



CONTENTS

CONTENTS.....	1
Who is the Code for?	3
Why should you use it?	3
Other parts of the Code.....	3
Five sections.....	4
Our aim	4
SECTION 1: BACKGROUND INFORMATION	5
The Data Protection Act 1998: key questions	5
The Employment Practices Code: key questions	9
SECTION 2: THE CODE	13
The role of data protection in recruitment and selection	13
The Code at a glance.....	13
1 MANAGING DATA PROTECTION.....	14
The benchmarks	14
Notes and examples.....	15
2 ADVERTISING.....	16
The benchmarks	16
Notes and examples.....	17
3 APPLICATIONS.....	18
The benchmarks	18
Notes and examples.....	19
4 VERIFICATION.....	20
The benchmarks	20
Notes and examples.....	21
5 SHORT-LISTING	22
The benchmarks	22
Notes and examples.....	23
6 INTERVIEWS	24
The benchmark	24
Notes and examples.....	25

7 PRE-EMPLOYMENT VETTING	26
The benchmarks	26
Notes and examples	27
8 RETENTION OF RECRUITMENT RECORDS	28
The benchmarks	28
Notes and examples	29
SECTION 3: FURTHER INFORMATION.....	30
Sensitive Personal Data	30
The Criminal Records Bureau	33
Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975.....	35
Useful addresses	36
SECTION 4: FREQUENTLY ASKED QUESTIONS.....	39
SECTION 5: CHECKLIST	42

ABOUT THE CODE

Who is the Code for?

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

Why should you use it?

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

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

What is the legal status of the Code?

The legal requirement on employers is to comply with the Act itself. The benchmarks in the Code are however designed to bring about compliance with the Act. They develop and apply the Act in the context of employment practices. They are the Information Commissioner's recommendations as to how the legal requirements of the Act can be met. Employers may have alternative ways of meeting these requirements but if they do nothing they risk breaking the law.

Any enforcement action would be based on a failure to meet the requirements of the Act itself. However;

- relevant benchmarks in the Code would be cited by the Commissioner in connection with any enforcement action that arises in relation to the processing of personal data in employment
- disregard for the data protection requirements that particular benchmarks are designed to help organisations meet is likely to mean that an employer will not comply with the Act.

Other parts of the Code

The Employment Practices Data Protection Code has three additional parts,

- **employment records** – is about collecting, storing, disclosing and deleting records

- **monitoring at work** – is about monitoring workers’ use of telephone or email systems and vehicles
- **medical information** – is about occupational health, medical testing, drug and genetic screening

Each part of the Code has been designed to stand alone and therefore much of the background information is the same. Which parts of the code you choose to use will depend on the relevance to your organisation of each area covered.



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

See Useful Addresses page 36 for contact details or contact the website www.dataprotection.gov.uk

Five sections

This booklet is divided into five sections

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

Throughout this booklet you will see signposts:



These indicate where you can go to get further information on certain subjects.

Our aim

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

SECTION 1: BACKGROUND INFORMATION

The Data Protection Act 1998: key questions

What does the Data Protection Act 1998 cover?

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

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

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

What are the responsibilities of data controllers under the Act?

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



Access the website www.dpr.gov.uk or contact the Information Commissioner for a copy of the *Notification Handbook* to find out more about notification and exemptions. See Useful Addresses page 36 for contact details.

What are the data protection principles?

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

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

6. processed in line with data subjects' rights
7. secure
8. not transferred to countries that don't protect personal data adequately.

What are the rights of data subjects under the Act?

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

Are there any exemptions from the Act?

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

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

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



Benchmark 1 page 14 explains more about allocating responsibility.

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

Enforcement

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

Prosecution

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

Assessment of Processing

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

Compensation

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

What is the role of the Information Commissioner?

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



See Useful Addresses page 36 for contact details.

Where can our organisation find out more about the Act?

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



See Useful Addresses page 36 for contact details.

The Employment Practices Code: key questions

What is this Code of Practice for?

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

Who does data protection cover in the workplace?

The Code is concerned with data that employers might collect and keep on any individual who might wish to work, work, or have worked for them. In the Code the term "workers" is used to cover all these individuals. As such it includes;

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

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

What data are covered by the Code?

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

Personal data

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

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

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

Processing

The Act applies to personal data that are subject to 'processing'. For the purposes of the Act, the term 'processing' applies to a comprehensive range of activities. It includes the initial obtaining of personal data, their keeping and use, accessing and disclosing them through to their final destruction.

Examples of personal data likely to be covered by the Act

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

Examples of information unlikely to be covered by the Act

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

In practice, therefore, nearly all useable information held about individual workers will be covered by the Code.

What are sensitive personal data?

The Act sets out a series of conditions, at least one of which has to be met before an employer can collect, store, use, disclose or otherwise process sensitive personal data. Sensitive data are information concerning an individual's

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,

- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- physical or mental health or condition,
- sexual life,
- commission or alleged commission of any offence, or
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

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

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

In the context of recruitment and selection typical circumstances in which sensitive personal data might be held include:-

- relevant criminal convictions to assess suitability for certain types of employment
- disabilities to ensure special needs are catered for at interview or selection testing
- racial origin to ensure recruitment processes do not discriminate against particular racial groups.



See *Further Information* Page 30 which explains more about the conditions for processing sensitive personal data.

What happens when a worker wishes to access information?

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

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

There are some exemptions that allow organisations to withhold information. These exemptions can apply in areas such as criminal investigation, management planning such as

promotion and transfer plans, and negotiations. The exemptions, though, are limited in their application even within these areas. Care must also be taken in deciding whether or not to release information identifying 'third parties' i.e. people, other than the individual who has made the subject access request.



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

What are workers' responsibilities under the Act?

Workers do have some responsibilities for data protection under the Act. Line managers have responsibility for the type of personal data they collect and how they use them. No workers should disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes. A worker disclosing personal data without the authority of the organisation may commit a criminal offence, unless there is some other legal justification for example under 'whistle-blowing' legislation.

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



Benchmark 1 page 14 explains more about allocating responsibility.

SECTION 2: THE CODE

The role of data protection in recruitment and selection

The Act gives individuals certain rights in respect of the processing of personal data about them that takes place during the recruitment process. 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.

The Code at a glance

The benchmarks are designed to help businesses to achieve compliance with the Act. They develop and apply the Act in the context of recruitment practices. They are the Information Commissioner's recommendations as to how the legal requirements of the Act can be met.

In the following pages, the benchmarks are dealt with in detail, with notes and examples given as further explanation of each individual benchmark.

1 MANAGING DATA PROTECTION

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

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

The benchmarks



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



Access the website www.dpr.gov.uk where you can view the register or contact the Information Commissioner for a copy of the *Notification Handbook* to find out more about notification. See Useful Addresses page 36 for contact details.

Notes and examples

1. In a small business the responsibility might simply be with the owner of the business. Where there is a management structure responsibility should be allocated to a senior manager in the personnel or human resources function or someone in a comparable position. Those with overall responsibility must be in a position to feed their knowledge into other areas of the business where information about workers is processed, and to ensure that the organisation has a co-ordinated approach to data protection compliance.

Ideally data protection should be seen as an integral part of employment procedures rather than as a stand alone requirement. For example, in the company's written procedure for dealing with selection, there should be a section on how to follow up on references, which should incorporate the relevant benchmarks in this Code. Procedures are only of value if they are current and adhered to. Review and update procedures as necessary and put a mechanism in place to ensure that they are being followed on the ground. This might involve some form of audit or self-certification by managers.

2. It is important to remember that data protection compliance is a multi-disciplinary matter. For example, a company's IT staff may be primarily responsible for keeping computerised personal data secure, whilst a human resources department may be responsible for ensuring that the information requested on a job application form is not excessive, irrelevant or inadequate. All workers, including line managers, have a part to play in securing compliance, for example by ensuring that waste paper bearing personal data is properly disposed of.

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

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

The collection and use of sensitive data must satisfy a sensitive data condition.



See further information, page 30 for conditions to be satisfied

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

2 ADVERTISING

Advertising includes any method used to notify potential applicants of a specific job vacancy or range of vacancies, using such media as notices, newspapers, radio, television and the internet.

The benchmarks

✓
<i>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</i>
<i>2. Recruitment agencies, used on behalf of an employer, must identify themselves and explain how personal data they receive will be used and disclosed unless this is self-evident.</i>
<i>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 now holding their information.</i>

Notes and examples

1. Individuals providing personal data, even if only giving their name and address, in response to a job advertisement should be aware of who they are giving their details to. They should be made aware of this before they supply their details. Individuals should not be asked simply to provide their details to a PO Box Number or to an inadequately identified answering machine or website. Provide this explanation
 - a. in the advertisement if postal, fax or email responses are sought
 - b. in the advertisement or at the start of the telephone call if telephone responses are sought
 - c. on the website before personal data are collected via an online application form.

Advertisements for specific jobs need not state how the information supplied will be used, provided that this is self-evident. Only where the link between the information being asked for and its potential use is unclear need an explanation be given. For example if an advertisement for a specific job simply asks those interested to send in personal details and these might also be passed on to a sister company to see if it has any suitable vacancies this should be explained in the advertisement.

2. Where a recruitment agency places an advertisement on behalf of an employer, the identity of the agency must be given. The agency must also be identified as such if this is not apparent from its name. The agency should also inform the applicant if it intends to use the information supplied by the applicant for some purpose of which the applicant is unlikely to be aware, for example where the information will be used to market goods or services to the applicant. If the information supplied in response to a recruitment advertisement is to be retained for use in connection with future vacancies, the advertisement should make this clear.
3. An advertisement placed by a recruitment agency need not show the identity of the employer on whose behalf it is recruiting. The agency may pass information to the employer provided that the applicant understands that his or her details will be passed on. Once the employer receives identifiable particulars it must, as soon as it can, inform the applicant of its identity and of any uses it might make of the information received that are not self-evident. It can arrange for the agency to provide this explanation on its behalf.

If for whatever reason the employer does not want to be identified to the applicant at an early stage in the recruitment process, it is acceptable for the agency to only send anonymised information about a candidate to the employer, and for the agency or employer to provide information as to the employer's identity once the employer has expressed interest in receiving personally identifiable information about the applicant.

3 APPLICATIONS

Applications include written responses to specific job advertisements, whether made on paper or on-line. Applications can be made on forms designed by the organisation, in answer to questions, or by supplying a CV. Benchmarks in this section also cover CVs sent 'on spec'.

The benchmarks



- | |
|--|
| 1. <i>State, on any application form, to whom the information is being provided and how it will be used if this is not self-evident.</i> |
| 2. <i>Only seek personal data that are relevant to the recruitment decision to be made.</i> |
| 3. <i>Only request information about an applicant's criminal convictions if that 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.</i> |
| 4. <i>Explain any checks that might be undertaken to verify the information provided in the application form including the nature of additional sources from which information may be gathered. (The verification checks should meet the benchmarks set out in the next section.)</i> |
| 5. <i>If sensitive data are collected ensure a sensitive data condition is satisfied.</i> |
| 6. <i>Provide a secure method for sending applications.</i> |

Notes and examples

1. Where an organisation is recruiting for a specific job, it is unnecessary to explain how the information will be used if this is self-evident. For example there is no need to explain that information will be passed from the personnel department to the department where the job is located. However, if an organisation is, for example, conducting an initial trawl of applicants for a range of different jobs, perhaps to keep on file and return to as needed, this should be explained.

Where an applicant makes an unsolicited application for recruitment to an employer, typically by sending a speculative letter or email, the employer need only provide the applicant with an explanation if;

- the application is to be retained, and
- the use made of the information on the application or the period of retention goes beyond what would be self-evident to the applicant.

Any necessary explanation could be included in a letter of acknowledgement sent by the employer, although if there is no unexpected use, then no acknowledgement letter is required. Employers should have a policy on the retention or disposal of unsolicited applications for employment.

2. Information should not be sought from applicants unless it can be justified as being necessary to enable the recruitment decision to be made, or for a related purpose such as equal opportunities monitoring. For example, there is no obvious reason why employers should ask applicants for information about their membership of a trades union.

The scope of the information gathered must be proportionate to what the employer is seeking to achieve, for example the extent and nature of information sought from an applicant for the post of head of security at a bank would be very different from that sought from an applicant for work in the bank's staff canteen.

Employers should also be aware of the difference between the information needed to process an application for employment and that needed to actually administer employment. There is no obvious justification, for example, for an employer to hold information about an applicant's banking details, although it will normally be legitimate to hold these details for payment purposes once employment starts.

3. The same questions should not necessarily be asked of all prospective workers. For example, an applicant for a purely administrative job with a haulage company should not be asked for details of driving convictions, if these are only relevant to the recruitment of drivers. However some questions will be clearly relevant to all applicants. It is acceptable to ask all candidates certain core questions, such as whether they are eligible to work in the U.K.

Information on criminal convictions should only be sought if it is relevant to the job being filled. Where appropriate questions should be designed to obtain no more than the information actually needed, e.g. 'Do you have any criminal convictions involving dishonesty?' Whether by omission of an explanation or otherwise applicants should not be led to believe they have to disclose spent convictions if they do not.



See Further Information, page 35 for details of the Rehabilitation of Offenders Exceptions Order

4. One example is, if, beyond taking up references you obtain information from other local employers or other companies in your group which the worker may have been employed by or may have applied to previously. Another example is where an applicant's qualifications are to be verified in the course of the recruitment process – this should be clearly stated in the application form or surrounding documentation.
5. The collection of sensitive data must satisfy a sensitive data condition



See Further Information, page 30 for conditions to be satisfied

6. The return of applications to a postal address or fax number should be organised so that access to applications is limited. A secure method of transmission should be provided if an employer provides an on-line application facility. The use of widely available encryption-based software could be used to do this. Once the application has been received, electronically or otherwise, it must be securely stored.

4 VERIFICATION

The term 'verification', as used in this Code, is the process of checking that details supplied by applicants are accurate and complete. Verification, therefore, should not go beyond the checking of information that is sought in the application or supplied later in the recruitment process, although in this Code it also includes the taking up of references provided by the applicant. The process can include confirmation of qualifications and financial information - if this is justified in order to meet the requirements of the position. Some specialised agencies now offer a verification service.

The benchmarks



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.*
2. *If it is necessary to secure the release of documents or information from a third party, obtain a signed consent form from the applicant unless consent to their release has been indicated in some other way.*
3. *Give the applicant an opportunity to make representations should any of the checks produce discrepancies.*

Notes and examples

1. Applicants may not always give complete and accurate answers to the questions they are asked. Employers are justified in making reasonable efforts to check the truthfulness of the information they are given. The verification process should be open; applicants should be informed of what information will be verified and how this will be done. Where external sources are to be used to check the responses to questions, this should be explained to the applicant.

Access to certain records needed for the verification process may only be available to the individual concerned. You should not force applicants to use their subject access right to obtain records from a third party by making it a condition of their appointment. This is known as 'enforced subject access'. Requiring the supply of certain records in this way, including certain criminal and social security records, will become a criminal offence under the Act when the Criminal Records Bureau starts to issue "disclosures".



a. See Further Information page 33 for more information and benchmarks relating to the Criminal Records Bureau.

2. For example, some organisations will require a signed approval form from an individual before they confirm his or her qualifications to a third party.
3. Where information obtained from a third party differs from that provided by the applicant, it should not simply be assumed that it is the information provided by the applicant that is incorrect or misleading. If necessary, further information should be sought and a reasoned decision taken as to where the truth lies. As part of this process the applicant should be asked to provide an explanation where information he or she has provided is suspected of being incorrect or misleading. This is necessary to ensure that the data held are accurate and processed fairly.

5 SHORT-LISTING

Short-listing is when a selection is made of applicants who will go on to a further stage in the recruitment process, usually an interview. It can be conducted through evaluating applications and/or by conducting tests.

The benchmarks



1. Be consistent in the way personal data are used in the process of short-listing candidates for a particular position.

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

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

Notes and examples

1. It is beyond the scope of the Code to set down general rules as to how short-listing and selection testing should be carried out. This should be primarily a matter of good employment practice, although short-listing and selection testing that leads to unlawful discrimination on the grounds of race, sex or disability is likely to breach the requirement that personal data are processed fairly and lawfully. The Information Commissioner's concern is more with ensuring that the selection criteria are applied in a way that is consistent and fair to applicants, rather than that the criteria are, in themselves, fair.
2. The Act contains specific provisions on decision-making carried out by solely automated means. To fall within these provisions the decision-making must evaluate matters such as an applicant's work performance or reliability. A system that automates a simple decision, for example, to reject all applicants who are under 18 years of age, is not covered by the provision.

An example of a decision that is covered is where an individual is short-listed purely on the basis of answers provided through a touch-tone telephone in response to psychometric questions posed by a computer. The Act requires that where the individual requests it, the logic involved in making such a decision should be explained and, in some circumstances, that the decision should be reconsidered or retaken on a different basis. This right will apply if an applicant is rejected or treated in a way that is significantly different from other applicants solely as a result of the use of an automated process.

This right will not apply if the automated process merely provides information, such as the score resulting from a psychometric test where this is just one of a range of factors taken into account as part a decision-making process that has an element of human intervention or scrutiny.

3. Only by using qualified people to assess psychometric and other complex tests can short-listing be done fairly. This is normally part of good human resource practice but should also help to meet the data protection requirement that personal data are adequate for the purpose for which they are used.

6 INTERVIEWS

Interviews are used either as the final basis of the decision of who to select, or as part of that decision. Interviews can be conducted face-to-face, by telephone or via a video link.

The benchmark



- 1. Ensure that personal data that are 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*

Notes and examples

1. This Code is not concerned with setting out how interviews should be conducted. This should be primarily a matter of good employment practice.

However, the collection of personal data at interview, their recording, storage and use are likely to represent processing which falls within the scope of the Act. This means that, for example, applicants will normally be entitled to have access to interview notes about them which are retained as part of the record of the interview.

7 PRE-EMPLOYMENT VETTING

The term 'pre-employment vetting' as used in this code means actively making enquiries from third parties about an applicant's background and circumstances. It goes beyond the verification of details addressed on page 20. 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 access to 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 under the Protection of Children Act 1999. The Department of Health is developing a Protection of Vulnerable Adults list which employers intending to recruit individuals to work with certain vulnerable adults may be required to consult. The Data Protection Act 1998 does not necessarily prohibit the use of such vetting, but regulates whether and how it may be carried out.

The benchmarks



1. *Only use vetting where there are particular and significant risks to the employer, clients, customers or others, and where there is no less intrusive and reasonably practicable alternative.*
2. *Only carry out pre-employment vetting on an applicant at an appropriate point in the recruitment process. Comprehensive vetting should only be conducted on a successful applicant.*
3. *Make it clear early in the recruitment process that vetting will take place and how it will be conducted.*
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*
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.*
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.*
7. *Where information is collected about a third party, e.g. the applicant's partner, ensure so far as practicable that the third party is made aware of this.*
8. *If it is necessary to secure the release of documents or information from a third party, obtain a signed consent form from the applicant.*

Notes and examples

1. Checks should be proportionate to the risks faced by an employer and be likely to reveal information that would have a significant bearing on the employment decision. The risks are likely to involve aspects of the security of the employer or of others. They could range from the risk of breaches of national security, or the risk of employing unsuitable individuals to work with children through to the risk of theft or the disclosure of trade secrets or other commercially confidential information.
2. As a general rule
 - do not routinely vet all applicants
 - do not subject all short-listed applicants to more than basic written checks and the taking up of references, e.g. against the list of persons considered unsuitable to work with children compiled under the Protection of Children Act 1999. Do not require all short-listed applicants to obtain a 'disclosure' from the Criminal Records Bureau.



See Further Information page 33 for more information and benchmarks relating to the Criminal Records Bureau.

3. This information could be provided on the initial application form or other recruitment material. Explain to the applicant the nature, extent and range of sources of the information that will be sought. Make clear the extent to which information will be released to third parties.
4. An employer intending to use pre-employment vetting must determine carefully the level of vetting that is proportionate to the risks posed to his or her business. Employers must be very clear as to what the objectives of the vetting process are and must only pursue avenues that are likely to further these objectives. Vetting should be designed in such a way that only information that would have a significant bearing on the employment decision is likely to be obtained.
5. In exceptional cases an employer might be justified in collecting information about members of the family or close associates of the applicant. This is most likely to arise in connection with the recruitment of police or prison officers.



If sensitive data are collected one of the conditions listed on page 30 must be satisfied.

6. Employers should use all reasonable means to ensure that any external sources used as part of the vetting process are reliable. Where the vetting results in the recording of adverse information about an applicant, the applicant should be made aware of this and should be given the opportunity to make representations, either in writing or face to face.
7. Where information about a third party, e.g. the applicant's partner, is to be recorded, the collection must be fair and lawful in respect of the third party. This will mean informing third parties that information about them has been obtained and informing them as to the purposes for which it will be processed, unless this would not be practicable or would involve disproportionate effort, for example where the employer does not have contact details for the third party or the information will be kept in an identifiable form for only a very short period. In such cases there is no obligation to act.
8. During the vetting process information might be sought from a third party, e.g. a previous employer that the applicant has not given as a referee. If the information is subject to a duty of confidentiality, the third party will need some basis on which to justify its release. The employer might obtain consent for this from the applicant in order to avoid the need for the third party to contact the applicant to seek consent.

8 RETENTION OF RECRUITMENT RECORDS

It falls primarily to the employer to set retention periods in respect of recruitment records. No specific period is given in the Act; the Act merely requires that the personal data in a record shall not be kept for longer than is necessary for a particular purpose or purposes. However, any period that is set must be based on business need and should take into account any relevant professional guidelines.

The benchmarks



- 1. Establish and adhere to retention periods for recruitment records that are based on a clear business need.*
- 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.*
- 3. Consider carefully which information contained on an application form is to be transferred to the worker's employment record. Delete information irrelevant to on-going employment.*
- 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.*
- 5. 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.*
- 6. Ensure that personal data obtained during the recruitment process are securely stored or are destroyed.*

Notes and examples

1. Employers must consider carefully the justification, if any, for retaining recruitment records once the recruitment process has been completed.

Retention of recruitment records may be necessary for the organisation to defend itself against discrimination claims or other legal actions arising from recruitment. However, the possibility that an individual may bring a legal action does not automatically justify the indefinite retention of all records relating to workers. A policy based on risk-analysis principles should be established.

Recruitment agencies have some legal obligations to retain records under the Employment Agencies Act 1973.

Employers should consider the possibility that some business needs might be satisfied by using anonymised rather than identifiable records. For example, if the organisation wishes to compare the success of various recruitment campaigns, this could be achieved by using anonymised records.

2. This is consistent with the Criminal Records Bureau Code of Conduct. However, where there is a legal obligation to retain specified information for longer than 6 months, this must be respected.



See Further Information page 33 for more information and benchmarks relating to the Criminal Records Bureau.

3. Some information is gathered during the recruitment process that may not be relevant to the employment situation. Only retain information that has on-going relevance or is needed as evidence of the recruitment process. For example, consider carefully whether there is a reason to retain information about an applicant's former salary once he or she has started employment. For practical reasons it may be difficult to delete some information on application forms whilst retaining the rest. Employers should however design application forms to facilitate the easy deletion of information which is irrelevant to the on-going employment relationship.
4. A note may be kept showing that a check was completed and the results of the findings.
5. Unless there is a reason to believe that an applicant wishes to be considered again, the assumption should be that he or she has applied only for the vacancy advertised. Application forms or recruitment advertisements can give the applicant the choice as to whether he or she wishes to apply only for the advertised post or would like his or her details to be kept on file in case another position arises.
6. Whether stored manually or electronically, personal data should be kept secure and as far as is practicable access to the data should be limited.

SECTION 3: FURTHER INFORMATION

Sensitive Personal Data

When can sensitive personal data be processed?

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

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

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

- ensure the health, safety and welfare at work of worker
- select safe and competent workers
- ensure a safe working environment
- not discriminate on the grounds of race, sex or disability
- ensure the reliability of workers with access to personal data
- protect customers' property or funds in the employer's possession
- check immigration status before employment

Thus an employer may be able to collect information as to an applicant's criminal record or health in the recruitment process if this can be shown to be necessary to enable the employer to meet its obligations in relation to the safety of its workers or others to whom it owes a duty of care. The collection of sensitive personal data must however be 'necessary' for exercising or performing a right or obligation which is conferred or imposed by law. This condition would not, for example, be satisfied if the employer obtains information on the criminal convictions of all applicants in order to protect its staff or customers if the protection could equally be provided by obtaining this information only on the successful applicant prior to confirmation of appointment.

- The processing –
- is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- is necessary for the purpose of obtaining legal advice, or

- is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Note: The application of this condition in the context of recruitment and selection is quite limited but it might for example be relied on to enable a prospective employer to process sensitive personal data to defend him or herself were an applicant to make a claim of unlawful discrimination.

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

Note: This condition will be relevant to equal opportunities monitoring related to racial origin, religion and disability. Processing must be “necessary” emphasising that wherever practicable monitoring should be based on anonymous or aggregated information.

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

Note: This condition is most likely to be relevant to public sector bodies that may have specific legal duties placed on them in relation to the qualifications, attributes, background or probity of their workers. It will also be relevant when a public sector body concludes that in order to discharge its wider statutory functions it is necessary for it to process sensitive personal data such as criminal convictions relating to applicants or, in exceptional cases, their family or close associates. It is likely, for example, to be relevant to the recruitment of police or prison officers.

- The data subject has given explicit consent to the processing

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

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

The extent to which consent can be relied upon in the context of employment is limited because of the need for any consent to be freely given. However in relation to the recruitment and selection of workers this is less of a constraint. Individuals in the open job market will usually have a free choice whether or not to apply for a particular job. If consent to some processing of sensitive data is a condition of an application being considered this does not prevent the consent being freely given. It must of course be clear to the applicant exactly what he or she is consenting to. As recruitment proceeds it becomes less likely that valid consent can be obtained. If, for example, the direct consequence of not consenting is the withdrawal of a job offer the consent is unlikely to be freely given.

The Criminal Records Bureau

Although 'enforced subject access' will shortly be an offence, it is recognised that in some circumstances it may be proper for an employer to know whether an applicant has a criminal record and, if so, what it contains.

With this in mind, the Government has set up the Criminal Records Bureau which is intended to put the disclosure of information about an individual's criminal history in England and Wales on a statutory footing and to put proper safeguards in place concerning the handling of this information.

Separate provisions are to be implemented in Scotland and will be administered by the Disclosure Bureau.



See Useful Addresses page 36 for contact details.

The information constituting a disclosure will be derived from an individual's criminal record. There is no obligation placed on employers to request a disclosure.

Three types of disclosure

The Bureau will issue three different types of disclosure;

- The basic disclosure
- The standard disclosure
- The enhanced disclosure

The basic disclosure will contain details of convictions held on the Police National Computer that are 'unspent' under the Rehabilitation of Offenders Act. The basic disclosure will not be issued to organisations directly. Instead, it will be made available on request to individuals and can be used by them when they seek paid or unpaid employment. There is no legal obligation on an applicant to supply a disclosure to an employer. The basic disclosure is due to be introduced in the second half of 2002.

The standard disclosure will be issued to organisations directly. It applies to posts exempted under the Rehabilitation of Offenders Act and relates particularly to certain sensitive areas of employment, such as posts involving regular contact with children and vulnerable adults. The standard disclosure contains details of both spent and unspent convictions, as well as cautions, reprimands and final warnings held on the Police National Computer. The standard disclosure is due to be introduced in the second half of 2002.

The enhanced disclosure will also be issued to organisations directly. It applies to posts involving greater contact with children or vulnerable adults, for example jobs involving caring, supervising, training or being in sole charge of children and vulnerable adults. The enhanced disclosure contains the same information as a standard disclosure together with information from

local police records if that is thought to be relevant to the position applied for. The enhanced disclosure is due to be introduced in the second half of 2002.

Status of the Criminal Record Bureau Code in relation to Data Protection

There is a Code of Practice issued by the Criminal Records Bureau that sets out employers' obligations in respect of the use of information obtained through standard and enhanced disclosure. The CRB Code does not attempt to address issues concerning the basic disclosure, but the Commissioner nevertheless considers many of its standards to be equally appropriate. In her view, a failure to comply with the relevant provisions of the CRB Code is likely to lead to a breach of the Data Protection Act 1998.

Benchmarks for the handling of information obtained through disclosure.

- **Consider carefully whether it is necessary for the protection or conduct of business to request a disclosure. The collection and holding of disclosure information that is excessive will breach the data protection principles.**
- **Once disclosure information has been obtained and an employment decision made, do not retain the information unless there is an overriding reason for doing so. Usually it will be sufficient to record that the check has been carried out and its result. In any event, do not retain the information for more than 6 months.**
- **Do not share with other employers the information obtained through a disclosure.**
- **Do not attempt to obtain information about criminal convictions by enforced subject access or from sources other than the CRB or the applicant. The carrying out of media checks to look for spent convictions for a post that is not eligible for standard or enhanced disclosure is likely to breach the Act. Media checks involve obtaining information from old newspaper articles or similar sources about an individual.**

Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975

Criminal offences that are "spent" do not normally have to be declared on application forms or in answer to other requests for information about criminal convictions. There are exceptions for certain types of job which are covered in this order.

The types of job covered by this Order are divided into 3 categories.

- 1) The professions e.g. medical practitioners, barristers, accountants, vets and opticians
- 2) Those employed to uphold the law e.g. judges, constables, prison officers and traffic wardens and those involved in the provision of social services
- 3) Certain regulated occupations e.g. firearms dealers, directors of insurance companies and those in charge of certain types of nursing home

Please note that this is **not** a full list. A full explanation of the Order can be obtained from The Stationery Office.



See Useful Addresses page 36 for contact details.

Useful addresses

Information Commissioner

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545745 (for information and other parts of the Code) OR
01625 545740 (for notification)

Fax: 01625 524 510

E-mail: data@dataprotection.gov.uk (for information and requests for other parts of the Code) OR
mail@notification.demon.co.uk (for notification information)

Websites: www.dataprotection.gov.uk (for information and to download other parts of the Code) OR
www.dpr.gov.uk (for notification)

Advisory, Conciliation and Arbitration Service (ACAS)

Brandon House
180 Borough High Street
London
SE1 1LW

Telephone: 020 7210 3606

Fax: 020 7210 3919

Website: www.acas.co.uk

Chartered Institute of Personnel and Development

CIPD House
Camp Road
London
SW19 4UX

Telephone: 020 8971 9000

Fax: 020 8263 3333

Website: www.cipd.co.uk

Commission for Racial Equality

Elliot House
10-12 Allington Street
London
SW1E 5EH

Telephone: 020 7828 7022
Fax: 020 7630 7605
E-mail: info@cre.gov.uk
Website: www.cre.gov.uk

Disability Rights Commission

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

Telephone: 08457 622 633
Fax: 08457 778 878
Textphone: 08457 622 644
E-mail: ddahelp@stra.sitel.co.uk
Website: www.drc-gb.org

Equal Opportunities Commission

Customer Contact Point
Arndale House
Arndale Centre
Manchester
M4 3EQ

Telephone: 0161 833 9244
Fax: 0161 838 8312
E-mail: info@eoc.org.uk
Website: www.eoc.org.uk

The Stationery Office

PO Box 29
Norwich
NR3 1GN

Telephone: General Enquiries 08700 600 5522
Fax: 08700 600 5533
E-mail: book.orders@theso.co.uk
Website: www.ukstate.com

Health & Safety Executive

Rose Court
Southwark Bridge
London
SE1 9HS

Telephone 08701 545500
Fax 02920 859260
Website: www.hse.gov.uk

British Psychological Society

St Andrews House
40 Princess Road East
Leicester
LE1 7DR

Telephone 016 254 9568
Fax 0116 247 0787
Website: www.bps.org.uk

Criminal Records Bureau

PO Box 91
Liverpool
L69 2UH

Telephone 0870 9090811
Website: www.crb.gov.uk

The Disclosure Bureau

The Scottish Criminal Record Office
1 Pacific Quay
Glasgow
Scotland
G51 1EA.

Telephone 0141 585 8495
Website: www.disclosurescotland.co.uk.

SECTION 4: FREQUENTLY ASKED QUESTIONS

Is all information about workers now covered by the Act?

No, but in practice most employment records will be. As well as computerised records manual data held within a “relevant filing system” are now covered by the Act. This is defined as any set of data which is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible. An example of a relevant filing system would be a personnel file with an worker’s name or individual reference number on it, in which it is possible to find information about the worker such as starting date, performance mark at last appraisal, previous employer etc. Less obviously structured records may also be caught, for example, a completed set of job application forms. Unstructured collections of information, such as those warehoused in no particular order will not be covered.

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

Consent to hold personal data relating to workers is not usually required. Indeed, the Commissioner considers it misleading to seek consent from workers if they have no real choice.

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



See further information page 30 for the conditions for processing Sensitive Data.

How can the company be expected to keep accurate records if applicants give us wrong information?

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

How can I check that a candidate isn't lying on his or her application form – doesn't the Act stop me doing this?

The Act does not prevent an employer from checking whether a candidate is lying. However, the Act requires that if checks on information are to be carried out the candidate is aware of this. In some cases, for example where a school or college is to be asked to disclose information to verify a candidate's qualifications, they may want the candidate's permission before doing so.

If we're only going to use the information that applicants supply to us on their application forms to process their application, what's the point of telling them this?

There is no obligation in the Act to tell individuals what is going to happen to information they have provided so long as it is no more than they are likely to expect. If the information is to be used for a purpose that might not be expected, for example where applicants' details are to be used for direct marketing purposes, they must be advised of this and any objections respected.

We employ staff who work with children – how can we protect these children if the Act prevents us from getting a copy of the applicant's police record?

There is a provision in the Act that will prohibit 'enforced subject access' in connection with employment or recruitment once the Criminal Records Bureau starts to issue 'disclosures' listing convictions and certain other information. Once the CRB system is in operation, then this will be the channel that must be used for checking applicants' police records.



See Further Information page 33 for more information on the Criminal Records Bureau

Do we have to show candidates the notes we make when we interview them?

There is no general exemption from the Act's subject access rights in respect of interview notes about candidates. This means that when an individual makes a request for access to the notes, it must be granted unless the set of notes is so unstructured as to fall outside the Act.

Isn't there an exemption in the Act for references?

There is no such general exemption from the right of subject access. There is, however, a special exemption from the right of access to a confidential reference when in the hands of the organisation which gave it. This exemption does not apply once the reference is in the hands of the person or organisation to whom the reference has been given. The recipient is, though, entitled to take steps to withhold information that reveals the identity of other individuals such as the author of the reference.



See Part 2 – Employment Records page 00 for more information on references.

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

The Act doesn't require that all information is deleted straight away. However, information that is retained for a particular purpose should not be kept for longer than is necessary for that purpose. This does not rule out keeping information to protect against legal action. Employers should however consider carefully what information they hold and why they hold it. A 'risk analysis' approach to data retention is recommended.

SECTION 5: CHECKLIST

Completing this checklist is not a requirement of either the Act or the Code but is meant to assist you in implementing the Code. The checklist is aimed at the person in the organisation who is responsible for implementation. Who has responsibility for the various actions will depend on the make up of your organisation.

1 Managing Data

Possible action points

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

Action	✓
Ensure that someone is responsible for delivering compliance.	
Ensure the person responsible reads all relevant parts of the Code.	
Obtain all written employment procedures and note unwritten procedures and practices and check them 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.	

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

Action	✓
Prepare a briefing to departmental heads and line managers about their responsibilities.	
Distribute or deliver the briefing and be available to answer questions.	

- 1.3 *Assess what personal data about workers are in existence and who is responsible for them.*

Action	✓
Consider using the checklists produced in conjunction with other parts of the Code to assess all personal data.	
Check with personnel functions as to the types of data that are held.	
Check with Departments as to the types of data that are held.	

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

Action	✓
<p>Consider each type of personal data that are held and determine whether any information could be deleted or not collected in the first place.</p> <p>Check that the collection and use of any sensitive personal data satisfies at least one of the sensitive data conditions.</p>	

- 1.5 *Ensure that workers are aware of the extent to which they can be criminally liable if they knowingly or recklessly disclose personal data outside their employer's policies and procedures. Make serious breaches of a data protection rules a disciplinary offence.*

Action	✓
<p>Prepare a guide explaining to workers the consequences of their actions in this area.</p> <p>Make sure that an infringement of data protection procedures is clearly indicated as a disciplinary offence.</p> <p>Ensure that the guide is brought to the attention of new staff. Ensure that staff can ask questions about the guide.</p>	

- 1.6 *Allocate responsibility for checking that your organisation has a valid notification in the register of data controllers that relates to the processing of personal data about workers, unless it is exempt from notification.*

Action	✓
<p>Consult the Data Protection Register website www.dpr.gov.uk to check the status of your organisation regarding notification.</p> <p>Check whether your organisation is exempt from notification using the website.</p> <p>Check whether all information about workers is described there, if your organisation is not exempt.</p> <p>Allocate responsibility for checking and updating this information on a regular basis, for example every 6 months.</p>	

- 1.7 *Consult trade unions or other workers' representatives, if any, or workers themselves over the development and implementation of employment practices and procedures that involve the processing of workers' data.*

Action	✓
On formulating new practices and procedures, assess the impact on processing personal data.	
Consult with workers or workers representatives about the processing. Take account of their suggestions and concerns.	

2 Advertising

Possible action points

- 2.1 *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.*

Action	✓
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 data are collected on an online application form.	
Ensure the purpose for which you may use the personal data is described in the advertisement, for example, to market your organisations products and service unless self evident.	

- 2.2 *Recruitment agencies, used on behalf of an employer, must identify themselves and explain how personal data they receive will be used and disclosed unless this is self-evident.*

Action	✓
Ensure that the recruitment agency 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.	

- 2.3 *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.*

Action	✓
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.	
<p>OR</p> <p>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.</p>	

3 Applications

Possible action points

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

Action	✓
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.	

- 3.2 *Only seek personal data that are relevant to the recruitment decision to be made.*

Action	✓
Determine whether all questions are relevant for all applicants.	
Consider customising application forms where posts justify the collection of more intrusive personal data.	
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.	

- 3.3 *Only request information about an applicant's criminal convictions if that 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.*

Action	✓
Consider whether the collection of information about criminal convictions can be justified.	
Check that it is stated that spent convictions do not have to be declared (unless the job is one covered by the Exceptions Order).	

- 3.4 *Explain any checks that might be undertaken to verify the information provided in the application form including the nature of additional sources from which information may be gathered.*

Action	✓
Ensure there is a clear statement on the application form or surrounding documents, explaining what information will be sought and from whom.	
Explain the nature of the verification process and the methods used to	

achieve this.

3.5 *If sensitive data are collected ensure a sensitive data condition is satisfied.*

Action	✓
Assess whether the collection of sensitive data is relevant to the recruitment process.	
Remove any questions about sensitive data that are not relevant. 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.	

3.6 *Provide a secure method for sending applications.*

Action	✓
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.	

4 Verification

Possible action points

- 4.1 *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.*

Action	✓
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. Ensure that applicants are not forced to use their subject access rights to obtain records from a third party (i.e. by making such a requirement a condition of getting a job.)	

- 4.2 *If it is necessary to secure the release of documents or information from a third party, obtain a signed consent form from the applicant unless consent to their release has been indicated in some other way.*

Action	✓
Ensure applicants provide signed consent if this is required to secure the release of documents from a third party.	

- 4.3 *Give the applicant an opportunity to make representations should any of the checks produce discrepancies.*

Action	✓
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.	

5 Short-listing

Possible action points

- 5.1 *Be consistent in the way personal data are used in the process of short-listing candidates for a particular position.*

Action	✓
Check shortlist methods with sources of good practice such as the Equal Opportunities Commission or Commission with Racial Equality - see Useful Addresses page 36.	

- 5.2 *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.*

Action	✓
<p>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.</p> <p>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.</p>	

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

Action	✓
Determine which such tests are operated within your organisation.	
Ensure all tests are assessed by properly qualified persons.	

6 Interviews

Possible action points

- 6.1 *Ensure that personal data that are 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.*

Action	✓
Ensure that all interviewers are aware that interviewees 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 dealing with applicants, how to deal with request for access to interview notes.	
If written procedures exist for interviews, ensure that these provisions are built into them.	

7 Pre-employment vetting

Possible action points

- 7.1 *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.*

Action	✓
<p>Find out for which jobs, if any, pre-employment vetting takes place.</p> <p>Consider whether pre-employment vetting is justified for each of these jobs and whether the information could be obtained in a less intrusive way.</p>	

- 7.2 *Only carry out pre-employment vetting on an applicant at an appropriate point in the recruitment process. Comprehensive vetting should only be conducted on a successful applicant.*

Action	✓
<p>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 short-listed applicants (only the people selected for the job should be submitted to comprehensive pre-employment vetting).</p>	

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

Action	✓
<p>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.</p> <p>If information is sought from a third party, ensure the third party has some basis to justify its release, such as evidence of the applicant's consent to the disclosure.</p>	

- 7.4 *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.*

Action	✓
<p>Ensure that there are clearly stated objectives in any vetting process.</p> <p>Consider the extent and nature of information that is sought against these objectives.</p> <p>Eliminate any verification that consists of general intelligence-gathering. Ensure that it is clearly focussed on furthering particular objectives.</p>	

7.5 *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.*

Action	✓
<p>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.</p> <p>Ensure that if family members or close associates are approached it can be justified by the nature of the job.</p>	

7.6 *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.*

Action	✓
<p>Ensure that information that has been collected from a vetting process is evaluated in the light of the reliability of the sources.</p> <p>Ensure that no recruitment decision is made solely on the basis of information obtained from a source that may be unreliable.</p> <p>Ensure that if information received will lead to the applicant not being appointed, then this will be made known to the applicant.</p> <p>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.</p> <p>Build these measures into any written recruitment procedure that already exists.</p>	

7.7 *Where information is collected about a third party, ensure so far as practicable that the third party is made aware of this.*

Action	✓
<p>Ensure that those conducting a vetting process are briefed to avoid discovering information about a third party unnecessarily.</p> <p>Where substantial personal data have been collected about a third party and are to be retained, ensure there is a process in place to inform the third party of this and of how the data will be used.</p> <p>Build these measures into any written recruitment procedure that already exists.</p>	

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

Action	✓
Ensure applicants provide signed consent if this is required to secure the release of documents from a third party.	

8 Retention of recruitment records

Possible action points

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

Action	✓
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.	

8.2 *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.*

Action	✓
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.	
If written procedures on vetting exist, incorporate these measures into them.	

8.3 *Consider carefully which information contained on an application form is to be transferred to the worker's employment record. Delete information irrelevant to on-going employment.*

Action	✓
Assess 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.	
Build this in to any written recruitment procedures.	

8.4 *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.*

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

8.5 *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.*

Action	✓
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.	

8.6 *Ensure that personal data received during the recruitment process are securely stored or are destroyed.*

Action	✓
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.	
Inform them that electronic files should kept securely, for example by using passwords and other technical security measures.	

FOLLOWING THE CODE WILL:

- increase trust in the workplace - there will be transparency about information held on workers in the organisation, thus helping to create an open atmosphere where workers have greater 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 guard themselves from challenges against their data protection practices.
- encourage workers to respect the personal data of customers - following the Code will create a general level of awareness of personal data issues, helping to ensure workers treat information about customers properly.
- aid organisations in meeting other legal requirements - the Code is intended to be consistent with other pieces of legislation such as The Human Rights Act 1998 and The Regulation of Investigatory Powers Act 2000 (RIPA).
- assist global businesses in complying with similar legislation in other countries - the Code is produced in the light of EC Directive 95/46/EC and should be in line with legal requirements in other European Union member states concerning data protection.
- help to prevent the illicit use of information by workers - informing workers 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.

Information Commissioner

Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF Telephone: 01625 545 700 Facsimile: 01625 524510
e-mail: data@dataprotection.gov.uk Website: www.dataprotection.gov.uk