.

Only a well structured manual system will qualify as a relevant filing system. This means that the system must amount to more than a bundle of documents about each worker filed in date order. There must be some sort of system to guide a searcher to where specific information about a named worker can be found readily. This might take the form of topic dividers within individually named personnel files or name dividers within a file on a particular topic, such as 'Training Applications'.

Processing

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

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

- details of a worker's salary and bank account held on an organisation's computer system
- an e-mail about an incident involving a named worker
- a supervisor's notebook containing information on a worker where there is an intention to put that information in that worker's computerised personnel file
- an individual worker's personnel file where the documents are filed in date order but there is an index to the documents at the front of the file
- an individual worker's personnel file where at least some of the documents are filed behind sub dividers with headings such as application details, leave record and performance reviews
- a set of leave cards where each worker has an individual card and the cards are kept in alphabetical order
- a set of completed application forms, filed in alphabetical order within a file of application forms for a particular vacancy.

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

- information on the entire workforce's salary structure, given by grade, where individuals are not named and are not identifiable

- a report on the comparative success of different recruitment campaigns where no details regarding individuals are held
- a report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals
- a personnel file that contains information about a named worker but where the information is simply filed in date order with nothing to guide a searcher to where specific information, such as the worker's leave entitlement, can be found.

Sensitive personal information

What are sensitive data?

Sensitive data are information concerning an individual's;

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

Sensitive data processed by an employer might typically be about a worker's;

- physical or mental health
  - as a part of sickness records revealed through monitoring e-mails sent by a worker to his or her manager or to an occupational health advisor
  - obtained as part of a pre-employment medical questionnaire or examination.
  - drug or alcohol test results
- criminal convictions
  - to assess suitability for certain types of employment
- disabilities
  - to facilitate adaptations in the workplace
  - to ensure special needs are catered for at interview or selection testing
  - in monitoring equality of opportunity

- racial origin
  - to ensure that recruitment processes do not discriminate against particular racial groups
  - to ensure equality of opportunity
- trade union membership
  - to enable deduction of subscriptions from payroll
  - revealed by internet access logs which show that a worker routinely accesses a particular trade union website.

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

See 'Supplementary guidance', page 72, which explains more about the conditions for processing sensitive data.

What responsibilities do workers have under the Act?

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

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

'Managing data protection', page 11, explains more about allocating responsibility.

Parts of the code

The 'Employment practices code' starts with a section on **managing data protection** in employment practices. It is then split into four parts;

- **recruitment and selection** – is about job applications and pre-employment vetting
- **employment records** – is about collecting, storing, disclosing and deleting records
- **monitoring at work** – is about monitoring workers' use of telephones, the internet, e-mail systems and vehicles
- **workers' health** – is about occupational health, medical testing, drug and genetic screening.

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

The good practice recommendations

Each part of the code consists of a series of good practice recommendations. These good practice recommendations may be relevant to either large or small employers, but some of them address activities that are of a more specialist nature than others or may occur only rarely, particularly in a small business, These recommendations are most likely to be relevant to larger organisations. However, how far they are applicable and what is needed to achieve them will, of course, depend very much not just on size but also on the nature of each organisation.

Supplementary guidance

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

Good practice recommendations – managing data protection

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

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

Key points and possible actions

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

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

Key points and possible actions

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

0.3 Assess what personal information about workers is in existence and who is responsible for it.

Key points and possible actions

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

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

Key points and possible actions

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

See 'Supplementary guidance', page 72, which explains more about the conditions for processing sensitive data.

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

- Consultation is only mandatory under employment law, in limited circumstances and for larger employers but it should nevertheless help to ensure that processing of personal information is fair.
- When formulating new employment practices and procedures, assess the impact on collection and use of personal information.

Part 1: Recruitment and selection

About Part 1 of the code

Data protection in recruitment and selection

The recruitment and selection process necessarily involves an employer in collecting and using information about workers. Much of this information is personal in nature and can affect a worker's privacy. The Act does not prevent an employer from carrying out an effective recruitment exercise but helps to strike a balance between the employer's needs and the applicant's right to respect for his or her private life.

What does this part of the code cover?

This part of the code covers all aspects of the recruitment and selection process from the advertising of vacancies through to the deletion of information on unsuccessful applicants. It does not though deal in detail with the collection and use of health information on job applicants. This is covered in Part 4. Nor does it deal in detail with the right of applicants to access to the information that an employer keeps about them. This is essentially no different from the right of access that a worker has once employed or engaged. This is covered in Part 2.

Some recommendations in the code are only likely to be of relevance to those using sophisticated selection methods such as psychometric testing or to those employing workers with responsibilities that mean that special checks are justified, for example, criminal record checks on those working with children. For this reason some sub sections are likely to be of relevance mainly to larger or specialist organisations.

Verification and vetting

The terms "verification" and "vetting" are both used in this part of the code. Verification covers the process of checking that details supplied by applicants (e.g. qualifications) are accurate and complete. Verification, therefore, is limited to checking of information that is sought in the application or supplied later in the recruitment process. As used here the term also includes the taking up of references provided by the applicant. Where an employer is justified in asking an applicant about any criminal convictions the Criminal Records Bureau provides a verification service covering certain, high risk areas of employment.

Vetting covers the employer actively making its own enquiries from third parties about an applicant's background and circumstances. It goes beyond the verification of details addressed above. As such it is particularly intrusive and should be confined to areas of special risk. It is for example used for some government workers who have regular access to highly classified information.

In some sectors vetting may be a necessary and accepted practice. Limited vetting may be a legal requirement for some jobs, for example, child care jobs under the Protection of Children Act 1999. The Department of Health has developed a Protection of Vulnerable Adults list which employers intending to recruit certain types of care workers are required to consult. Such vetting usually takes place through the Criminal Records Bureau.

See 'Supplementary guidance', page 17, for background information on the Criminal Records Bureau.

Good practice recommendations – Part 1

The parts of the code in this section are:

1.1 Advertising

This sub-section covers any method used to notify potential applicants of job vacancies, using such media as notices, newspapers, radio, television and the internet.

1.1.1 Inform individuals responding to job advertisements of the name of the organisation to which they will be providing their information and how it will be used unless this is self-evident.

Key points and possible actions

- Ensure that the name of your organisation appears in all recruitment advertisements.
- Ensure that your organisation is named on the answerphone message which invites potential applicants to leave details.
- Ensure that your organisation is named on your website before personal information is collected on an online application form.
- To the extent that it is not self evident describe in the advertisement the purposes for which you may use personal information, for example, to market your organisations products and service.

1.1.2 Recruitment agencies, used on behalf of an employer, should identify themselves and explain how personal information they receive will be used and disclosed unless this is self-evident.

Key points and possible actions

- If you use a recruitment agency check that it identifies itself in any advertisement, and that it informs applicants if the information requested is to be used for any purpose of which the applicant is unlikely to be aware.

1.1.3 On receiving identifiable particulars of applicants from an agency ensure, as soon as you can, that the applicants are aware of the name of the organisation holding their information.

Key points and possible actions

- Inform the applicant as soon as you can of the employer's identity and of any uses that the employer might make of the information received that are not self-evident.

  OR

- If the employer does not wish to be identified at an early stage in the recruitment process, ensure the agency only sends anonymised information about applicants. Ensure the employer is identified to individuals whose applications are to be pursued further.

1.2 Applications

This sub-section covers CVs sent 'on spec' as well as more formal responses to job advertisements.

1.2.1 State, on any application form, to whom the information is being provided and how it will be used if this is not self-evident.

Key points and possible actions

- Ensure the name of your organisation is stated on the application form.

- If information from the application form will be used for any other purpose than to recruit for a specific job or passed to anyone else, make sure that this purpose is stated on the application form.

1.2.2 Only seek personal information that is relevant to the recruitment decision to be made.

Key points and possible actions

- Determine whether all questions are relevant for all applicants.
- Consider customising application forms where posts justify the collection of more intrusive personal information.
- Remove or amend any questions which require the applicant to provide information extraneous to the recruitment decision.
- Remove questions that are only relevant to people your organisation goes on to employ (e.g. banking details) but are not relevant to unsuccessful applicants.

1.2.3 Only request information about an applicant's criminal convictions if and to the extent that the information can be justified in terms of the role offered. If this information is justified, make it clear that spent convictions do not have to be declared, unless the job being filled is covered by the Exceptions Order to the Rehabilitation of Offenders Act 1974.

Key points and possible actions

- Consider whether the collection of information about criminal convictions can be justified for each job for which it is sought.
- Check that it is stated that spent convictions do not have to be declared (unless the job is one covered by the Exceptions Order).
- In any case limit the collection of information to offences that have a direct bearing on suitability for the job in question.

See 'Supplementary guidance', page 19, for more information on the Exceptions Order.

1.2.4 Explain the nature of and sources from which information might be obtained about the applicant in addition to the information supplied directly by the applicant.

Key points and possible actions

- Ensure there is a clear statement on the application form or surrounding documents, explaining what information will be sought and from whom.

1.2.5 If sensitive data are collected ensure a sensitive data condition is satisfied.

Key points and possible actions

- Assess whether the collection of sensitive data is relevant to the recruitment process.
- Remove any questions about sensitive data that do not have to be asked at the initial application stage.
- Ensure that the purpose of collecting any relevant sensitive data is explained on the application form or surrounding documentation.
- Ensure the purpose of collection satisfies one of the sensitive data conditions.
- If health information is to be collected, refer to Part 4 of the code: Information About Workers' Health.

See 'Supplementary guidance', page 72, which explains more about the conditions for processing sensitive data.

1.2.6 Provide a secure method for sending applications.

Key points and possible actions

- Ensure that a secure method of transmission is used for sending applications online. (e.g. encryption-based software).
- Ensure that once electronic applications are received, they are saved in a directory or drive which has access limited to those involved in the recruitment process.
- Ensure that postal applications are given directly to the person or people processing the applications and that these are stored in a locked drawer.
- Ensure that faxed applications are given directly to the person or people processing the applications and that these are stored in a locked drawer.
- If applications are processed by line managers, make sure line managers are aware of how to gather and store applications.

1.3 Verification

1.3.1 Explain to applicants as early as is reasonably practicable in the recruitment process the nature of the verification process and the methods used to carry it out.

Key points and possible actions

- Ensure that information provided to applicants for example on an application form or associated documents explains what information will be verified and how, including in particular any external sources that will be used.
- Do not force applicants to use their subject access rights to obtain records from another organisation (i.e. by making such a requirement a condition of getting a job).

1.3.2 Where the need to protect the employer's business, customers, clients or others warrants the collection and verification of details of an applicant's criminal convictions use only a disclosure from the Criminal Records Bureau (CRB) or Disclosure Scotland for this verification.

Key points and possible actions

- Do not attempt to obtain information about criminal convictions by forcing an applicant to use his/her subject access right or from sources other than the CRB, Disclosure Scotland or the applicant.
- Confine the obtaining of a disclosure, as far as practicable, to an applicant it is intended to appoint. Avoid requiring all short-listed applicants to obtain a disclosure.
- Do not share with other employers the information obtained through a "disclosure".
- Abide by the CRB or Disclosure Scotland's code of Practice in obtaining and handling disclosure information.

1.3.3 If it is necessary to secure the release of documents or information from another organisation or person, obtain a signed consent form from the applicant unless consent to their release has been indicated in some other way.

Key points and possible actions

- Ensure applicants provide signed consent if this is required to secure the release of documents to you from another organisation or person.
- Remember that if you mislead another person or organisation into giving you personal information about an applicant you may be committing a criminal offence.

1.3.4 Give the applicant an opportunity to make representations should any of the checks produce discrepancies.

Key points and possible actions

- Ensure that those staff who are involved in verification in your organisation are aware what to do should inconsistencies emerge between what the applicant said in the application and what your checks have discovered.
- Make sure that in this situation, staff inform the applicant and allow them the opportunity to provide an explanation of the inconsistencies.
- Ensure this feedback to the applicant is incorporated into any recruitment procedures.

1.4 Short-listing

1.4.1 Be consistent in the way personal information is used in the process of short-listing candidates for a particular position.

Key points and possible actions

- Check shortlist methods with sources of good practice such as the Equality and Human Rights Commission.

See 'Supplementary guidance', page 83, for contact details.

1.4.2 Inform applicants if an automated short-listing system will be used as the sole basis of making a decision. Make provisions to consider representations from applicants about this and to take these into account before making the final decision.

Key points and possible actions

- Ensure all the applicants are informed that an automated system is used as the sole basis of short-listing and of how to make representations against any adverse decision.
- Test and keep the results produced by the system under review to ensure they properly and fairly apply your short-listing criteria to all applicants.

1.4.3 Ensure that tests based on the interpretation of scientific evidence, such as psychological tests, are only used and interpreted by those who have received appropriate training.

Key points and possible actions

- Determine which such tests are used within your organisation.
- Ensure all tests are assessed by properly qualified persons.

1.5 Interviews

1.5.1 Ensure that personal information that is recorded and retained following interview can be justified as relevant to, and necessary for, the recruitment process itself, or for defending the process against challenge.

Key points and possible actions

- Ensure that all interviewers are aware that interviewees may have a right to request access to their interview notes.
- Ensure that all interviewers are given instructions on how to store interview notes.
- Make provisions for interview notes to be destroyed after a reasonable time, allowing the organisation to protect itself from any potential claims such as those for race or sex discrimination.
- Explain to interviewers or those in contact with applicants, how to deal with a request for access to interview notes.

1.6 Pre-employment vetting

1.6.1 Only use vetting where there are particular and significant risks involved to the employer, clients, customers or others, and where there is no less intrusive and reasonably practicable alternative.

Key points and possible actions

- Find out for which jobs, if any, pre-employment vetting takes place.
- Consider whether pre-employment vetting is justified for each of these jobs and whether the information could be obtained in a less intrusive way.
- Wherever practicable obtain relevant information directly from the applicant and, if necessary, verify it rather than undertake pre-employment vetting.
- Do not vet workers just because a customer for your products or services imposes a condition requiring you to do so, unless you can satisfy yourself that the condition is justified.

1.6.2 Only carry out pre-employment vetting on an applicant as at late a stage as is practicable in the recruitment process.

Key points and possible actions

- Ascertain at which point pre-employment vetting takes place and who is subject to it. Eliminate any comprehensive pre-employment vetting that takes place for all shortlisted applicants (only the people selected for the job should be submitted to comprehensive pre-employment vetting).

1.6.3 Make it clear early in the recruitment process that vetting will take place and how it will be conducted.

Key points and possible actions

- Provide information about any vetting that might take place on application forms or other recruitment material. This should explain the nature, extent and range of sources to be used to carry out the vetting.
- Make clear the extent to which you will release information about the applicant to the sources you use.

1.6.4 Only use vetting as a means of obtaining specific information, not as a means of general intelligence gathering. Ensure that the extent and nature of information sought is justified.

Key points and possible actions

- Ensure that there are clearly stated objectives in any vetting process.
- Consider the extent and nature of information that is sought against these objectives.
- Eliminate any vetting that consists of general intelligence-gathering. Ensure that it is clearly focussed information that will have a significant bearing on the employment decision.

1.6.5 Only seek information from sources where it is likely that relevant information will be revealed. Only approach the applicant's family or close associates in exceptional cases.

Key points and possible actions

- Ensure that those who will seek the information are briefed about which sources to use, ensuring that those sources are likely to produce relevant information.
- Ensure that if family members or close associates are approached it can be justified by the special nature of the job.

1.6.6 Do not place reliance on information collected from possibly unreliable sources. Allow the applicant to make representations regarding information that will affect the decision to finally appoint.

Key points and possible actions

- Ensure that information that has been collected from a vetting process is evaluated in the light of the reliability of the sources.
- Ensure that no recruitment decision is made solely on the basis of information obtained from a source that may be unreliable.
- Ensure that if information received will lead to the applicant not being appointed, then this will be made known to the applicant.
- Put in place a mechanism for providing this feedback, allowing the applicant to respond and obliging those involved in the recruitment decision to take this response into account.

1.6.7 Where information is collected about a person other than the applicant that affects the other person's privacy, ensure so far as practicable that the other person is made aware of this.

Key points and possible actions

- Ensure that those conducting a vetting process are briefed to avoid discovering information about other people unnecessarily.
- Where substantial personal information has been collected about another person and is to be retained, ensure there is a process in place to inform the other person of this and of how the information will be used.

1.6.8 If it is necessary to secure the release of documents or information from a third party, obtain a signed consent from the applicant.

Key points and possible actions

- If you are asking a third party, such as a previous employer, to disclose confidential personal information to you the third party will need the applicant's permission before doing so.
- It may be easier for you to obtain this permission from the applicant and pass it on to the third party than for the third party to obtain permission directly.

1.7 Retention of recruitment records

1.7.1 Establish and adhere to retention periods for recruitment records that are based on a clear business need.

Key points and possible actions

- Assess who in your organisation retains recruitment records (e.g. are they held centrally, at departmental level or in the line).
- Ensure that no recruitment record is held beyond the statutory period in which a claim arising from the recruitment process may be brought unless there is a clear business reason for exceeding this period.
- Consider anonymising any recruitment information that is to be held longer than the period necessary for responding to claims.

1.7.2 Destroy information obtained by a vetting exercise as soon as possible, or in any case within 6 months. A record of the result of vetting or verification can be retained.

Key points and possible actions

- Check who in your organisation retains information from vetting. Ensure that vetting records are destroyed after 6 months. Manual records should be shredded and electronic files permanently deleted from the system.
- Inform those responsible for the destruction of this information that they may keep a record that vetting was carried out, the result and the recruitment decision taken.

1.7.3 Consider carefully which information contained on an application form is to be transferred to the worker's employment record. Do not retain information that has no bearing on the on-going employment relationship.

Key points and possible actions

- Check how information is transferred from recruitment records to employment records.
- Ensure those responsible for such transfers only move information relevant to on-going employment to employment files.

1.7.4 Delete information about criminal convictions collected in the course of the recruitment process once it has been verified through a Criminal Records Bureau disclosure unless, in exceptional circumstances, the information is clearly relevant to the on-going employment relationship.

Key points and possible actions

- Make sure it is only recorded whether a check has yielded a satisfactory or an unsatisfactory result. Delete other information.

1.7.5 If it is your practice to do so advise unsuccessful applicants that there is an intention to keep their names on file for future vacancies (if appropriate) and give them the opportunity to have their details removed from the file.

Key points and possible actions

- Ensure that application forms or surrounding documentation tell applicants that, should they be unsuccessful, their details will be kept on file unless they specifically request that this should not be the case.

1.7.6 Ensure that personal information received during the recruitment process are securely stored or are destroyed.

Key points and possible actions

- Assess who in your organisation presently processes recruitment information.
- Inform them that manual records should be kept securely, for example in a locked filing cabinet.
- Make sure that electronic files are kept securely, for example by using passwords and other technical security measures.

2

Part 2: Employment records

About Part 2 of the code

Data protection in employment records

Running a business necessarily involves keeping records about workers. Such records will contain information that is personal in nature and can affect a worker's privacy. The Act does not prevent an employer from collecting, maintaining and using records about workers but helps to strike a balance between the employer's need to keep records and the worker's right to respect for his or her private life. This part of the code will assist employers not only to comply with the law but also to follow good records management practice.

What does this part of the code cover?

This part of the code covers all aspects of the collection, holding and use of employment records from the initial obtaining of information once a worker has been employed or engaged through to the ultimate deletion of the former worker's record. It also deals with the rights of job applicants as well as workers to access to information the employer keeps about them. It does not though deal in detail with the collection and use of health information. This is covered in Part 4.

Some recommendations in the code are only likely to be of relevance to those involved in particular activities such as marketing to their workers or to those who find themselves in particular situations such as a business merger or acquisition. For this reason some sub sections are likely to be of relevance mainly to larger organisations.

Sickness and injury records

For the purposes of this code it is necessary to distinguish between records that include "sensitive data" and those that do not. The term 'sickness record' is therefore used to describe a record which contains details of the illness or condition responsible for a worker's absence. Similarly, an injury record is a record which contains details of the injury suffered. The term 'absence record' is used to describe a record that may give the reason for absence as 'sickness' or 'accident' but does not include any reference to specific medical conditions.

Many employers keep accident records. Such a record will only be an "injury record" if it includes details of the injury suffered by an identifiable worker.

Sickness and injury records include information about workers' physical or mental health. The holding of sickness or injury records will therefore involve the processing of sensitive personal data. This means one of the conditions for processing sensitive personal data must be satisfied.

Employers are advised as far as practicable to restrict their record keeping to absence records rather than sickness or injury records.

See 'Supplementary guidance', page 72, which explains more about the conditions for processing sensitive data.

Workers' access to information about themselves

Workers, like any other individuals, have a right to gain access to information that is kept about them. This right is known as subject access. The right applies, for example, to sickness records, disciplinary or training records, appraisal or performance review notes, e-mails, word-processed documents, e-mail logs, audit trails, information held in general personnel files and interview notes, whether held as computerised files, or as structured paper records. A fee of up to £10 can be charged by the employer for giving access.

Responding to a subject access request involves:

- telling the worker if the organisation keeps any personal information about him or her;
- giving the worker a description of the type of information the organisation keeps, the purposes it is used for and the types of organisations which it may be passed on to, if any;
- showing the worker all the information the organisation keeps about him or her, explaining any codes or other unintelligible terms used;
- providing this information in a hard copy or in readily readable, permanent electronic form unless providing it in that way would involve disproportionate effort or the worker agrees to receive it in some other way;
- providing the worker with any additional information the organisation has as to the source of the information kept about him or her.

There are a number of exemptions from the right of subject access which can be relevant in an employment context.

See 'Supplementary guidance' – Exemptions from the subject access right, page 42, for details.

References

The provision of a reference about a worker from one party, such as a present employer, to another, such as a prospective employer, will generally involve the disclosure of personal data. In considering how the Act applies to such disclosure it is important to establish who the reference is being given by or on behalf of.

The code therefore distinguishes between a reference given in a personal capacity and one given in a corporate capacity. A corporate reference is one given on behalf of the employer by one of its staff. Many employers have rules about who can give such a reference and what it can include. The employer remains legally responsible for compliance with the Data Protection Act.

A personal reference is one given by a member of staff in an individual capacity. It may refer to work done but it is not given on behalf of the employer. References that are given in a personal capacity do not, at least in data protection terms, incur a liability for the employer.

Under a specific exemption in the Act, a worker does not have the right to gain access to a confidential job reference from the organisation which has given it. However, once the reference is with the organisation to which it was sent then no such specific exemption from the right of access exists. That organisation is though entitled to take steps to protect the identity of third parties such as the author of the reference.

Disclosure requests

Employers regularly receive requests for information about individual workers that come from outside the employer's organisation. An employer has a responsibility to its workers to be cautious in responding to such requests. It risks a breach of the Act if it does not take sufficient care to ensure the interests of its workers are safeguarded. In some cases though the employer has no choice but to respond positively to a request for disclosure. This is where there is a legal obligation to disclose. It is not the Data Protection Act but other laws that create such obligations. Where they do so the Act does not stand in the way of disclosure.

In some other cases the employer will have a choice whether or not to disclose but provided sensitive data are not involved it is clear that the Act will not stand in the way of disclosure. This is where the circumstances of the disclosure are covered by one of the exemptions from the 'non-disclosure provisions' of the Act.

See 'Supplementary guidance': Exemptions from non-disclosure, page 43, for details.

Good practice recommendations – Part 2

The parts of the code in this section are:

2.1 Collecting and keeping general records

2.2 Security

2.3 Sickness and injury records

2.4 Pension and insurance schemes

2.5 Equal opportunities monitoring

2.6 Marketing

2.7 Fraud detection

2.8 Workers' access to information about themselves

2.9 References

2.10 Disclosure requests

2.11 Publication and other disclosures

2.12 Merger, acquisition, and business re-organisation

2.13 Discipline, grievance and dismissal

2.14 Outsourcing data processing

2.15 Retention of records

2.1 Collecting and keeping general records

2.1.1 Ensure that newly appointed workers are aware of the nature and source of any information stored about them, how it will be used and who it will be disclosed to.

Key points and possible actions

- It is not generally necessary to seek a worker's consent to keep employment records. It will usually be sufficient to ensure that the worker is aware that records are being kept and is given an explanation of the purposes they are kept for and the nature of any intended disclosures.
- It is only if sensitive data are collected that consent may be necessary.
- Decide on how best to inform new workers about how information about them will be held, used and disclosed.
- If your organisation has not done so previously, distribute this information to existing workers.
- In large organisations, randomly check with a sample of workers, that they did in fact receive this information. Rectify any communication gaps.

2.1.2 Inform new workers and remind existing workers about their rights under the Act, including their right of access to the information kept upon them.

Key points and possible actions

- Ensure that information given to new workers includes information about their rights under the Act.
- Set up a system to remind existing workers of their rights.

2.1.3 Ensure that there is a clear and foreseeable need for any information collected from workers and that the information collected actually meets that need.

Key points and possible actions

- Review all forms where information is requested from workers.
- Remove or amend any questions which require the worker to provide information extraneous to your needs.

2.1.4 Provide each worker with a copy of information that may be subject to change, e.g. personal details such as home address, annually or allow workers to view this on-line. Ask workers to check their records for accuracy and ensure any necessary amendments are made to bring records up-to-date.

Key points and possible actions

- Determine the different types of personal data kept about workers and whether they are likely to be subject to change.
- Decide whether data that change could easily be viewed electronically and make any changes to systems necessary to enable this.
- Ensure that the system restricts access to individuals' records so that each worker can only get access to his or her own record.
- If it is only possible for workers to view data manually, consider how this can best be done.
- Make provision to amend any details that are incorrect on individual workers' files.

2.1.5 Incorporate accuracy, consistency and validity checks into systems.

Key points and possible actions

- Review computerised systems to see if accuracy checks can be easily built in.
- Put in place arrangements to ensure that when systems are updated or new systems purchased they facilitate data protection compliance.
- Remember that legal responsibility for data protection compliance rests with users rather than suppliers of systems.

2.2 Security

2.2.1 Apply security standards that take account of the risks of unauthorised access to, accidental loss of, destruction of, or damage to employment records.

Key points and possible actions

- BS 7799: 1995 (code of Practice for Information Security Management) provides guidance which, if followed, should address the main security risks.
- Obtain a copy of BS7799 if you do not have one already and compare its recommendations to your own existing procedures.
- Put in place measures to rectify any shortfalls, bearing in mind that not all controls will be relevant to all organisations.

2.2.2 Institute a system of secure cabinets, access controls and passwords to ensure that staff can only gain access to employment records where they have a legitimate business need to do so.

Key points and possible actions

- Review who in your organisation has access to employment records and determine whether it is necessary for everyone who currently has access to retain it.
- Remove access rights from those who have unnecessary or over-extensive access to personal information about others.
- Make sure manual files that hold personal information are securely held with locks and only those who should have access retain the key.
- In the case of computerised records, ensure that passwords or similar controls are set up to limit unauthorised access.

2.2.3 Use the audit trail capabilities of automated systems to track who accesses and amends personal information.

Key points and possible actions

- Check whether computerised systems that retain personal information currently have audit trail capabilities. If they do, check that the audit trail is enabled.
- If they do not, see if it would be possible to create audit trails of who accesses and amends personal information.
- If you have a system with audit trails, ensure that regular checks occur to detect unauthorised or suspicious use. Set up a procedure to investigate patterns of unusual or unauthorised access of personal information.

2.2.4 Take steps to ensure the reliability of staff that have access to workers' records.

Key points and possible actions

- Carry out background checks on staff that will have access to workers' records, for example by taking up references.
- Review the contracts of workers who deal with personal information to ensure they include confidentiality clauses concerning the unauthorised disclosure and use of personal information.
- Set up induction training for these staff that contains explanation about their responsibilities. Organise refresher training as and when necessary.

2.2.5 Ensure that if employment records are taken off-site, e.g. on laptop computers, this is controlled. Make sure only the necessary information is taken and there are security rules for staff to follow.

Key points and possible actions

- Formulate a procedure for taking laptop computers off-site (or review the existing procedure). Include points regarding the information that may be taken off-site, security of passwords and keeping the laptop in view or secured at all times.
- Inform all workers, including senior staff, of the procedure.

2.2.6 Take account of the risks of transmitting confidential worker information by fax or e-mail. Only transmit information between locations if a secure network or comparable arrangements are in place.

Key points and possible actions

- Check that your security policy properly addresses the risk of sending and receiving worker information by e-mail or fax and review the relevant procedures.
- Ensure that all managers use a secure system if workers' records are to be transmitted by fax.
- In the case of e-mail deploy some technical means of ensuring security, such as effective password protection and encryption.
- Advise all managers about permanently deleting e-mails that contain personal information about workers from their work-stations.
- Check whether deleted e-mails will still be kept on a server. Wherever possible ensure these too can be permanently deleted. In any case, restrict access to them.

2.3 Sickness and injury records

2.3.1 Where possible keep sickness and injury records separate from absence and accident records. Do not use sickness records for a particular purpose when records of absence could be used instead.

Key points and possible actions

- Review how sickness and accident records are currently kept.
- If necessary, change the way information on sickness and accidents is kept so that information on workers' health is not accessed when only information on absence or the circumstances of an accident at work is needed.
- Inform those accessing both sickness/injury and absence records of when it is and is not necessary to access the full sickness or injury records.

2.3.2 Ensure that the holding and use of sickness and injury records satisfies a sensitive data condition.

Key points and possible actions

- Check current practices on the use of sickness and injury records against the sensitive data conditions in the code.
- Take any remedial action necessary including restricting the purposes for which records can be used and/or deleting records if no condition can be satisfied.
- Inform those handling sickness and injury records of any changes in procedures or practices.

See 'Supplementary guidance', page 72, which explains more about the sensitive data conditions.

2.3.3 Only disclose information from sickness or injury records about an identifiable worker's illness, medical condition or injury where there is a legal obligation to do so, where it is necessary for legal proceedings or where the worker has given explicit consent to the disclosure.

Key points and possible actions

- Ensure that all those who deal with workers' sickness or injury records are aware in which circumstances there may be a legal obligation to disclose.
- Ensure when appropriate, written consent is obtained from the worker.

2.3.4 Do not make the sickness, injury or absence records of individual workers available to other workers unless it is necessary for them to do their jobs.

Key points and possible actions

- Managers can be provided with information about those who work for them in so far as this is necessary for them to carry out their managerial roles.
- No 'league tables' of individual records should be published.
- Ensure that managers are aware of the sensitive nature of sickness and injury records.

2.4 Pension and insurance schemes

Pension or insurance-based schemes such as those offering private medical care are usually controlled by a third party but can be administered in-house. Some employers also insure their business against sickness by key workers. These recommendations are directed at employers who are party to such schemes rather than at insurance companies or pensions providers.

2.4.1 Do not access personal information required by a third party to administer a scheme, in order to use it for general employment purposes.

Key points and possible actions

- Identify and review schemes currently in operation in your business.
- Identify where information could possibly 'leak' from a scheme to be used for other employment purposes.
- Identify ways of stopping this occurring, for example by passing information in sealed envelopes.

2.4.2 Limit your exchange of information with a scheme provider to the minimum necessary for operation of the scheme bearing in mind the scheme's funding obligations.

Key points and possible actions

- Remember that if information on a worker's sickness, injury or other sensitive data is exchanged a sensitive data condition must be satisfied.
- Bear in mind that your funding of a scheme does not give you a right to receive information about individual scheme members beyond that necessary for the operation of the scheme.
- Review the exchange of information with any scheme providers.
- Identify and eliminate any personal information passed to you by the scheme provider that is not essential to the operation of the scheme.

2.4.3 Do not use information gained from the internal trustees or administrators of pension schemes for general employment purposes.

Key points and possible actions

- Inform trustees and administrators of their general data protection responsibilities. In particular make sure they know they must not use personal information acquired in their capacity as trustee or administrator in their capacity as employer.

2.4.4 If your business takes on the role of broker or your staff act as group secretary for a private medical insurance scheme, ensure that personal information gathered is kept to minimum, limit access to the information and do not use it for general employment purposes.

Key points and possible actions

- Consider carefully what information is actually needed to administer the scheme.
- Limit access to personal data arising from the administration of the scheme and ensure that information gathered in this context is not used for any other purposes.

2.4.5 Ensure that when a worker joins a health or insurance scheme it is made clear what, if any, information is passed between the scheme controller and the employer and how it will be used.

Key points and possible actions

- Assess the information given to workers when they join a health or insurance scheme.
- If no specific mention is made about the transfer of information, amend the documentation about the scheme accordingly.

2.5 Equal opportunities monitoring

2.5.1 Information about a worker's ethnic origin, disability, religion or sexual orientation is sensitive personal data. Ensure that equal opportunities monitoring of these characteristics satisfies a sensitive data condition.

Key points and possible actions

- Check your organisation's current equal opportunities monitoring against the sensitive data conditions in the code.
- Make any necessary changes to the monitoring procedure to ensure that a sensitive data condition can always be satisfied.

See 'Supplementary guidance', page 72, for conditions to be satisfied.

2.5.2 Only use information that identifies individual workers where this is necessary to carry out meaningful equal opportunities monitoring. Where practicable, keep the information collected in an anonymised form.

Key points and possible actions

- Review current practices. Check whether any monitoring form gives the impression that information is anonymous, when in fact, it can be traced back to individuals.
- If identifiable information is held but it can be anonymised, do this.
- When there is no reasonable alternative but to be able to identify individuals, check whether the monitoring form states this and explains how the information is to be used.
- Ensure that identifiable information collected for equal opportunities monitoring is not used for any other purposes.
- Make any necessary changes to procedures and ensure that staff involved in monitoring understand why these changes have been made.

2.5.3 Ensure questions are designed so that the personal information collected through them is accurate and not excessive.

Key points and possible actions

- Check that questions allow people to identify themselves accurately. For example, in ethnic origin monitoring, do not limit the range of choices given so that workers are forced to make a choice that does not properly describe them.
- If you assign workers to categories ensure the record is clear that it is your assumption and not a matter of fact.

2.6 Marketing

2.6.1 Inform new workers if your organisation intends to use their personal information to deliver advertising or marketing messages to them. Give workers a clear opportunity to object (an 'opt-out') and respect any objections whenever received.

Key points and possible actions

- Review whether your business markets its, or anyone else's, products or services to current or former workers.
- Ensure that any new worker who will receive marketing information from your company has been informed that this will happen.
- Ensure that a clear procedure for 'opting-out' is made known to all workers.

2.6.2 Do not disclose workers' details to other organisations for their marketing unless individual workers have positively and freely indicated their agreement (an 'opt-in').

Key points and possible actions

- Review whether your business discloses workers' details. If so, put in place a procedure to ensure that a worker's details are not passed on until you have received a positive indication of agreement from him or her.

2.6.3 If you intend to use details of existing workers for marketing for the first time either in ways that were not explained when they first joined or that they would not expect, do not proceed until individual workers have positively and freely indicated their agreement (an 'opt-in').

Key points and possible actions

- When considering this type of campaign, construct an approval form to send to workers. Only direct material to those workers who have given a positive indication of agreement.
- Enclosing details of particular offers within a communication that workers will receive anyway, for example in a pay-slip, is acceptable as long as the offer includes an explanation of how to object.

2.7 Fraud detection

Public sector employers, in particular, use workers' records in the prevention and detection of fraud, for example, in order to check that they are not paying state benefits to those who by virtue of their employment are not entitled to receive them. Such exercises involve the electronic comparison of data sets held for different purposes in order to identify inconsistencies or discrepancies which may indicate fraud. This is known as data matching.

2.7.1 Consult workers, and/or trade unions or other representatives before starting a data matching exercise.

Key points and possible actions

- Inform trade unions and other workers' representatives of any proposed data matching exercise.
- Discuss how the plan will work in detail and take account of legitimate concerns raised before starting the exercise.

2.7.2 Inform new workers of the use of payroll or other information in fraud prevention exercises and remind them of this periodically.

Key points and possible actions

- Explain how fraud prevention exercises operate to new workers as part of information given about data protection.
- Set up regular reminders to workers on how the data matching exercise works – e.g. prior to the start of each new exercise.

2.7.3 Do not disclose worker information to other organisations for the prevention or detection of fraud unless:

- you are required by law to make the disclosure, or
- you believe that failure to disclose, in a particular instance, is likely to prejudice the prevention or detection of crime, or
- the disclosure is provided for in workers' contracts of employment.

Key points and possible actions

- Ensure staff who would be approached by outside agencies for this type of information, understand the rules of disclosure.

2.8 Workers' access to information about themselves

Workers, like any other individuals, have a right to gain access to information that is kept about them. This right is known as subject access.

2.8.1 Establish a system that enables your organisation to recognise a subject access request and to locate all the information about a worker in order to be able to respond promptly and in any case within 40 calendar days of receiving a request.

Key points and possible actions

- Assess what personal information about workers is in existence and who is responsible for it **(See recommendation 0.3, page 12)**
- Ensure that the information is accessible.
- Establish who in the organisation is responsible for responding to subject access requests.
- Ensure that all workers who are likely to receive subject access requests can recognise them and know who to pass them to.
- Have a checklist in place listing all places where personal information might be held that should be checked.
- Use the checklist to gather all personal information in time to enable a response within 40 days.

2.8.2 Check the identity of anyone making a subject access request to ensure information is only given to the person entitled to it.

Key points and possible actions

- In smaller organisations where workers make access requests in person, identity checks may not be necessary, but in large organisations it should not simply be assumed all requests are genuine.
- Brief anyone responsible for responding to a subject access request on how to check the identity of the person making it.

2.8.3 Provide the worker with a hard copy of the information kept, making clear any codes used and the sources of the information.

Key points and possible actions

- In the checklist used to gather all personal information include a check to ensure that the information supplied is intelligible, that it includes sources and that if at all possible it is in hard copy form.
- Although a hard copy of the subject access information does not have to be provided if this would involve "disproportionate effort" some form of access to the information still has to be given.

2.8.4 Make a judgement as to what information it is reasonable to withhold concerning the identities of third parties.

Key points and possible actions

- Information released to a worker could include information that enables a third party such as another worker to be identified. The employer has to balance the worker's right to know against an expectation of privacy that the third party might have.
- You can use the guidance on Access when Information about Third Parties is involved on **page 40 of the 'Supplementary guidance'** to help you make the necessary judgement.
- Brief those handling subject access requests on how to make decisions concerning third party information.

2.8.5 Inform managers and other relevant people in the organisation of the nature of information that will be released to individuals who make subject access requests.

Key points and possible actions

- Managers should be made aware of the extent to which information relating to them might be released to workers.
- If managers and others are aware of the extent and nature of the information that an individual could gain access to it should encourage them to record only what is truly relevant and useful.

2.8.6 Ensure that on request, promptly and in any event within 40 calendar days, workers are provided with a statement of how any automated decision-making process, to which they are subject, is used, and how it works.

Key points and possible actions

- Determine whether your organisation has any automated systems which are used as the sole basis for decision-making, for example during short-listing.
- If so, document how the system works and the basis of its decisions.
- Make this information available to those who are responsible for responding to requests about the process and make sure that they are aware of the requirement to respond within 40 calendar days.

2.8.7 When purchasing a computerised system ensure that the system enables you to retrieve all the information relating to an individual worker without difficulty.

Key points and possible actions

- Ensure that the supplier of a system that you will use to take automated decisions about workers provides the information needed to enable you to respond fully to requests for information about how the system works.
- Put in place arrangements to ensure that when systems are updated or new systems purchased they facilitate responses to subject access requests.

2.9 References

The provision of a reference about a worker from one party, such as a present employer, to another, such as a prospective employer, will generally involve the disclosure of personal data. This sub section of the code applies not only to references given to prospective employers, but also references given in other circumstances, for example character references given in connection with legal proceedings or financial references given in connection with a worker's application for a mortgage.

References given:

2.9.1 Set out a clear company policy stating who can give corporate references, in what circumstances, and the policy that applies to the granting of access to them. Make anyone who is likely to become a referee aware of this policy.

Key points and possible actions

- Determine who is allowed to give corporate references, this may, for example, be done by grade. Check whether your organisation distinguishes between corporate and personal references. If not, consider doing so.
- Draw up a policy explaining how reference requests should be handled, outlining the types of information that can be provided and the extent to which workers are given access. Ensure the policy is brought to the attention of anyone who is likely to receive a reference request.

2.9.2 Do not provide confidential references about a worker unless you are sure that this is the worker's wish.

Key points and possible actions

- As part of the policy, include a requirement that all those giving corporate references must be satisfied that the worker wishes the reference to be provided.
- As part of an Exit Policy, include on file a record of whether the worker wishes references to be provided after he/she has left.

References received:

2.9.3 When responding to a request from a worker to see his or her own reference and the reference enables a third party to be identified, make a judgement as to what information it is reasonable to withhold.

Key points and possible actions

- You can use the guidance on Access when Information about Third Parties is Involved on **page 40 of the 'Supplementary guidance'** to help you make this judgement.
- Brief those responsible for responding to requests for access to references received on how to make decisions concerning third party information.

2.10 Disclosure requests

This is concerned with requests for information about individual workers that come from outside the employer's organisation.

2.10.1 Establish a disclosure policy to tell staff who are likely to receive requests for information about workers how to respond, and to where they should refer requests that fall outside the policy rules.

Key points and possible actions

- Distribute information, based on this code, on how to handle disclosure requests and ensure that all those likely to handle such requests receive the information.
- Give examples of situations where a member of staff might need to refer a request to a higher authority within the organisation.
- Provide contact details of whom staff should contact, should they be unsure of how to deal with a disclosure request.

2.10.2 Ensure that disclosure decisions that are not covered by clear policy rules are only taken by staff who are familiar with the Act and this code, and who are able to give the decision proper consideration.

Key points and possible actions

- Determine who will be responsible for dealing with disclosure requests not covered by the policy.
- Organise any necessary training for those who will take on this role.

2.10.3 Unless you are under a legal obligation to do so, only disclose information about a worker where you conclude that in all the circumstances it is right to do so.

Key points and possible actions

- In some cases you will be under a legal obligation to disclose. Where this is the case you have no choice but to disclose. The Act does not stand in your way provided that you disclose no more than you are obliged to.
- In some cases you will not be under an obligation to disclose but you will be able to rely on an exemption in the Act if you choose to do so. This is most likely to arise in the case of criminal or tax investigations or where legal action is involved.
- Where you can relay on an exemption in the Act you still need to take care with the disclosure of confidential or sensitive information.
- In other cases you could breach the Act if you disclose. Only disclose, if in all the circumstances you are satisfied that it is fair to do so. Bear in mind that the duty of fairness is owed primarily to the worker. Where possible seek and take account of the workers' views.
- Only disclose confidential information if the worker has clearly agreed or you are satisfied that despite the duty of confidence the worker's interest or the wider public interest justifies disclosure.
- Ensure that if you intend to disclose sensitive personal data a sensitive data condition is satisfied.

2.10.4 Where a disclosure is requested in an emergency, make a careful decision as to whether to disclose, considering the nature of the information being requested and the likely impact on the individual of not providing it.

Key points and possible actions

- Make sure staff who are likely to receive such requests know whether they can handle them themselves or if not, who to refer them to. If they handle them themselves make them aware of their responsibility to assess the nature of the emergency and determine whether the request could be submitted in writing.

2.10.5 Make staff aware that those seeking information sometimes use deception to gain access to it. Ensure that they check the legitimacy of any request and the identity and authority of the person making it.

Key points and possible actions

- As part of the disclosure policy, make it a requirement that staff check the identity of any person making a request, the authority of the individual concerned and the basis for the request.
- Ensure that when a request is made on the basis of a stated legal obligation, that it is received in writing, spelling out the legal obligation on which it is based. If the stated legal obligation is in doubt check it against the law.

2.10.6 Where the disclosure involves a transfer of information about a worker to a country outside the European Economic Area (EEA), ensure that there is a proper legal basis for making the transfer.

Key points and possible actions

- The Act restricts the transfer of personal information outside the EEA.
- Review the Information Commissioner's guidance at www.ico.gov.uk, if you intend to pass workers' information outside the EEA.
- Keep a record of the legal basis on which you make the transfer.

2.10.7 Inform the worker before or as soon as is practicable after a request has been received that a non-regular disclosure is to be made, unless prevented by law from doing so, or unless this would constitute a "tip off" prejudicing a criminal or tax investigation.

Key points and possible actions

- For each non-regular disclosure, make a judgment as to whether the worker can be informed and whether a copy of the information can be provided to him or her. (A reminder of this could be placed in any system for handling non-regular disclosures.)
- In cases where the information can be provided to the worker do so as soon as possible.

2.10.8 Keep a record of non-regular disclosures. Regularly check and review this record to ensure that the requirements of the Act are being satisfied.

Key points and possible actions

- Set up a system for non-regular disclosures recording the details of the person who made the disclosure, the person who authorised it, the person requesting the disclosure, the reasons for the disclosure, the information disclosed and the date and time.
- Also set up a system to regularly check and review this record.

2.11 Publication and other disclosures

2.11.1 If publishing information about workers ensure that:

- there is a legal obligation to do so, or
- the information is clearly not intrusive, or
- the worker has consented to disclosure, or
- the information is in a form that does not identify individual workers.

Key points and possible actions

- An employer must balance the benefits of publishing information about workers with the reasonable expectations of its workers that their employer will respect the privacy of their personal information.
- Assess the current information published about named workers (e.g. in annual reports or on the website or in other publications) and the basis on which this takes place.
- Determine whether it is necessary to obtain consent from workers who are named and if so, set up an arrangement for obtaining consent from workers who are named in publications in the future.

2.11.2 Where information about workers is published on the basis of consent, ensure that when the worker gives consent he or she is made aware of the extent of information that will be published, how it will be published and the implications of this.

Key points and possible actions

- In any arrangement for obtaining consent for the publication of information on named workers, ensure that the worker is made aware of the full extent of any information to be published and where it is to be published. This is particularly important if information is to be published on the internet.

2.11.3 Personal information about workers should only be supplied to a trade union for its recruitment purposes if;

- the trade union is recognised by the employer,
- the information is limited to that necessary to enable a recruitment approach, and
- each worker has been previously told that this will happen and has been given a clear opportunity to object.

Key points and possible actions

- If your organisation has a recognised trade union that is requesting personal information about workers for a recruitment drive, inform all workers and give them an opportunity to object if they so wish.

2.11.4 Where staffing information is supplied to trade unions in the course of collective bargaining, ensure the information is such that individual workers cannot be identified.

Key points and possible actions

- Review your arrangements for the supply of information in connection with collective bargaining to ensure that in future all information on workers is supplied in an anonymised form.

2.12 Merger, acquisition, and business re-organisation

Business mergers and acquisitions will generally involve the disclosure of information about workers. This may take place during evaluation of assets and liabilities prior to the final merger or acquisition decision. Once a decision has been made disclosure is also likely to take place either in the run-up to or at the time of the actual merger or acquisition. A similar situation arises in business re-organisations that involve the transfer of workers' employment from one legal entity to another. This sub-section of the code will be relevant to such situations.

2.12.1 Ensure, wherever practicable, that information handed over to another organisation in connection with a prospective acquisition, merger or business re-organisation is anonymised.

Key points and possible actions

- Ensure that in any merger or acquisition situation, those responsible for negotiation are aware of the code, including its provisions on sensitive data.
- Assess any request for personal information from the other organisation. If at all possible, limit the information given to anonymised details.

2.12.2 Only hand over personal information prior to a final merger or acquisition decision after securing assurances that it will be used solely for the evaluation of assets and liabilities, it will be treated in confidence and will not be disclosed to other parties, and it will be destroyed or returned after use.

Key points and possible actions

- Remind those negotiating that they must receive strict assurances about how personal information will be used and what will happen to it should discussions end.
- Consider setting up a "data room" with accompanying rules of access.

2.12.3 Unless it is impractical to do so, tell workers if their employment records are to be disclosed to another organisation before an acquisition, merger or re-organisation takes place. If the acquisition, merger or re-organisation proceeds make sure workers are aware of the extent to which their records are to be transferred to the new employer.

Key points and possible actions

- In some circumstances "insider trading" or similar restrictions will apply. An example is where providing an explanation to workers would alert them to the possibility of a takeover of which they would otherwise be unaware and could thereby affect the price of a company's shares. The obligation to provide an explanation to workers is lifted in such circumstances.

2.12.4 Where a merger, acquisition or re-organisation involves a transfer of information about a worker to a country outside the European Economic Area (EEA) ensure that there is a proper basis for making the transfer.

Key points and possible actions

- Review the Information Commissioner's guidance at www.ico.gov.uk if you intend to pass workers' information outside the EEA.
- Check that there is a legal basis for the transfer that you intend to make.

2.12.5 New employers should ensure that the records they hold as a result of a merger, acquisition or re-organisation do not include excessive information, and are accurate and relevant.

Key points and possible actions

- Remember that a new employer's use of workers' information acquired as the result of a merger, acquisition or re-organisation is constrained by the expectations the workers will have from their former employer's use of information.
- When taking over an organisation assess what personal information you now hold as outlined in 0.3 and 0.4 **(see page 12)**.

2.13 Discipline, grievance and dismissal

2.13.1 Remember that the Data Protection Act applies to personal information processed in relation to discipline, grievance and dismissal proceedings.

Key points and possible actions

- Assess your organisation's disciplinary procedures and grievance procedures. Consider whether they need to be amended in the light of the code.
- Ensure that managers are aware that subject access rights apply even if responding to a request might impact on a disciplinary or grievance investigation or on forthcoming proceedings, unless responding would be likely to prejudice a criminal investigation.
- Ensure that those involved in investigating disciplinary matters or grievances are aware that they must not gather information by deception.
- Ensure that records used in the course of proceedings are of good enough quality to support any conclusion drawn from them.
- Ensure that all records are kept securely.
- Check that unsubstantiated allegations have been removed unless there are exceptional reasons for retaining some record.

2.13.2 Do not access or use information you keep about workers merely because it might have some relevance to a disciplinary or grievance investigation if access or use would be either:

- incompatible with the purpose(s) you obtained the information for, or
- disproportionate to the seriousness of the matter under investigation.

Key points and possible actions

- Make those in the organisation who are likely to carry out investigations aware that they do not have an unrestricted right of access to all information held about workers under investigation.
- Put in place a system to ensure that decisions on whether access is justified take into account the provisions of this code and the Act.

2.13.3 Ensure that there are clear procedures on how "spent" disciplinary warnings are handled.

Key points and possible actions

- Determine what is meant by a "spent" warning in your organisation. Assess the disciplinary procedure and decide whether it needs to be amended to clarify what happens once a warning period has expired.
- Set up a diary system, either manual or computerised, to remove spent warnings from individual's records, if this is a requirement of your procedure.

2.13.4 Ensure that when employment is terminated the reason for this is accurately recorded, and that the record reflects properly what the worker has been told about the termination.

Key points and possible actions

- Ensure that if a worker has resigned, even if asked to do so, that this is recorded on his or her record, as "resigned" rather than "dismissed".

2.14 Outsourcing data processing

Frequently, organisations do not process all the information they hold on workers themselves but outsource this to other organisations. Such organisations are termed 'data processors' in the Data Protection Act.

2.14.1 Satisfy yourself that any data processor you choose adopts appropriate security measures both in terms of the technology it uses and how it is managed.

Key points and possible actions

- Check whether the data processor has in place appropriate security measures. Is it, for example, certified to BS7799?
- Check that the processor actually puts their security measures into practice.

2.14.2 Have in place a written contract with any data processor you choose that requires it to process personal information only on your instructions, and to maintain appropriate security.

Key points and possible actions

- If there is no contract, put one in place.
- Check that any contract you have with a data processor includes clauses ensuring proper data security measures.

2.14.3 Where the use of a data processor would involve a transfer of information about a worker to a country outside the European Economic Area (EEA), ensure that there is a proper basis for making the transfer.

Key points and possible actions

- Review the Information Commissioner guidelines at www.ico.gov.uk if you intend to pass workers' information outside the EEA.
- Check that there is a legal basis for the transfer that you intend to make.

2.15 Retention of records

See Part 1: Recruitment and selection for specific recommendations on retention of recruitment records.

2.15.1 Establish and adhere to standard retention times for the various categories of information to be held on the records of workers and former workers. Base the retention times on business need taking into account relevant professional guidelines.

Key points and possible actions

- Remember that the Act does not override any statutory requirement to retain records, for example, in relation to income tax or certain aspects of health and safety.
- Only retain information on records that is still needed; eliminate personal information that is no longer of any relevance, once the employment relationship has ended.
- As far as possible set standard retention times for categories of information held in employment records. Consider basing these on a risk analysis approach.

- Assess who in your organisation retains employment records **(see 0.3 on page 12)**. Make sure no one retains information beyond the standard retention times unless there is a sound business reason for doing so.
- If possible, set up a computerised system which flags information retained for more than a certain time as due for review or deletion.

2.15.2 Anonymise any information about workers and former workers where practicable.

Key points and possible actions

- Where statistical information only is required, anonymised records should be sufficient.

2.15.3 If the holding of any information on criminal convictions of workers is justified, ensure that the information is deleted once the conviction is 'spent' under the Rehabilitation of Offenders Act.

Key points and possible actions

- Use a computerised or manual system to ensure spent convictions are deleted from the system.
- Identify if your organisation may be justified in making exceptions to this, for example, certain convictions held in connection with workers who work with children.

2.15.4 Ensure that records which are to be disposed of are securely and effectively destroyed.

Key points and possible actions

- Review arrangements for dealing with old records to ensure they are securely disposed of and advise anyone holding employment records of these arrangements for disposal.
- Do not assume that pressing the "delete" key on a computer based system necessarily removes a record completely from the system. Check that computer records that are to be deleted are in practice removed completely.
- Make sure that computer equipment that has held employment records is never sold on unless you are sure the records have been fully removed.

Part 3: Monitoring at work

About Part 3 of the code

Data protection and monitoring at work

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

How does the Data Protection Act regulate monitoring?

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

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

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

What does this part of the code cover?

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

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

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

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

Examples of monitoring

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

- gathering information through point of sale terminals, to check the efficiency of individual supermarket check-out operators
- recording the activities of workers by means of CCTV cameras, either so that the recordings can be viewed routinely to ensure that health and safety rules are being complied with, or so that they are available to check on workers in the event of a health and safety breach coming to light
- randomly opening up individual workers' e-mails or listening to their voice-mails to look for evidence of malpractice
- using automated checking software to collect information about workers, for example to find out whether particular workers are sending or receiving inappropriate e-mails

- examining logs of websites visited to check that individual workers are not downloading pornography
- keeping recordings of telephone calls made to or from a call centre, either to listen to as part of workers training, or simply to have a record to refer to in the event of a customer complaint about a worker
- systematically checking logs of telephone numbers called to detect use of premium-rate lines
- videoing workers outside the workplace, to collect evidence that they are not in fact sick
- obtaining information through credit reference agencies to check that workers are not in financial difficulties.

Outside this part of the code

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

See Part 2: Employment records, page 54, for guidance relating to grievance and disciplinary investigations.

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

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

Impact assessments

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

In all but the most straightforward cases, employers are likely to find it helpful to carry out a formal or informal 'impact assessment' to decide if and how to carry out monitoring. This is the means by which employers can judge whether a monitoring arrangement is a proportionate response to the problem it seeks to address. This code does not prejudge the outcome of the impact assessment. Each will necessarily depend on the particular circumstances of the employer. Nor does the code attempt to set out for employers the benefits they might gain from monitoring. What it does do is assist employers in identifying and giving appropriate weight to the other factors they should take into account.

An impact assessment involves

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

Adverse impact

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

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

- what impact, if any, will there be on individuals with professional obligations of confidentiality or secrecy, e.g. solicitors or doctors?
- whether the monitoring will be oppressive or demeaning.

Alternatives

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

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

Obligations

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

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

See Part 2 – Employment records, page 34, for more information on security requirements.

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

See Part 2 – Employment records, page 43, which explains more about rights to access.

Is monitoring justified?

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

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

See 'Supplementary guidance', page 57, for a chart to help assess the degree of intrusiveness involved in monitoring the content of various types of communication

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

Is a worker's consent needed?

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

Are there special rules for electronic communications?

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

See 'Supplementary guidance', page 58, for more details on The Lawful Business Practice Regulations.

Good practice recommendations – Part 3

The parts of the code in this section are:

3.1 The general approach to monitoring

Core principles

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

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

Key points and possible actions

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

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

Key points and possible actions

- Identify the monitoring that currently takes place in your organisation.
- Identify any monitoring that you plan to implement.
- Consider conducting an impact assessment on either current or planned monitoring based on the guidance on page 60.

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

Key points and possible actions

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

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

Key points and possible actions

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

3.1.5 If sensitive information is collected in the course of monitoring, ensure that a sensitive data condition is satisfied.

Key points and possible actions

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

See 'Supplementary guidance', page 72, which explains more about the conditions for processing sensitive data.

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

Key points and possible actions

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

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

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

3.2 Monitoring electronic communications

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

3.2.1 If you wish to monitor electronic communications, establish a policy on their use and communicate it to workers – see 'Policy for the use of electronic communications' below.

Key points and possible actions

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

Policy for the use of electronic communications

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

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

- Lay down clear rules for private use of the employer's communication equipment when used from home or away from the workplace, e.g. the use of facilities that enable external dialling into company networks.
- Explain the purposes for which any monitoring is conducted, the extent of the monitoring and the means used.
- Outline how the policy is enforced and penalties which exist for a breach of policy.

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

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

Key points and possible actions

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

See 'Supplementary guidance', page 58, for more information about the Lawful Business Practice Regulations.

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

3.3. Video and audio monitoring

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

See www.ico.gov.uk and search for the CCTV code of practice.

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

3.4. Covert monitoring

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

3.5 In-vehicle monitoring

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

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

Key points and possible actions

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

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

Key points and possible actions

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

3.6 Monitoring through information from third parties

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

See Part 1 – Recruitment and selection, page 14, for more information about the Criminal Records Bureau.

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

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

3.6.4 Take particular care with information about workers which you have as a result of a nonemployment relationship with them.

Key points and possible actions

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

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

Key points and possible actions

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

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

Key points and possible actions

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

4 Part 4: Information about workers' health

About Part 4 of the code

Data protection and information about workers' health

The Data Protection Act's sensitive data rules come into play whenever an employer wishes to process information about workers' health. These rules do not prevent the processing of such information but limit the circumstances in which it can take place. The processing must also be consistent with the other requirements of the Act. Employers, especially in the public sector, need to bear in mind Article 8 of the European Convention on Human Rights which creates a right to respect for private and family life.

What does this part of the code cover?

This part of the code addresses the collection and subsequent use of information about a worker's physical or mental health or condition. Collection will often be done by some form of medical examination or test, but may involve other means such as health questionnaires.

The issues addressed in this part of the code will arise typically from the carrying out of medical examination and testing or from the operation of an occupational health scheme. This part of the code is therefore most likely to be of relevance to larger organisations and those with specific health and safety obligations.

Examples of information about workers' health

This part of the code applies to information such as:

- a questionnaire completed by workers to detect problems with their health
- information about a worker's disabilities or special needs
- the results of an eye-test taken by a worker using display screens
- records of blood tests carried out to ensure a worker has not been exposed to hazardous substances
- the results of a test carried out to check a worker's exposure to alcohol or drugs
- the results of genetic tests carried out on workers

- an assessment of fitness for work to determine entitlement to benefits or suitability for continued employment
- records of vaccination and immunisation status and history.

Outside the code

The Data Protection Act only comes into play when personal information is or will be held electronically or recorded in a structured filing system. This will often be the case but sometimes it may not, for example where a line-manager enquires about a worker's health but does not keep, or intend to keep, any record of the conversation, or only keeps a note in a general notebook.

Where samples are taken, as might be the case with drug or alcohol testing, the code only applies from the point at which samples yield personal information about a worker. This code does not address consent for any physical intervention involved in taking a sample from a worker in the course of medical testing.

Sensitive data rules

Where information about workers' health is to be processed, one of the Act's sensitive data conditions must be satisfied. There are various conditions. Below we have listed the ones likely to be of most relevance to employers. Employers holding information about workers' health ought to be able to answer 'yes' to one or more of these questions:

- Is the processing necessary to enable the employer to meet its legal obligations, for example to ensure health and safety at work, or to comply with the requirement not to discriminate against workers on the grounds of sex, age, race or disability?
- Is the processing for medical purposes, e.g. the provision of care or treatment, and undertaken by a health professional or someone working under an equivalent duty of confidentiality, e.g. an occupational health doctor?
- Is the processing in connection with actual or prospective legal proceedings?
- Has the worker given consent explicitly to the processing of his or her medical information?

This is not an exhaustive list of all the conditions.

See 'Supplementary guidance', page 72, for more information on these and other sensitive data conditions.

Relying on the worker's consent

There are limitations as to how far consent can be relied on as a basis for the processing of information about workers' health. To be valid, consent must be:

- **explicit**. This means the worker must have been told clearly what personal data are involved and have been properly informed about the use that will be made of them. The worker must have given a positive indication of agreement, e.g. a signature.
- **freely given**. This means the worker must have a real choice whether or not to consent and there must be no penalty imposed for refusing to give consent.

See 'Supplementary guidance', page 75, for further explanation of what this means in practice.

Impact assessments

Once a sensitive data condition is satisfied, an employer then needs to be clear that either:

- it is under a legal duty to process information about workers' health, e.g. the duty to monitor workers' possible exposure to hazardous materials under the Control of Substances Hazardous to Health Regulations 2002, or
- the benefits gained from processing information about workers' health justify the privacy intrusion or any other adverse impact on them. In other words, the collection and use of information about workers' health must be a proportionate response to a particular problem.

An 'impact assessment' is a useful tool for employers to use to help them to judge whether the second of the above options applies.

Particularly where medical testing is involved, employers are likely to find it helpful to carry out a formal or informal 'impact assessment' to decide how or whether to collect information about workers' health. This code does not prejudge the outcome of the impact assessment. Each will necessarily depend on the particular circumstances of the employer. Nor does the code attempt to set out for employers the benefits they might gain from holding information about workers' health. What it does do is assist employers in identifying and giving appropriate weight to the other factors they should take into account.

An impact assessment involves

- identifying clearly the **purpose(s)** for which health information is to be collected and held and the benefits this is likely to deliver
- identifying any likely **adverse impact** of collecting and holding the information
- considering **alternatives** to collecting and holding such information
- taking into account the **obligations** that arise from collecting and holding health information
- judging whether collecting and holding health information is **justified**.

Purpose(s)

It is important that a realistic assessment is made of the extent to which the collection of health information will actually address the risks it is directed at. Decisions based on, for example, the effect of particular medical conditions on a worker's future employability or the effect of particular drugs on safety should be based on relevant and reputable scientific evidence.

Adverse impact

Identifying any likely adverse impact means taking into account the consequences of collecting and holding health information, not only for workers, but also for others who might be affected by it, such as a worker's family. Consider:

- how extensive will the intrusion into the private lives of workers and others be as a result of collecting information about their health?
- whether health information will be seen by those who do not have a business need to know, e.g. IT workers involved in maintaining electronic files about workers
- what impact, if any, will the collection of health information have on the relationship of mutual trust and confidence that should exist between workers and their employer?
- whether the collection of health information will be oppressive or demeaning.

Alternatives

Considering whether it is necessary to collect information about workers' health, and if so how to do this in the least intrusive manner, means asking questions such as:

- can health questionnaires rather than tests be used to obtain the information the employer requires?
- can changes in the workplace, for example eliminating exposure to a hazardous substance, remove the need to obtain information through testing?
- can medical testing be targeted at individuals who have exhibited behavioural problems that may be drink or drug related, rather than at all workers?
- can the collection of health information be confined to areas of highest risk, e.g. can it be directed at a few individuals the nature of whose jobs mean they pose a particular risk rather than at everyone?
- can medical testing be designed to reveal only a narrow range of information that is directly relevant to the purpose for which it is undertaken?
- can access to health information be limited so that it will only be seen by medically qualified staff or those working under specific confidentiality agreements?

Obligations

Taking into account the obligations that arise from collecting information about workers' health means considering such matters as:

- whether and how workers will be notified about the collection of their health information
- how information about workers' health will be kept securely and handled in accordance with the Act.

See Part 2 – Employment records, page 34, for more information on security requirements.

- the implications of the rights that individuals have to obtain a copy of information that has been collected about their health.

See Part 2 – Employment records, page 43, which explains more about rights to access.

Is health information justified?

Making a conscious decision as to whether the current or proposed collection and use of health information is justified involves:

- establishing the benefits the collection and use of health information will bring
- considering any alternative method of obtaining these benefits and/or the information needed
- weighing these benefits against the adverse impact
- placing particular emphasis on the need to be fair to individual workers
- ensuring that the intrusion is no more than absolutely necessary
- bearing in mind that health information can be particularly sensitive, that its obtaining can be particularly intrusive and that significant intrusion will not normally be justified unless the employer's business is at real risk of serious damage
- taking into account the results of consultation with trade unions or other representatives, if any, or with workers themselves.

Making an impact assessment need not be a complicated or onerous process. Even in the context of health information it may sometimes be enough for an employer to make a simple mental evaluation of the risks faced by his or her business and to assess whether the collection and use of information about workers' health would reduce or eradicate those risks or would bring particular benefits. In other cases the impact assessment will be more complicated, for example where an employer faces a number of different risks of varying degrees of seriousness. In such cases appropriate documentation would be advisable.

Good practice recommendations – Part 4

The parts of the code in this section are:

4.1 Information about workers' health: general considerations

4.2 Occupational health schemes

4.3 Information from medical examination and testing

4.4 Information from drug & alcohol testing

4.5 Information from genetic testing

Sickness and Injury records are dealt with in Part 2 of the code. See page 36.

4.1 Information about workers' health: general considerations

Core principles

- It will be intrusive and may be highly intrusive to obtain information about your workers' health.
- Workers have legitimate expectations that they can keep their personal health information private and that employers will respect their privacy.
- If employers wish to collect and hold information on their workers' health, they should be clear about the purpose and satisfied that this is justified by real benefits that will be delivered.
- One of the sensitive data conditions must be satisfied.
- Workers should be aware of the extent to which information about their health is held and the reasons for which it is held.
- Decisions on a worker's suitability for particular work are properly management decisions but the interpretation of medical information should be left to a suitably qualified health professional.

4.1.1 Identify who within the organisation can authorise or carry out the collection of information about workers' health on behalf of the organisation and ensure they are aware of their employer's responsibilities under the Act.

Key points and possible actions

- Those who handle information about workers' health, or who can authorise the collection of such information, should be briefed on the Act and this code.
- There are non-compliance risks if those lacking proper authority and any necessary training introduce the collection of health information and in particular medical testing.
- Leave the interpretation of medical information to those who are qualified to do this.

4.1.2 If health information is to be collected ensure a sensitive data condition can be satisfied.

Key points and possible actions

- The collection and use of information about workers' health is against the law unless a sensitive data condition is satisfied.
- In general employers should only collect health information where this is necessary for the protection of health and safety, to prevent discrimination on the grounds of disability, to satisfy other legal obligations or if each worker affected has given his or her explicit consent.
- If consent is to be relied on, it must be freely given. That means a worker must be able to say 'no' without penalty and must be able to withdraw consent once given. Blanket consent obtained at the outset of employment cannot always be relied on.
- Consent should not be confined to the testing itself, it should also cover the subsequent recording, use and disclosure of the test results.

See 'Supplementary guidance', page 72, which explains more about the conditions for processing sensitive data.

4.1.3 Identify clearly the purposes behind the collection of information about workers' health and the specific business benefits which it is likely to bring.

Key points and possible actions

- Identify the collection and use of information about workers' health that currently takes place in your organisation.
- Identify any collection or use of information about workers' health that you plan to implement.
- Consider conducting an impact assessment on current or planned collection and use of health information.

See page 81 for information on how to carry out an impact assessment.

4.1.4 Protect information about workers' health with appropriate security measures. Ensure that wherever practicable only suitably qualified health professionals have access to medical details.

Key points and possible actions

- Managers should not have access to more information about a worker's health than is necessary for them to carry out their management responsibilities. As far as possible the information should be confined to that necessary to establish fitness to work, rather than consist of more general medical details.
- Safety representatives should be provided with anonymised information unless any workers concerned have consented to the provision of information in an identifiable form.
- Unless the general standard of information security in your organisation is sufficiently high, medical information about workers should be separated from other personnel information, for example by keeping it in a sealed envelope, or subject to additional access controls on an electronic system.
- Information about workers' health collected to run a pension or insurance scheme should not be available to the employer unless this is necessary for the employer's role in administering the scheme.

4.1.5 Do not collect more information about workers' health than is necessary for the purpose(s) behind its collection.

Key points and possible actions

- Review any health questionnaires to ensure that only information that is really needed is collected.
- If commissioning a medical report on a sick employee, seek information on the worker's fitness for continued employment rather than medical details.
- Do not ask workers to consent to the disclosure of their entire general practitioner record as a matter of expediency. Only seek the disclosure of the whole record, or substantial parts of it, where this is genuinely necessary.
- If seeking a report from a worker's general practitioner or other medical practitioner who has been responsible for the care of the worker, ensure that you meet the requirements of the Access to Medical Reports Act 1988. This includes obtaining the worker's consent to your application for a report.

4.2 Occupational health schemes

This sub-section gives good practice recommendations for employers with occupational health schemes. It does not provide detailed professional guidance to doctors, nurses and others involved in such schemes.

4.2.1 Ensure workers are aware of how information about their health will be used and who will have access to it.

Key points and possible actions

- Unless told otherwise workers are entitled to assume that information they give to a doctor, nurse or other health professional will be treated in confidence and not passed to others.
- Set out clearly to workers, preferably in writing, how information they supply in the context of an occupational health scheme will be used, who it might be made available to and why.

4.2.2 Do not compromise any confidentiality of communications between workers and health professionals in an occupational health service.

Key points and possible actions

- If workers are allowed to use telephone or e-mail for confidential communication with their occupational health service, do not compromise this confidentiality by monitoring the contents of these communications.

4.2.3 Act in a way that is consistent with the Guidance on Ethics for Occupational Physicians published by the Faculty of Occupational Medicine.

Key points and possible actions

- Although this is guidance for occupational physicians rather than employers, it should give you a clear understanding of the legal and ethical constraints that apply to the exchange of information when working with occupational health professionals.

4.3 Information from medical examination and testing

This sub-section gives good practice recommendations specific to the collection and handling of information derived from medical examination and testing. The general recommendations in section 4.1 should also be taken into account.

Employers should bear in mind that obtaining a worker's consent or satisfying another sensitive data condition is not, on its own, sufficient to ensure data protection compliance. There is still an obligation to ensure that information obtained through medical examination is relevant, is accurate, is up to date and is kept secure.

See 'Supplementary guidance', page 72, for more Information on the Sensitive Data Conditions.

4.3.1 Where information obtained from medical testing is used to enforce the organisation's rules and standards make sure that the rules and standards are clearly set out in a policy which workers are aware of.

Key points and possible actions

- Ensure workers understand these rules and standards.
- Set out the circumstances in which medical testing may take place, the nature of the testing, how information obtained through testing will be used, and the safeguards that are in place for the workers that are subject to it.

4.3.2 Only obtain information through medical examination or testing of applicants or other potential workers at an appropriate point in the recruitment process, i.e. where there is a likelihood of appointing them. You must also be satisfied that the testing is a necessary and justified measure to:

- Determine whether the potential worker is fit or likely to remain fit to carry out the job in question, or
- Meet any legal requirements for testing, or
- Determine the terms on which a potential worker is eligible to join a pension or insurance scheme.

Key points and possible actions

- Record the business purpose for which examination or testing is to be introduced and the sensitive data condition that can be satisfied.
- Consider less intrusive ways of meeting the objectives, for example using a health questionnaire as an alternative to a medical examination or as a means to select those required to undergo a full examination.
- Only carry out a pre-employment medical examination or medical testing where there is a real likelihood that the individual will be appointed.
- Make it clear early on in the recruitment process that individuals may be subjected to medical examination or testing once there is a likelihood that they will be appointed.

4.3.3 Only obtain information through a medical examination or medical testing of current workers if the testing is part of a occupational health and safety programme that workers have a free choice to participate in, or you are satisfied that it is a necessary and justified measure to:

- Prevent a significant risk to the health and safety of the worker, or others, or
- Determine a particular worker's fitness for carrying out his or her job, or
- Determine whether a worker is fit to return to work after a period of sickness absence, or when this might be the case, or
- Determine the worker's entitlement to health related benefits e.g. sick pay, or
- Prevent discrimination against workers on the grounds of disability or assess the need to make reasonable adjustments to the working environment, or
- Comply with other legal obligations.

Key points and possible actions

- Record the business purpose for which the programme of examination or testing of workers is to be introduced and the sensitive data condition that can be satisfied.
- Establish and document who will be tested, what precisely are they being tested for, the frequency of testing, and the consequences of a positive or negative test.
- Consider less intrusive ways of meeting the employer's objectives, for example collecting information via a health questionnaire either as a first stage or as an alternative to a medical examination.

4.3.4 Do not obtain a sample covertly or use an existing sample, test result or other information obtained through a medical examination for a purpose other than that for which it was originally obtained.

Key points and possible actions

- Be clear about the purpose(s) for which any testing is being carried out and communicate this to workers.
- The covert obtaining of bodily samples for testing is most unlikely ever to be justified.
- If there is a wish to carry out a different test on an existing sample, this can only be done if the worker has been told about it and has freely consented.

4.3.5 Permanently delete information obtained in the course of medical examination or testing that is not relevant for the purpose(s) for which the examination or testing is undertaken.

Key points and possible actions

- Health information that is excessive, irrelevant or out of date should not be retained by an employer.
- If the retention of medical information is necessary only for the operation of an occupational health service, it should be kept in a confidential occupational health file.

4.4 Information from drug and alcohol testing

This part of the code gives good practice recommendations specific to the collection and handling of information derived from drug and alcohol testing. The recommendations in sub-sections 4.1 and 4.3 should also be taken into account.

4.4.1 Before obtaining information through drug or alcohol testing ensure that the benefits justify any adverse impact, unless the testing is required by law.

Key points and possible actions

- The collection of information through drug and alcohol testing is unlikely to be justified unless it is for health and safety reasons.
- Post-incident testing where there is a reasonable suspicion that drug or alcohol use is a factor is more likely to be justified than random testing.
- Given the intrusive nature of testing employers would be well advised to undertake and document an impact assessment.

See page 81 for information about how to carry out an impact assessment.

4.4.2 Minimise the amount of personal information obtained through drug and alcohol testing.

Key points and possible actions

- Only use drug or alcohol testing where it provides significantly better evidence of impairment than other less intrusive means.
- Use the least intrusive forms of testing practicable to deliver the benefits to the business that the testing is intended to bring.
- Tell workers what drugs they are being tested for.
- Base any testing on reliable scientific evidence of the effect of particular substances on workers.
- Limit testing to those substances and the extent of exposure that will have a significant bearing on the purpose(s) for which the testing is conducted.

4.4.3 Ensure the criteria used for selecting workers for testing are justified, properly documented, adhered to and are communicated to workers.

Key points and possible actions

- It is unfair and deceptive to lead workers to believe that testing is being carried out randomly if, in fact, other criteria are being used.
- If random testing is to be used, ensure that it is carried out in a genuinely random way.
- If other criteria are used to trigger testing, for example suspicion that a worker's performance is impaired as a result of drug or alcohol use, the employer should ensure workers are aware of the true criteria that are used.

4.4.4 Confine the obtaining of information through random testing to those workers who are employed to work in safety critical activities.

Key points and possible actions

- Collecting personal information by testing all workers in a business will not be justified if in fact it is only workers engaged in particular activities that pose a risk.
- Even in safety-critical businesses such as public transport or heavy industry, workers in different jobs will pose different safety risks. Therefore collecting information through the random testing of all workers will rarely be justified.

4.4.5 Gather information through testing designed to ensure safety at work rather than to reveal the illegal use of substances in a worker's private life.

Key points and possible actions

- Very few employers will be justified in testing to detect illegal use rather than on safety grounds. Testing to detect illegal use may, exceptionally, be justified where illegal use would:
  - breach the worker's contract of employment, conditions of employment or disciplinary rules, and
  - cause serious damage to the employer's business, e.g. by substantially undermining public confidence in the integrity of a law enforcement agency.

4.4.6 Ensure that workers are fully aware that drug or alcohol testing is taking place, and of the possible consequences of being tested.

Key points and possible actions

- Explain your drug or alcohol policy in a staff handbook.
- Explain the consequences for workers of breaching the policy.
- Ensure workers are aware of the blood-alcohol level at which they may be disciplined when being tested for alcohol.
- Do not conduct testing on samples collected without the worker's knowledge.

4.4.7 Ensure that information is only obtained through drug and alcohol testing that is;

- of sufficient technical quality to support any decisions or opinions that are derived from it and,
- subject to rigorous integrity and quality control procedures and,
- conducted under the direction of, and positive test results interpreted by, a person who is suitably qualified and competent in the field of drug testing.

Key points and possible actions

- Use a professional service with qualified staff and that meets appropriate standards.
- Ensure workers have access to a duplicate of any sample taken to enable them to have it independently analysed as a check on the accuracy of the employer's results.
- Do not assume that the tests are infallible and be prepared to deal properly with disputes arising from their use.

4.5 Information from genetic testing

Genetic testing has the potential to provide employers with information predictive of the likely future general health of workers or with information about their genetic susceptibility to occupational diseases. Genetic testing is, though, still under development and in most cases has an uncertain predictive value. It is rarely, if ever, used in the employment context. The Human Genetics Commission advises that employers should not demand that an individual take a genetic test as a condition of employment. It should therefore only be introduced after very careful consideration, if at all.
This sub-section supplements sub-sections 4.1 and 4.3.

4.5.1 Do not use genetic testing in an effort to obtain information that is predictive of a worker's future general health.

Key points and possible actions

- Obtaining information through genetic testing is too intrusive and the information's predictive value is insufficiently certain to be relied on to provide information about a worker's future health.

4.5.2 Do not insist that a worker discloses the results of a previous genetic test.

Key points and possible actions

- It is important that workers are not put off taking genetic tests that may be beneficial for their health care by the fear that they may have to disclose the results to a current or future employer.
- You can ask for information that is relevant to your health and safety or other legal duties but the provision of the information should be voluntary.

4.5.3 Only use genetic testing to obtain information where it is clear that a worker with a particular, detectable genetic condition is likely to pose a serious safety risk to others or where it is known that a specific working environment or practice might pose specific risks to workers with particular genetic variations.

Key points and possible actions

- Only seek information through genetic testing as a last resort, where:
  - it is not practicable to make changes to the working environment or practices so as to reduce risks to all workers, and
  - it is the only reasonable method to obtain the required information.
- Inform the Human Genetics Commission of any proposals to use genetic testing for employment purposes.

4.5.4 If a genetic test is used to obtain information for employment purposes ensure that it is valid and is subject to assured levels of accuracy and reliability.

Key points and possible actions

- There should be scientific evidence that any genetic test is valid for the purpose for which it is used.
- Ensure the results of any test undertaken are always communicated to the person tested and professional advice is available.
- Ensure test results are carefully interpreted, taking account of how they might be affected by environmental conditions.

If you would like to contact us please call 0303 123 1113

www.ico.gov.uk

Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF

November 2011

ico.
Information Commissioner's Office

Upholding information rights