The Employment Practices Code

Supplementary Guidance

Information Commissioner's Office

contents

About the Supplementary Guidance 3

Managing Data Protection: Supplementary Guidance 5

GOOD PRACTICE RECOMMENDATIONS: NOTES AND EXAMPLES 6

Part 1: Recruitment & Selection: Supplementary Guidance 9

GOOD PRACTICE RECOMMENDATIONS: NOTES AND EXAMPLES 10

THE CRIMINAL RECORDS BUREAU AND DISCLOSURE SCOTLAND 17

REHABILITATION OF OFFENDERS ACT 1974 (EXCEPTIONS) ORDER 1975 19

Part 2: Employment Records: Supplementary Guidance 21

GOOD PRACTICE RECOMMENDATIONS: NOTES AND EXAMPLES 22

ACCESS WHEN INFORMATION ABOUT THIRD PARTIES IS INVOLVED 40

EXEMPTIONS FROM THE SUBJECT ACCESS RIGHT 42

EXEMPTIONS FROM NON-DISCLOSURE 43

Part 3: Monitoring at Work: Supplementary Guidance 45

GOOD PRACTICE RECOMMENDATIONS: NOTES AND EXAMPLES 46

HOW INTRUSIVE IS YOUR MONITORING? 56

LAWFUL BUSINESS PRACTICE REGULATIONS 58

Part 4: Information About Workers' Health: Supplementary Guidance 63

GOOD PRACTICE RECOMMENDATIONS: NOTES AND EXAMPLES 64

Conditions for Processing Sensitive Data 72

Frequently Asked Questions 76

Useful Addresses 83

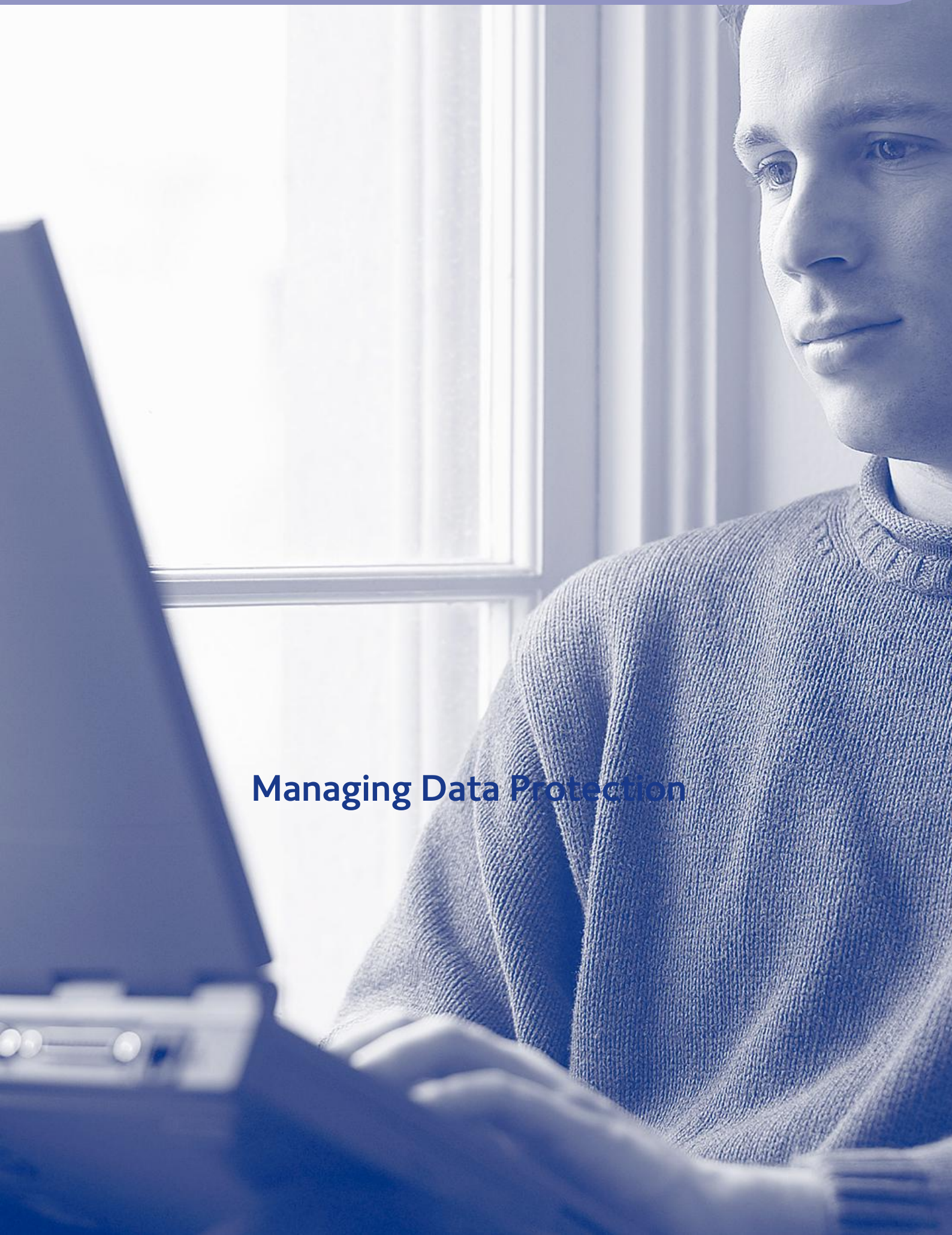
Information Commissioner's Office

About the Supplementary Guidance

This supplementary guidance does not in itself form part of the Information Commissioner's Employment Practices Data Protection Code'. It is intended to complement the main Code by giving supplementary information about the issues covered in it.

This guidance includes notes and examples which are intended to give readers a better understanding of some of the practical issues that may arise when implementing the Information Commissioner's good practice recommendations. It also includes a set of frequently asked questions and useful contact details. We hope it will be of use to those seeking a more in-depth understanding of the issues covered in the Code itself.

Supplementary Guidance



Managing Data Protection

Good Practice Recommendations Managing Data Protection: Notes and Examples

0.1 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 IT security procedure there should be a section on monitoring which should be based on the relevant benchmarks in this Code. Procedures are only of value if they are current and adhered to. Review and upgrade 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.

0.2 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 information 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 information is properly disposed of. An employer is liable to pay compensation for damage suffered by an individual as a result of a breach of data protection law arising from the actions of a line manager 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.

0.3 It may be helpful to assess personal information held on workers using the same categories as are used in the various parts of this Code, i.e. personal information processed in connection with recruitment and selection, employment records, monitoring at work and health 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.

0.4 When making your assessment of personal information 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 information must satisfy a sensitive data condition.

0.5 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

0.6 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.

0.7 Consultation about decisions likely to lead to changes in work organisation or contractual relations is starting to become mandatory under employment law for larger employers. Whether a legal obligation or not consultation should help ensure processing of personal information is fair to the workers to whom the information relates.

Part 1: Recruitment and Selection

Good Practice Recommendations Part 1: Notes and Examples

1.1 Advertising

1.1.1 Individuals providing personal information, 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.

1.1.2 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.

1.1.3 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.

1.2 Applications

1.2.1 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. 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.

1.2.2 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.

1.2.3 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 in the last 5 years 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 page 19 for details of the Rehabilitation of Offenders Exceptions Order.

1.2.4 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.

1.2.5 No further guidance on this recommendation

1.2.6 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.

1.3 Verification

1.3.1 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 basic disclosures .

1.3.2 One method that is sometimes used to try to find information about a worker's criminal record is a media check. This involves obtaining information from old newspaper articles or similar sources about the person. 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.

The obtaining of information about an applicant through the CRB or Disclosure Scotland is an intrusion into an applicant's private life. The intrusion may be justified by the nature of the job being filled but it should not be undertaken unnecessarily. It should therefore be left as late as is practicable in the recruitment process.

See page 17 for more information relating to the Criminal Records Bureau and Disclosure Scotland.

1.3.3 Some organisations will require a signed approval form from an individual before they confirm information such as his or her qualifications to a third party.

Under the Act it can be an offence to bring about a disclosure of personal information without the consent of the holder of the information. You would not have the holder's consent if you misled them into disclosing the information to you, for example, by saying that an applicant for a job had agreed to a disclosure when the applicant had not in fact done so.

1.3.4 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 information held is accurate and processed fairly.

1.4 Short-listing

1.4.1 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.

1.4.2 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.

1.4.3 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 information is adequate for the purpose for which it is used.

1.5 Interviews

1.5.1 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 information at interview, its recording, storage and use may well represent processing which falls within the scope of the Act. This means that, for example, applicants will then be entitled to have access to interview notes about them which are retained as part of the record of the interview.

See Part 2 Employment Records, page 39 for more information about Workers Access to Information about Themselves.

1.6 Pre-employment vetting

1.6.1 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.

It is less intrusive to obtain relevant information directly from the applicant and then verify it than it is to obtain information about the applicant directly from third parties. The former approach should be adopted wherever practicable.

Sometimes a customer for a supplier's products or services may seek to impose a condition requiring the supplier to carry out pre-employment vetting of its workers. For example, a contractor working in a defence establishment may be required to vet workers taken on to work on the relevant contract. If this vetting involves processing personal information about the workers it will not be justified simply because it is a condition of business. Such a condition cannot override the employer's obligation to comply with the Act. Vetting of workers by the supplier or contractor must be based on the outcome of its own assessment. This does not stop the supplier or contractor being guided by any assessment the customer for its products or services might have undertaken for itself.

1.6.2 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

1.6.3 No further guidance on this recommendation

1.6.4 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.

1.6.5 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 72 must be satisfied.

1.6.6 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.

1.6.7 Where information about a third party, e.g. the applicant's partner, that affects the third party's privacy 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.

1.6.8 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.

Under the Act it can be an offence to bring about a disclosure of personal information without the consent of the holder of the information. You would not have the holder's consent if you misled them into disclosing the information to you, for example, by saying that an applicant for a job had agreed to a disclosure when the applicant had not in fact done so.

1.7 Retention of recruitment records

1.7.1 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. Employers must though consider carefully the justification, if any, for retaining recruitment records once the recruitment process has been completed. Any relevant professional guidelines should be taken into account.

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.

1.7.2 This is consistent with the Criminal Records Bureau and Disclosure Scotland Codes of Practice. However, if you are required by law to retain specified information for longer than 6 months, the legal obligation must be complied with.

See page 17 for more information relating to the Criminal Records Bureau and Disclosure Scotland.

1.7.3 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.

1.7.4 A note may be kept showing that a check was completed and the results of the findings.

1.7.5 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.

1.7.6 Whether stored manually or electronically, personal information should be kept secure and as far as is practicable access to the information should be limited.

See Part 2 Employment Records, page 31 for recommendations on security.

The Criminal Records Bureau and Disclosure Scotland

It is recognised that in some circumstances it will be proper for an employer to know whether an applicant for a job has a criminal record and, if so, what it contains. With this in mind, the Government has set up the Criminal Records Bureau (CRB) which puts the disclosure of information about an individual's criminal history on a statutory footing and puts some safeguards in place concerning the handling of this information.

The CRB covers England and Wales. The equivalent body in Scotland is called Disclosure Scotland. There is, as yet, no equivalent in Northern Ireland.

See Useful Addresses page 84 for contact details.

The CRB and Disclosure Scotland issue what are known as disclosures . The information constituting a disclosure is derived from an individual's criminal record. In some circumstances it may also include non-conviction information from local police records. There is no general obligation placed on employers to request a disclosure.

Three types of disclosure

The CRB and Disclosure Scotland issue three different types of disclosure;

- the basic disclosure
- the standard disclosure
- the enhanced disclosure.

The basic disclosure contains details of convictions held on central police records that are unspent' under the Rehabilitation of Offenders Act. The basic disclosure is not issued to organisations directly. Instead, it is 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. Basic disclosures are currently only available from Disclosure Scotland. There is no firm date for their introduction in England and Wales.

The standard disclosure is issued to organisations directly. It applies to posts covered by the Exceptions Order to 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 central police records. It is available from both the CRB and Disclosure Scotland.

The enhanced disclosure is also 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. Enhanced disclosures are available from both the CRB and Disclosure Scotland.

Status of the CRB and Disclosure Scotland codes in relation to data protection

There are Codes of Practice issued by the Criminal Records Bureau and Disclosure Scotland that set out employers' obligations in respect of the use of information obtained through standard and enhanced disclosure. The Codes do not attempt to address issues concerning the basic disclosure, but the Commissioner nevertheless considers many of their standards to be equally appropriate. A failure to comply with the relevant provisions of the CRB or Disclosure Scotland Code could well lead to a breach of the Data Protection Act 1998.

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 can be divided into 5 broad 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.
3) Certain regulated occupations e.g. firearms dealers, directors of insurance companies, those in charge of certain types of nursing homes and taxi drivers.
4) Those who work with children, those whose work is concerned with the provision of care services to vulnerable adults and those whose work is concerned with the provision of health services.
5) Those whose work could put national security at risk e.g. air traffic controllers and certain employees of the Crown.

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 85 for contact details.

Part 2: Employment Records

Good Practice Recommendations Part 2: Notes and Examples

2.1 Collecting and keeping general records

2.1.1 There is no need to provide workers with details that are self evident. They do not, for example, need to be told that information on their earnings will be disclosed to the Inland Revenue. Consent may be needed if sensitive data are held but there may be alternative ways of meeting the sensitive data conditions.

See page 72 which explains more about the conditions for processing sensitive personal data.

Possible different ways of informing workers include distribution of a fact sheet, information given on an intranet or inclusion of relevant material in an induction course.

2.1.2 This information can, of course, be combined with that provided under 2.1.1.

2.1.3 For example, employers often require an emergency contact to be used should a worker be taken ill at work. If you ask for next of kin' you will not necessarily obtain the information needed.

2.1.4 Some employers may decide that it is not practicable to provide each worker with a copy of their personal details annually. If so they must ensure they have an effective alternative for ensuring records are kept accurate and up to date. In some cases employers may be able to take advantage of the capabilities of automated systems. For example, workers' PCs could prompt them to check their personal details from time to time and require them to acknowledge that they have done so. Employers must be prepared to give access to records when a worker makes a subject access request but employers should not rely on this alone as a means of ensuring accuracy.

2.1.5 For example, a computerised personnel system could have a built-in facility to automatically query the input date of birth of workers, highlighting ages above or below the normal working age. Similar flagging can be used to automatically alert the organisation to information that may be out of date. This could be used as part of a review and deletion policy. Systems which incorporate audit trails showing who has created or altered a record and when also assist in ensuring accuracy. They enable the employer to trace the sources of inaccurate records and to take action to prevent recurrence.

Many businesses buy computerised personnel systems off the shelf'. The business should make sure the system facilitates data protection compliance. The legal responsibility for compliance rests clearly with users rather than suppliers of systems. Users cannot simply blame the system. The Information Commissioner does though recognise that it may take businesses some time to bring existing systems up to the desired standards. This will be taken into account should the possibility of enforcement action arise as a result of a breach of the Act.

2.2 Security

2.2.1 It is beyond the scope of this Code to set general security standards that may have no special relevance to employment records. BS7799: 1995 (Code of Practice for Information Security Management, British Standards Institution, ISBN: 580236420) provides guidance and recommendations which, if followed, should address the main risks. Not all the controls described in BS 7799 will necessarily be relevant to all organisations but many are as applicable to small as well as to large organisations.

See page 83 Useful Addresses for British Standards Institute

2.2.2 For example, confidential worker information should not be stored on laptop computers that do not have adequate access controls, i.e. controls that would prevent access to the information stored on the computer should it be stolen or misplaced. Give access to such information sparingly; for example, access to confidential worker information should not normally be given to technical staff for use in testing computer hardware or software. The basic principle should be that information about workers is only available to those who need it to do their job. Access rights should be based on genuine need not seniority.

2.2.3 Computer systems increasingly incorporate audit trails. These can record automatically when and how records have been altered and by whom. In some cases they also record when a record has been accessed and by whom. Where systems detect unusual patterns of access to personal information, for example where one worker accesses information noticeably more frequently than other workers in a similar position, this should be investigated and if necessary preventative action taken.

2.2.4 It is important to check the reliability of workers who have access to personal information. They should be made aware of the security regime that surrounds it. Where appropriate a confidentiality clause should be incorporated into their contracts. Do not overlook workers in management positions as they may pose as great a risk as other workers, or even a greater one, as they may enjoy wider access to information than other workers.

2.2.5 There should be a procedure for taking employment records, whether computerised or in paper files, off-site if this is allowed at all. This should make clear who, if anyone, is allowed to take information and what information they can take. It should address security risks, e.g. laptops not to be left unattended in vehicles. Do not overlook senior managers who may think procedures like this do not apply to them.

2.2.6 There are risks with the use of faxes. A confidential fax message may be received on a machine to which many people have access. It can also be retained in the memory of the sending and/or receiving machine. Fax messages can easily be misdirected, for example, by miskeying the fax number of the intended recipient. Do not use general company e-mail addresses or fax numbers for the transmission of confidential information.

An employer must not allow the transmission of confidential worker information by e-mail without taking appropriate security measures. Encryption may protect e-mail in transit but it may still be vulnerable at either end. If a confidential e-mail is deleted bear in mind that a copy may nevertheless be retained on the system.

To secure fax and e-mail systems

- ensure that copies of e-mails and fax messages containing sensitive information received by managers are held securely and that access to them is restricted.
- provide a means by which managers can permanently delete e-mails from their personal work-stations that they receive or send and make them responsible for doing so.
- check whether deleted' information is still stored on a server. If so, ensure that this too is permanently deleted unless there is an overriding business need to retain it. In any event, restrict access to information about workers held on servers. Don't forget that those providing IT support have access to servers. They may be outside contractors.
- draw the attention of all workers to the risks of sending confidential or sensitive personal information by e-mail or fax.

2.3 Sickness and injury records

2.3.1 With computer based systems the separation of sickness and injury records from absence records can be achieved by logical rather than physical separation, perhaps with additional password protection.

Do not access information about sickness or injury when information only about the length of absence is needed. For example, when calculating a benefit, it may only be necessary to see the length of absence rather than the nature of the sickness responsible for the absence.

2.3.2 The Act does not prevent employers from keeping sickness and injury records about their workers. Such records are clearly necessary for an employer to review the ability of workers to undertake the work for which they are employed, and for other purposes such as the detection of health and safety hazards at work and the payment of health-related benefits to workers.

Where an employer is obliged by law to process sensitive personal data, for example under health and safety or social security legislation, it is easy to satisfy a sensitive data condition. In other cases, particularly involving sickness records, it may be less clear cut that a sensitive data condition is satisfied. Because of this some employers have sought to rely on obtaining the worker's explicit consent for the processing. The Commissioner recognises that employers need to keep some sickness records but doubts the validity of consent as a basis for the processing of the health data involved. He takes the view that an employer keeping and using sickness records in a reasonable manner is likely to satisfy one of the other sensitive data conditions. Whilst the Data Protection Act, as it currently stands, does not place this question beyond doubt, he understands the Government is considering changes to the law that will do so.

2.3.3 This recommendation does not stand in the way of the disclosure of number of days of absence such as might be involved, for example, in giving a reference.

See Part 2 Employment Records, page 42 for recommendations relating to references.

2.3.4 League tables of sickness absences of individual workers should not be published because the intrusion of privacy in doing so would be disproportionate to any managerial benefit. It is permissible for a manager to access the record of an individual's sickness in order to investigate repeated or long-term absence. It is also permissible to publish totals of sickness absence by department or section provided that individual workers are not identifiable.

2.4 Pension and insurance schemes

2.4.1 Care must be taken to ensure that information legitimately required in connection with the administration of the scheme is not made available to the employer unless this is a necessary consequence of the funding or other arrangements of the scheme. Mechanisms can be put in place to ensure this. For example, information, perhaps about medical or pensions history, passed from workers to a scheme administrator via the employer could be provided in a sealed envelope so that it remains confidential.

2.4.2 An employer's funding of a pension or insurance scheme does not give the employer the right to receive information about individual workers who are members of the scheme unless this is necessary for the operation of the scheme, e.g. to enable the employer to deduct contributions from pay or to decide whether to continue funding. This does not prevent the provision of anonymised, statistical information which should be used wherever possible. Some employers insure their businesses against sickness by key workers. If, as is likely, the insurer requires information about the worker's sickness in the event of a claim and the employer supplies this, one of the sensitive data conditions must be satisfied.

See page 72 for conditions to be satisfied

2.4.3 Although the trustees or administrators may in some cases be workers or directors, information that they receive in their capacity as trustees or administrators of the pension scheme should not be used in relation to general employment issues. For example, a medical report on a new worker that is needed because he or she has applied to join the employer's pension scheme may not be used in connection with decisions about the worker's eligibility for sick pay.

2.4.4 Whilst there is no obvious reason why an employer should require access to medical information in connection with private medical insurance, the same is not necessarily true of permanent health insurance. If a worker becomes unfit for work and makes a claim, the insurer might justifiably approach the employer to determine whether suitable alternative work is available. This could involve the disclosure of some health information. In such cases notify the worker concerned about the disclosure and make the information available to the worker on request.

2.4.5 This may require an explanation of how the funding obligations for the scheme fall on the parties involved.

2.5 Equal opportunities monitoring

2.5.1 The sensitive data conditions should mean that most equal opportunities monitoring can take place without the need to obtain a worker's consent.

See page 72 for conditions to be satisfied.

2.5.2 Effective equal opportunities monitoring may mean employers have to keep records about workers' backgrounds and their work history in a form that identifies them. For example, if your organisation wants to track how many workers with disabilities are being promoted and to what grades, it is difficult to see how this can be done without keeping records in a form that identifies them. Where tracking of individuals is involved it will not always be possible to use only anonymised information. However, where the employer only wants to monitor the proportion of external candidates with particular characteristics that apply for jobs, this alone will not justify the keeping of information about unsuccessful candidates in a form that identifies them. Although the removal of identifying details, e.g. name, may assist the protection of privacy, records will not be truly anonymous if they can still be linked back to individual workers, for example by putting serial numbers on anonymous' questionnaires but keeping a list of which worker was given a particular questionnaire. Do not give workers the impression that information about them is anonymised unless this is truly the case.

2.5.3 Employers should take account of the advice of relevant bodies before designing, distributing, collating and evaluating an equal opportunities monitoring initiative and incorporating it into procedures. Public sector employers will also need to take into account the requirements of the Race Relations Act 1976 (Statutory Duties) Order 2001 and the Race Relations (Amendment) Act 2000. Advice about the forms, procedures and ethnic grouping categories to be used in equal opportunities monitoring are available from bodies such as the Commission for Racial Equality, the Equal Opportunities Commission and the Disability Rights Commission.

See Useful Addresses page 83 for details.

For example do not limit the range of choices of ethnic origin to such an extent that individuals are forced to make a choice that does not properly describe their ethnic origin. Employers should consider carefully precisely what they are trying to monitor and should not collect unnecessarily detailed information about workers' nationality or linguistic group. Again, they should seek advice from bodies such as the Commission for Racial Equality about this. If monitoring involves the employer assigning workers to categories, perhaps in the case of those who decline to assign themselves, the record must make clear, whenever information is extracted, that the categorisation is merely the employer's assumption and is not a matter of fact.

2.6 Marketing

2.6.1 Some employers distribute marketing material to their workers. They may market their own products or services, or those of other organisations such as insurance companies and charities which they believe might be of interest to their workers. Workers have a right not to have their personal information used for this purpose.

If your organisation uses workers' details for advertising or marketing you should explain this fully at the outset, making clear what personal details will be used. You should give workers a clear opportunity to object and respect any objections. An objection might be received, for example, in response to a human resources department telling workers that there is an intention to market to them unless they object. This arrangement is often described as offering an opt-out'. The worker's right to prevent information about him or her being used for marketing does not just apply to the marketing of products or services, but also to marketing or advertising in a broader sense, such as the promotion of another organisation's aims and ideals.

2.6.2 The disclosure to another organisation of workers' details for marketing requires express approval from each individual, for example by the worker sending an e-mail to the human resources department indicating agreement. This is often described as an opt-in'. It would arise, for example, where a company wants to pass workers' home addresses to a sister organisation so it can market them with its products. The positive indication of consent is required because the disclosure of workers' information is intrusive and could amount to a breach of the employer's duty of confidence unless consent is obtained.

2.6.3 This benchmark applies equally to former workers such as pensioners whose details are still kept for payroll purposes, if their details are to be used for marketing. An opt-in' will not be needed if the new use of workers' details is likely to be expected by them. For example, if the offering of discounts on your products and services to workers is accepted practice within the industry concerned it may well be that they would expect to receive details of such offers personally addressed to them.

2.7 Fraud detection

2.7.1 There is no obligation to set up representative bodies where they do not already exist, nor is consultation on data matching mandatory under employment law. However, consultation provides an opportunity to identify and address data protection risks and concerns, helping to ensure that the data matching is fair to the workers concerned.

2.7.2 This information could for example be included in a fact-sheet for workers or other arrangements adopted to meet the recommendations earlier in the Code.

See Part 2 Employment Records, page 30 Collecting and Keeping General Records for benchmarks on informing workers.

2.7.3 The fact that disclosure of information may be required by law does not remove the obligation to inform workers. This is only removed if informing workers would be likely to prejudice the prevention or detection of crime, for example by amounting to a tip off' to the worker that he or she is under investigation for suspected fraud.

2.8 Workers' access to information about themselves

2.8.1 This is linked closely to the recommendations in the section on Managing Data Protection. A subject access request need not mention the Data Protection Act. When a worker makes a written request to an employer for access to information about him or her, this should be recognised as a subject access request and handled accordingly. Unless the employer knows what personal information is held about workers and who is responsible for the information, it will be difficult to fully respond to subject access requests. It may be necessary to carry out some form of audit to find out what information about workers is held. There should then be a system for ensuring all relevant information is located and provided in the event of a request being made. An employer can however ask a worker making an access request for information to help it locate the information about the worker, for example by asking when were you employed by us and in which department?

2.8.2 Making a false subject access request is one method that can be used by those trying to get access to information about workers to which they are not entitled.

See Part 2 Employment Records, page 43 Disclosure Requests, for more information about this.

2.8.3 The employer must provide a copy of the subject access information in a permanent form unless providing it in that form would involve disproportionate effort. Even if disproportionate effort would be involved in providing a copy, the employer must still give access to the record, perhaps by allowing the worker to inspect it. The Act does not define disproportionate effort'. Matters to be taken into account include the cost, the length of time it would take, the difficulty of providing the information, and also the size of the organisation to which the request has been made. These factors have to be balanced against the impact on the individual of not providing a copy. Given the significance of employment records, an employer should only rely on the disproportionate effort exemption from providing a copy in exceptional circumstances.

One area that can cause employers difficulties is access to e-mail. Workers are entitled, under subject access, to copies of the information in e-mails that is about them. Employers are not though required to search through all e-mail records merely on the off-chance that somewhere there might be a message that mentions the worker who has made the request. For information to fall within the Data Protection Act's subject access provisions, the worker must be the focus of the information and the information must affect the worker's privacy. This means, for example, that an e-mail about a worker's conduct or performance must be provided. However, an e-mail that merely mentions a worker, perhaps because his or her name appears on the e-mail's address list, need not be provided. Employers should check wherever there is some likelihood that messages might exist, for example in the mail box of the worker's manager. In doing so they should take into account any details the worker has provided to assist them in locating the information about him or her.

Detailed guidance about subject access is available in the Data Protection: Your Information Rights' section of the Information Commissioner's website at www.informationcommissioner.gov.uk

It is sometimes asked whether an employer will be a data controller for personal e-mail messages held on its system. If it is not a data controller for such messages it does not have to provide access to them. Employers will though usually be data controllers for all e-mail messages held on their systems. This is because they will keep at least some control over how and why messages are processed, for example by restricting the purposes for which workers can send personal e-mails or by retaining or monitoring personal e-mails to ensure the security of their systems.

Employers are free to agree alternatives to formal subject access with workers, but no pressure should be put on workers not to make or to withdraw subject access requests. For example, a worker might agree to withdraw a formal request if the employer provides particular information, about which the worker is concerned, free of charge. However if the worker proceeds with a formal request the employer must provide a full response.

2.8.4 Information released to a worker could include information that identifies another person, for example a fellow worker. This other person is referred to as a third party'. Responding fully to a subject access request could lead to the third party's rights under the Act being violated. One example is when a complaint is received about a worker and releasing information on the complaint, in its entirety, would identify the complainant to the worker. In many cases simply removing the third party's name from the information before it is released to the worker will solve the problem. However this will not always be the case. Sometimes the worker might be able to work out the third party's identity from the information itself, for example only X could possibly have written that about me'. The employer has to strike a balance between the right of the worker to access and the right of the third party to privacy. Before releasing information to the worker the organisation should follow a clear decision-making process to ensure it gets the balance right.

See page 40 for the process to follow for access when information about third parties is involved.

2.8.5 No further guidance on this recommendation.

2.8.6 Such automated systems are most common in recruitment exercises. 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. Workers have a right, under the Act, to know the logic behind any such automated decision. Either a separate request can be made for which a fee of £10 can be charged, or, if specifically stated, the request can be included in a more general subject access request.

See Part 1 - Recruitment and Selection, page 20 for more information on the use of automated selection methods.

2.8.7 Responsibility for responding fully to a subject access request rests with the employer rather than the systems supplier. An employer cannot blame the shortcomings of the system it uses, or a lack of information provided by the systems supplier, as a defence for its failure to respond properly to a subject access request.

2.9 References

2.9.1 It is in the employer's interest to make clear to staff the limits it places on their authority to give corporate references. Good indicators of whether a reference has been given in a corporate capacity are whether it is written on corporate headed notepaper and whether the referee provides his or her job title. If there is no company policy on the giving of corporate / personal references, the assumption should be that, in the absence of evidence to the contrary, references given from the workplace are given on behalf of the organisation.

Where confidential corporate references are given by the employer, an exemption in the Act allows the employer to deny workers access to these. Employers should decide and make clear to those providing corporate references whether they take advantage of this exemption or whether they adopt a policy of openness. In deciding the approach to take bear in mind that good data protection practice is to be as open as possible with workers about information which relates to them. Workers should be able to challenge information that they consider to be inaccurate or misleading, particularly when, as in the case of a reference, this may have an adverse impact on them.

It should be noted that in any case this exemption only applies to corporate references given by the employer. It does not cover references provided by one part of the employer's business to another, as might be the case when a worker seeks a transfer between departments. Access to such internal references should be treated in the same way as access to other information the employer keeps about the worker.

2.9.2 The provision of references on workers is common practice but they do contain personal information, often of a private nature. Employers should therefore be sure that the worker is content for a reference to be provided. Requests that are clearly from reputable businesses and that request that the reference is returned to a recognised address can generally be taken at face value, but if there are any doubts the employer should check with the worker. It is a criminal offence under the Data Protection Act to use deception to obtain personal data, such as might be included in a reference, where the data controller would not have agreed to the disclosure involved.

Employers should, where it is practicable, clarify the expectations of workers who leave. If a worker wants references to be provided in future the employer should still make sure that those requesting references are genuine and are not attempting to obtain information about the worker by deception.

2.9.3 The information released to a worker could include information that identifies another person, for example the author of the reference. This other person is referred to as a third party'. Responding fully to an access request could lead to the third party's rights under the Act being violated.

See page 40 for the process to follow for access when information about third parties is involved.

2.10 Disclosure requests

2.10.1 Junior or inexperienced staff should not be left to make difficult decisions about disclosure without guidance. A policy should be established. This does not need to be lengthy or complex but should set out some basic rules for staff who are likely to receive requests.

2.10.2 Ensure that unusual requests not covered by the disclosure policy are forwarded to those who have a proper grasp of the legal issues involved.

2.10.3 There are a number of legal obligations placed on employers to disclose information about their workers. Where you are under such an obligation, the disclosure must be made. However, prior to disclosing you should satisfy yourself that there is in fact a duty to disclose and should avoid disclosing more information than you are legally obliged to. Even if you are legally required to disclose information about a worker, the worker should still be told, where practicable, about the disclosure, for example what information is being disclosed, who to and why.

The most common sources of requests for disclosure that employers are legally required to comply with come from;

- the Inland Revenue
- the Child Support Agency
- the Benefits Agency
- the Department of Work and Pensions
- the Financial Services Authority.

In some cases you will not be under a legal obligation to disclose but you will be able to rely on an exemption in the Data Protection Act if you choose to do so. This is most likely to arise in the case of criminal or tax investigations or where it is necessary for you to disclose to obtain legal advice or in the course of legal proceedings such as an employment tribunal. In such cases provided sensitive information is not involved, it is clear the Act will not stand in the way of disclosure. You should still take a balanced decision whether to disclose taking into account the interests of the worker. If the information requested is confidential, for example information about sickness or earnings, only disclose if you have obtained the worker's consent or you are satisfied the public interest served by disclosure is sufficiently strong to justify the breach of confidence.

See page 43 for details of the exemptions from the non-disclosure provisions of the Act.

In other cases you risk a breach of the Act if you disclose. Where it is reasonable to do so inform the worker about the request for disclosure and take account of any objection. If the information that you intend to disclose includes sensitive data you should be sure that the disclosure satisfies a sensitive data condition. If confidential information is involved you should not disclose if there is an objection. If the information is not confidential, for example dates of employment, position employed in, still only disclose if in all the circumstances you

are satisfied that it is fair to do so. This can be a difficult decision but you should remember that you must mainly consider what is fair to the worker. If it is not reasonable or not possible to contact the worker and they have not indicated their consent to disclosure in any way, you should not disclose confidential information unless it is clearly in the worker's interest that you do so. With non-confidential information still only disclose if in all the circumstances, including in particular what the worker's view would be likely to be, you are satisfied that it is fair to do so.

See page 72 for details of the sensitive data conditions.

2.10.4 Even in apparent emergencies care should be taken to protect the interests of workers whose information might be disclosed. How urgent is the situation? Is it a matter of life and death? In many cases there is, for example, no reason why requests cannot be submitted in writing given the wide availability of fax and e-mail facilities.

2.10.5 Always establish the identity and authority of the person making a request for disclosure before providing any information about workers. Those seeking disclosure, particularly on the telephone, are often persuasive. Approaches to an employer are a favourite route for those trying to get access to information to which they are not entitled e.g. debt collectors, private investigators, recruitment agencies or journalists. Employers should be aware that people requesting information might use deceit, for example by pretending to be from the Inland Revenue, and should guard against this. They should also be aware that sometimes officials, perhaps from government department, may not fully understand their own powers to demand information. They may mistakenly tell an employer it is required by law to disclose information about workers when this is not the case. Where practicable, obtain the request in writing. Take particular care with telephone requests, for example by calling back to a known number. In particular,

- establish the authority, if any, of the person making a request. If this is not clear, seek further information from the person concerned.
- inform the Commissioner where requests based on deception are detected and there appears to be a reasonable prospect of obtaining evidence as to who is behind the deception.
- where those requesting information maintain that the employer is under a legal obligation to respond, ensure that the request is received in writing and spells out the basis on which the legal obligation is asserted. Check that any assertion they make is valid and that the law is not being misrepresented.

2.10.6 The Act imposes restrictions on the transfer of personal information to countries outside the EEA. Countries in the EEA are the member states of the European Union together with Iceland, Norway and Liechtenstein. The Information Commissioner provides separate detailed guidance on international transfers. The European Commission provides both a model contract that can be used to legitimise a transfer outside the EEA and a list of countries outside the EEA that are deemed to provide adequate protection by virtue of their data protection law. The European Commission has also entered into a special arrangement with the USA known as the safe harbor'.

See the Information Commissioner's website: www.informationcommissioner.gov.uk: Data Protection: Your Legal Obligations: International transfers.
The European Commission website is at
www.europa.eu.int/comm/internal_market/privacy/index_en.htm

2.10.7 A non-regular disclosure would be one where a one-off enquiry is received about an individual worker, perhaps from the Inland Revenue or a local authority housing benefits department. It would not include, for example, information on tax deductions supplied regularly to the Inland Revenue on all workers or the regular passing of information to a trade union on subscriptions deducted from pay for its members.

Where there is a non-regular disclosure, even one required by law, and the information that is to be or has been disclosed might be challenged by the worker, make a copy available to the worker and give the worker an opportunity to check its accuracy. Even if the accuracy of the information is not in doubt it may well be helpful to the worker to know that a disclosure of information about him or her has been made, for example to the Child Support Agency. There will though be cases, for example an enquiry from the Inland Revenue seeking confirmation of tax deducted, where the employer might reasonably conclude that to specifically inform the worker would involve disproportionate effort.

2.10.8 Where non-regular disclosures are made, a record should be kept so that those making the disclosures are accountable for their actions and so that any security breaches can be traced and remedied. The record should include details of the person who made the disclosure, the person who authorised it, the person requesting the disclosure, the reasons for the disclosure, the information disclosed and the date and time. This record can be incorporated into an automated system or be held manually.

2.11 Publication and other disclosures

2.11.1 Publication of information about workers commonly arises as part of the publication of information about a business, for example, in an annual report or marketing material. It may for example be expected by academic staff that information about their fields of expertise and research interests will be widely published, including on the internet. On the other hand, many workers would not expect any information identifying them to be published.

There are some legal obligations to publish information about individual workers, for example in company annual reports. Where there is no legal obligation to do so, only publish information about workers if;

- the information is not intrusive, for example information about a worker's job title, field of expertise or direct dial work telephone number, and taking into account the nature of the employer's business and the position held by the worker, either:-
  - publication would be expected or
  - if publication might not be expected it is nevertheless reasonable, workers have been informed in advance and any reasonable objections have been respected, or

- the worker has consented, or
- the information is in a statistical or other form that does not identify individual workers.

2.11.2 If information about workers is published on the basis of consent, ensure that when the worker gives consent he or she is aware of the extent of information that will be published and how it will be published, including whether the information will be published on a web site and the implications of this. Ensure too that if consent is being relied on, the worker is genuinely free not to consent to the publication.

2.11.3 Personal information about a worker can also be disclosed to a trade union where there is consent for this.

2.11.4 There is no obvious reason why in the course of collective bargaining a trade union need be provided with information from which individual workers can be identified. Aggregated or statistical information should suffice.

2.12 Merger, acquisition and re-organisation

2.12.1 Wherever practicable, information from which individual workers cannot be identified should be used, so details such as names and individual job titles should be omitted. This might be possible where, for example, a company merely wants to know how many workers of a particular type are employed and their average rates of pay. In other cases a company might require detailed information about particular workers in order to appraise a company's human resources assets properly. This might be the case where the expertise or reputation of individual workers has a significant bearing on the value of the company. Similarly where a company has a significant liability, perhaps as the result of a worker's outstanding legal claim, it may have to disclose information identifying the worker with details of the company's liability.

In some cases even the removal of names from the information will not prevent identification, for example where without a name it is still obvious that the information relates to a particular senior manager. Removal of names may nevertheless help protect privacy, even if identification is still possible.

Remember that handing over sickness records will entail the processing of sensitive personal data (see page 72).

2.12.2 It is important to gain formal assurances about how the information will be used. Information should be returned or destroyed by the shredding of paper or the expunging of electronic files, should the merger or acquisition not go ahead. The provision of information is sometimes achieved by the use of a data room' in which information about the business is made available to prospective purchasers. Strict conditions must be accepted by those granted access to the data room'.

2.12.3 Businesses may not always expect to be involved in mergers acquisitions, or re-organisations and may not therefore have told their workers, at the time they were recruited, what would happen to their personal information in such an event. Reasons of

commercial confidentiality and legal duties relating to matters such as insider trading' may make it difficult to be explicit at the time the merger or acquisition is being considered. In some circumstances the corporate finance exemption in the Act may be relevant and may relieve companies of the obligation to inform workers of the disclosure of their information. This could occur, for example, where providing an explanation to workers could affect the price of a company's shares or other financial instruments.

One business may also be under a legal obligation to disclose to another. Where there is a legal obligation to disclose, there is an exemption from some of the provisions of the Act. The employer is relieved of the obligation to inform workers of the disclosure if this would be inconsistent with the disclosure, perhaps because it would breach commercial confidentiality.

The processing of sensitive personal information involved in a disclosure related to an acquisition or merger must satisfy a sensitive data condition. This will not be an obstacle where there is an employment related legal obligation on one business to disclose to another, but may well prevent the disclosure of sensitive personal information in the run up to a merger or acquisition where there is no such obligation and the worker has not been asked for and given explicit consent.

See page 72 for conditions to be satisfied.

2.12.4 The Act imposes restrictions on the transfer of personal information to countries outside the EEA. Countries in the EEA are the member states of the European Union together with Iceland, Norway and Liechtenstein. The Information Commissioner provides separate detailed guidance on international transfers The European Commission provides both a model contract that can be used to legitimise a transfer outside the EEA and a list of countries outside the EEA that are deemed to provide adequate protection by virtue of their data protection law. The European Commission has also entered into a special arrangement with the USA known as the safe harbor'.

See the Information Commissioner's website: www.informationcommissioner.gov.uk: Data Protection: Your Legal Obligations: International Transfers.
The European Commission website is at
www.europa.eu.int/comm/internal_market/privacy/index_en.htm

2.12.5 It is the new employer who now has a responsibility for the type and extent of personal information retained and who will have liability for it under the Act. The new employer must not assume that the personal information it receives from the original employer is accurate or relevant and not excessive in relation to its purposes. Within a few months of the merger or takeover it should review the records it has acquired, for example by checking the accuracy of a sample of records with the workers concerned and should make any necessary amendments.

2.13 Discipline, grievance and dismissal

2.13.1 The activity of disciplining or dismissing workers or the handling of their grievances will often involve the processing of personal information such as the consultation of records or the compilation of dossiers of information about those involved.

The Act applies to this personal information. This means that;

- subject access rights apply, even when responding to a request might impact on a disciplinary investigation or on forthcoming proceedings. Access rights also apply to opinions expressed about workers and to information indicating the employer's intentions in respect of them. Access need not be provided if doing so would prejudice the investigation of criminal matters.

  See page 42 for details of the exemptions from subject access.

- personal information to be used as evidence to support disciplinary proceedings must not be obtained by deception or by misleading those from whom it is obtained as to why it is required or how it will be used.
- records used in the course of disciplinary and grievance proceedings must be accurate and sufficiently detailed to support any conclusions that are drawn from them.
- records relating to disciplinary and grievance investigations, proceedings and action must be kept secure. Be particularly careful that such records are only made available to those staff whose duties require that they should have access to them. Where information is to be provided to a worker's representative or legal advisor, check that this person has been authorised by the worker to act on his or her behalf.
- records of allegations about workers that have been investigated and found to be without substance should not normally be retained once an investigation has been completed. There are some exceptions to this where for its own protection the employer has to keep a limited record that an allegation was received and investigated, for example where the allegation relates to abuse and the worker is employed to work with children or other vulnerable individuals. There may also be a case for keeping records of unsubstantiated allegations of bullying or abuse of workers by a colleague, provided that it is made clear in the record what is an unsubstantiated allegation and what has been established as fact.

2.13.2 Information about workers must not be used in a way that is incompatible with the purpose(s) for which the information was obtained. For example, a worker in a business that issues credit cards might also be a holder of one of the business's cards. The business should not access information it obtains about the worker because he or she is a card holder, for use in connection with disciplinary or grievance investigations arising from his or her employment. Similarly, an employer might store e-mail messages for a limited period to ensure the security of its communications system. It must not access stored, personal messages sent by or to workers for incompatible purposes such as checking whether workers have been making adverse comments about their managers. A purpose will not be incompatible if workers have been told in advance that information obtained from them will be used for that purpose. Where the use of information about workers in disciplinary or grievance investigations is not incompatible, it must still be fair.

Personal information about workers should not be accessed if the intrusion into workers' privacy would be out of proportion to the seriousness of the matter under investigation.

For example, an employer storing e-mail messages might suspect that within a group of workers there is someone who has been spending too long conducting personal business in the employer's time. Accessing the content of all messages, including private and personal ones, sent by all members of the group is unlikely to be justified simply on the basis of tracking down the culprit even if workers have been told their messages might be accessed in the course of disciplinary investigations. This is because the nature of the offence would not justify the degree and extent of the intrusion, particularly given the availability of other less intrusive means of enforcing any rules the employer might have. On the other hand, accessing the personal e-mails of one particular worker where there is evidence that the worker has been using e-mail messages to racially or sexually harass another worker might well be justified.

See Part 3: Monitoring Workers pages 64 and 56 for recommendations relating to monitoring workers' e-mail and guidance on how to assess whether an intrusion is proportionate.

2.13.3 Disciplinary procedures generally provide for warnings to expire after a set period of time. Ensure the procedure clarifies what is meant by expire . For example, is the warning removed from the record or is it simply disregarded in determining a future disciplinary penalty? Put in place arrangements, such as a diary system, to ensure that the procedure is put into practice and that where the procedure provides for warnings to be removed or deleted, that this is actually done.

2.13.4 A breach of the Act's requirement of accuracy could arise, for example, where a worker has been allowed to resign but, because he or she has been left with little choice, the employer has recorded dismissed . Particular care should be taken in distinguishing resignation from dismissal.

2.14 Outsourcing data processing

2.14.1 Frequently, organisations do not process all the information they hold on workers themselves but outsource this to other organisations. Organisations which process the information on behalf of other organisations include specialist businesses which run payroll systems, sister companies which manage the centralised computer system on which group worker records are kept, and organisations which provide a secure facility for the storage of archived manual records. Such organisations are termed data processors'.

Where an employer outsources a service to a data processor, it falls to the employer to ensure that the data processor puts in place appropriate technical and organisational security measures. The employer must also take reasonable steps to ensure the processor complies with these measures. In deciding what are appropriate security measures, account must be taken of the nature of the information being processed and the harm that might result from a security breach.

In terms of practical steps the obligations on the employer might involve checking whether a potential data processor is certified to BS7799, and/or putting clauses in a contract to give the employer access to the data processor's audit or security reports. It may also

mean visiting the data processor periodically to check that the service that has been outsourced is being provided securely. The aim is to ensure that once personal information has been handed over to a data processor, it is no less well protected than it would have had to have been were it to have remained with the employer.

BS7799: 1995 Code of Practice for Information Security Management can be obtained from the BSI (British Standards Institution), ISBN: 580236420.

See page 83 Useful Addresses for BSI.

2.14.2 There must be a written contract in place between the employer and the data processor, or at least evidence in writing that there is such a contract.

2.14.3 The Act imposes restrictions on the transfer of personal information to countries outside the EEA. Countries in the EEA are the member states of the European Union together with Iceland, Norway and Liechtenstein. The Information Commissioner provides separate detailed guidance on international transfers. The European Commission provides both a model contract that can be used to legitimise a transfer outside the EEA and a list of countries outside the EEA that are deemed to provide adequate protection by virtue of their data protection law. The European Commission has also entered into a special arrangement with the USA known as the safe harbor'.

See the Information Commissioner's website: www.informationcommissioner.gov.uk Data Protection: Your Legal Obligations: International transfers.
The European Commission website is at www.europa.eu.int/comm/internal_market/privacy/index_en.htm

2.15 Retention of records

2.15.1 It falls primarily to the employer to set retention periods. No specific period is given in the Act, which merely requires that the personal information 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 professional guidelines.

In setting retention times employers must ensure that personal information is not kept for longer than is necessary but equally that it is not deleted where there is a real business need to retain it. Retention times may therefore vary from one employer to another depending on the use of the employer makes of particular types of information. For example, the need for retention of records for health and safety purposes is likely to be different in the case of those working with hazardous substances to those working in an office environment.

Base standard retention times on a clearly established business need for retention. Take into account any relevant professional guidelines and observe any statutory requirement to retain records. In particular:

- bear in mind that information should not be retained simply on the basis that it might come in useful one day without any clear view of when or why;
- establish how often particular categories of information are actually accessed after, say, 2,3,4 or 5 years;

- adopt a risk analysis' approach to retention by considering what realistically would be the consequences for your business, for workers and former workers and for others, should information that is accessed only very occasionally be no longer available;
- base any decision to retain a record on the principle of proportionality. This means, for example, that records about a very large number of workers should not be retained for a lengthy period on the off-chance that one of them might at some point question some aspect of his or her employment;
- treat items of information individually or in logical groupings. Do not decide to retain all the information in a record simply because there is a need to retain some of it.

Ensure that records are not kept beyond the standard retention time unless there is a business justification for doing so. With a computerised system this might be facilitated by the automated deletion or automatic flagging of information that is due for deletion. With paper files this is likely to involve the occasional weeding' of expired information, perhaps annually for current workers. As far as possible, structure systems to facilitate the retention policy, for example, by making sure that items of information with significantly different retention periods are not recorded on the same piece of paper.

The Chartered Institute of Personnel and Development (CIPD) has published a useful checklist of statutory and recommended retention periods for various classes of personnel documents. This is available on their website.

See page 84 Useful Addresses for the CIPD.

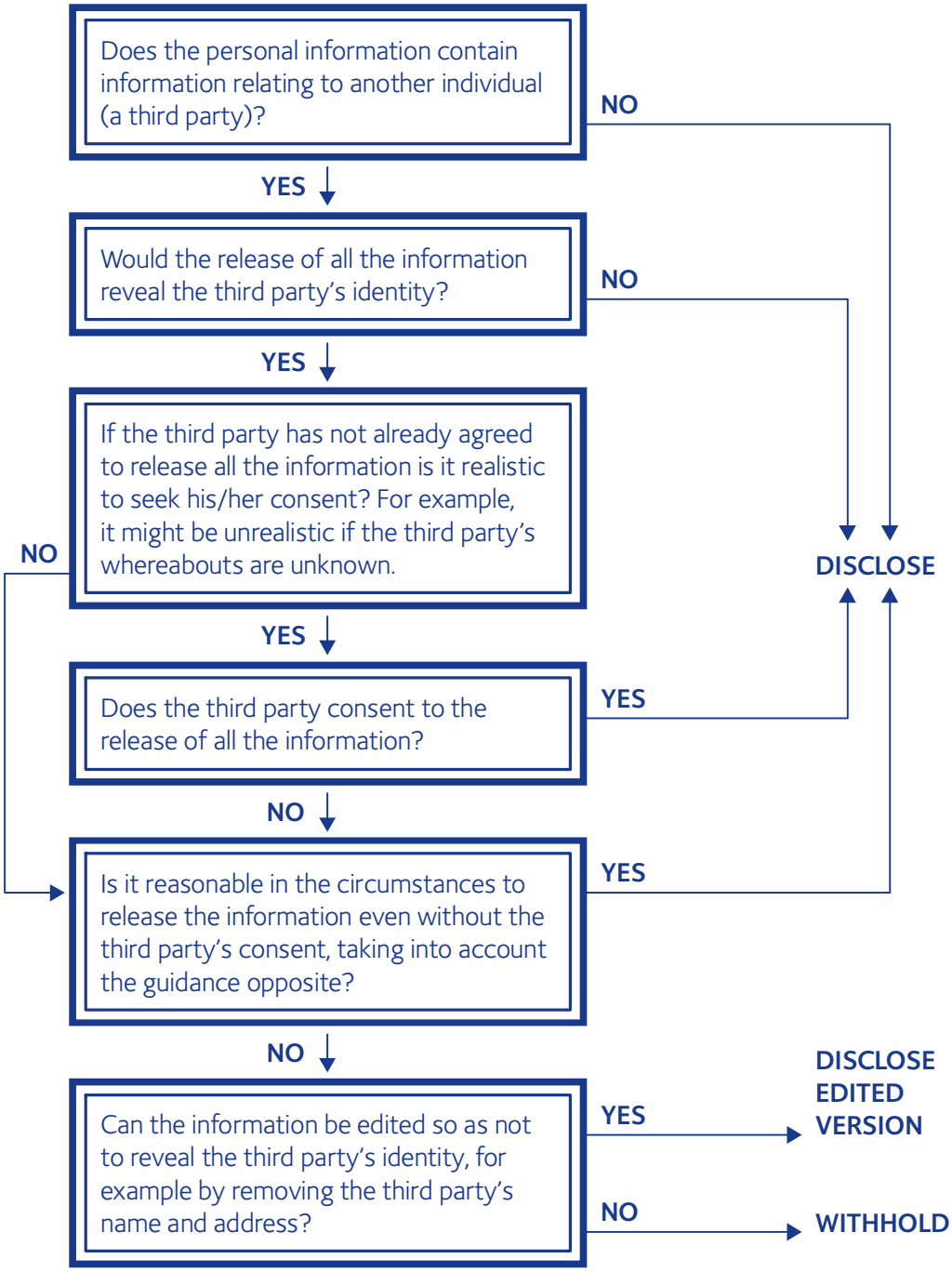
2.15.2 If records are maintained for management analysis, for example, to check the average period for which various grades of staff remain employed with a company, delete the information which enables particular individuals to be identified.

2.15.3 For example an employer might have a valid business reason for keeping information about the driving convictions of those who are employed to drive the employer's vehicles. However it is difficult to see any justification for retaining this information once the convictions become spent' under the provisions of the Rehabilitation of Offenders Act 1974. In exceptional circumstances which involve jobs covered by the Exceptions Order to this Act there might be a business need that justifies the continued retention of spent' convictions. An example might be the retention of information about a relevant criminal conviction of a worker who was employed to work with children and was dismissed because of the conviction. This would be held to ensure the worker is not reemployed in a similar role.

2.15.4 Take particular care to ensure that when computer records are deleted they are actually removed from the system. Copies of such records that might have been retained within the system, perhaps on a separate server, or as paper print-outs should be identified and also removed. Establish secure arrangements for the disposal of paper records containing sensitive or confidential information about workers, for example by having them shredded on-site or by a reputable contractor. Do not sell on computer equipment unless you are certain that any employment records have been completely removed. Simple deletion' will not necessarily achieve this.

Access when information about third parties is involved

The following diagram shows how to deal with subject access requests when the identity of a third party, i.e. a person other than the worker making the request, might be revealed within the personal information being released to the worker.



The employer must decide whether on balance the worker's right to know what information is held about him or her and its source outweighs the right to privacy of the third party who can be identified through releasing the information.

Factors to weigh in this balance include:-

- whether the information can easily be edited to remove the part that reveals the identity of a third party without significantly changing its likely value to the worker.
- whether releasing the information would breach a duty of confidence owed by the employer to the third party. (NB: When considering the release of references it is hard to see how releasing factual information about the worker such as his or her sickness record or allegations which have been or ought to have been put to him or her by an employer would breach such a duty.)
- whether the third party has expressly refused consent to release of the information and the reasons given, if any.
- what the third party was told when the information was supplied about its possible release or, if told nothing, what the third party's reasonable expectations would be. (NB: those asked to give references should not be led to believe and cannot expect that their references will be kept confidential in all circumstances. They may, for example, have to be released under disclosure procedures in the event of a claim of unlawful discrimination.)
- the impact the information has had or might have in the future on actions or decisions affecting the worker.
- the nature of the information, in particular whether its release could be damaging to the third party or whether it would reveal sensitive data about the third party.
- the extent to which the worker is likely to be aware already of the information.
- whether the information includes facts which the worker ought to be made aware of because he or she might dispute them.
- whether the information identifies the third party in a business or personal capacity. (NB: When considering the release of references the third party's right to privacy is greater if he or she is the author of a personal reference rather than of a corporate one).
- the fact that if information is released in error the error cannot subsequently be corrected, but if information is withheld the error can subsequently be corrected by its later release, perhaps on the order of the Information Commissioner or a court.

The Commissioner's view is that, where the information from which a third party can be identified consists of an employment reference received by the employer it should normally be released to the worker unless the referee provides some compelling reason as to why it should be edited or not released at all. If, in other cases, the release of such information would breach a duty of confidentiality owed by the employer to the third party, the information should only be released if its nature is such that it has had or is likely to have a significant adverse impact on the worker.

Exemptions from the subject access right

There are some exemptions from the subject access right which are particularly relevant to employment:

- information held for management forecasting or management planning, for example information about plans to promote, transfer or make a worker redundant, may be withheld to the extent to which access would be likely to prejudice conduct of the employer's business.
- information consisting of records of the intentions of the employer in relation to negotiations with a worker may be withheld to the extent to which access would be likely to prejudice those negotiations, for example because it would give away the employer's fall-back position'.
- information that consists of a reference given or to be given in confidence by the employer for;
  - the education, training or employment of the worker
  - the appointment of the worker to any office
  - the provision by the worker of any service

  may be withheld.
- information held for;
  - the prevention or detection of crime
  - the apprehension or prosecution of offenders
  - the assessment or collection of any tax or duty or of any other imposition of a similar nature

  may be withheld to the extent to which access would be likely to prejudice any of these matters.

There is also an exemption which applies in limited circumstances where releasing information could affect the price of a company's shares or other financial instrument. This is known as the corporate finance exemption.

In addition, information that identifies someone other than the worker can sometimes be withheld.

See Access when information about third parties is involved page 40 for further details.

Exemptions from non-disclosure

The general approach that employers should take to the disclosure of information about workers is that the information should not be disclosed unless after taking into account the worker's interests, there is a legitimate reason for doing so. The Act sets out a number of circumstances in which, provided sensitive data are not involved, it is clear that the Act will not stand in the way of disclosure. One is where the disclosure is required by law whether as a statutory requirement or in response to a court order. The others most relevant to employers are;

- where the disclosure is needed for legal proceedings or prospective proceedings or for obtaining legal advice.
- where a failure to disclose would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of tax.

For the second of these exemptions to apply there must be a substantial chance, rather than a mere risk, that the matters referred to would be noticeably damaged by a failure to disclose in the particular case in question. There is though no requirement that the police or other law enforcement agencies are necessarily involved.

Employers should be aware that the exemptions do not impose an obligation to disclose. They merely allow a disclosure to be made without the Act being breached. The choice remains with the employer even if, for example, a failure to disclose would prejudice police enquiries. A court order would be needed to impose an obligation to disclose. Where there is a statutory obligation to disclose, the disclosure must be made.

Supplementary Guidance

Part 3: Monitoring at Work

Good Practice Recommendations Part 3: Notes and Examples

3.1 The general approach to monitoring

3.1.1 There are risks that the Act will be breached if line managers institute monitoring of their workers without authority and without taking into account the provisions of this Code. Business practices should be designed to ensure that monitoring does not take place without careful consideration of the requirements of the Act and this Code.

3.1.2 No further guidance on this recommendation.

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

3.1.4 Workers who are subject to monitoring should be aware when it is being carried out, and why it is being carried out. Simply telling them that, for example, their e-mails may be monitored may not be sufficient. They should be left with a clear understanding of when information about them is likely to be obtained, why it is being obtained, how it will be used and who, if anyone, it will be disclosed to. The necessary information can be provided, for example, through signage in areas subject to monitoring or through details given in a staff handbook. Workers should be kept aware of existing monitoring, perhaps by reminding them periodically. Where significant changes to monitoring arrangements are introduced they should be told about these.

3.1.5 No further guidance on this recommendation.

3.1.6 Monitoring may involve others having access to personal information about workers. In some cases the information may be of a private nature, for example if monitoring extends to the content of e-mail messages. As far as possible such information should be excluded from monitoring. Where this is not possible and monitoring is nevertheless justified the numbers of those who have access to the information must be kept to a minimum. They must be subject to rules to ensure the information is kept securely, not misused or improperly disclosed. They should also be trained to understand the data protection principles that arise when carrying out monitoring. Monitoring may well be more intrusive if those who have access to private information are close colleagues or the manager of a worker. Therefore employers should take care to identify the most appropriate

person/people to undertake monitoring, for example for larger businesses this might be those with security or personnel responsibilities.

3.1.7 Personal information obtained for a particular purpose should not be used in a way that is incompatible with that purpose. If monitoring is justified on the basis of addressing a specific risk faced by the employer, the use of information to address a lesser risk, that on its own would not justify monitoring, should be avoided. It is in any case likely to be unfair to workers to tell them that the monitoring is undertaken for a particular purpose and then use the information for another purpose that they have not been told about unless it is clearly in the worker's interest to do this or the information reveals activity that no employer could reasonably be expected to ignore. The type of activities that an employer could not reasonably be expected to ignore might include criminal activity at work, gross misconduct or breaches of health and safety rules that jeopardise other workers.

3.1.8 Websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising or mis-keying. Workers should have the opportunity of explaining or challenging any information before action is taken against them. Systems malfunction can cause information collected through monitoring to be misleading or inaccurate. Information can also be misinterpreted or even deliberately falsified.

3.1.9 Many businesses buy monitoring systems off the shelf'. In such cases the business should make sure the system facilitates data protection compliance. In other cases appropriate system requirements should be specified. Particular care should be taken with suppliers from outside the EU who may not be used to working within the confines of data protection law. The legal responsibility for compliance rests clearly with users rather than suppliers of systems. Users cannot simply blame the system. The Information Commissioner does though recognise that it may take some time to bring existing systems up to the desired standards. He will take this into account should the possibility of enforcement action arise as a result of a breach of the Act.

If personal information about a worker is kept or collected by an employer for its purposes the information must be made available to the worker if an access request is made, unless an exemption applies. With e-mail or video monitoring this may be onerous, particularly if the system used does not store information in a way that makes any personal information readily retrievable. This is a factor employers should take into account in their impact assessment.

3.1.10 Sometimes a customer for a supplier's products or services may seek to impose a condition requiring the supplier to monitor its workers. For example a contractor working in a defence establishment may be required to undertake periodic security checks on those workers employed on the relevant contract. If this monitoring involves processing personal information about the workers it will not be justified simply because it is a condition of business. Such a condition cannot override the employer's obligation to comply with the Act. Monitoring of workers by the supplier or contractor must be based on the outcome of its own assessment. This does not stop the supplier or contractor being guided by any assessment the customer for its products or services might have undertaken for itself.

See Part 2, Employment Records, page 39 , Workers access to information about themselves' for more information.

3.2 Monitoring electronic communications

3.2.1 It is a fundamental requirement of data protection law that workers are aware of the monitoring. One way to achieve this is for the employer to establish, document and communicate a policy on the use of electronic communications systems. However workers will base their expectations of privacy not only on the employer's stated policy but also on its practice. For example, if the employer's policy imposes a ban on personal telephone calls but in practice the employer turns a blind eye' to a limited number of personal calls, the employer will not be able to depend on there being a complete ban as its justification for carrying out monitoring. The capabilities of electronic systems should be used to remind workers of their responsibilities. These can be set so that workers cannot proceed to access the internet or e-mail services without acknowledging the acceptance of certain conditions.

3.2.2 Except in limited circumstances that are unlikely to apply to the monitoring of communications by employers, interception, without the consent of sender and recipient, is against the law unless it is authorised by the Lawful Business Practice Regulations. This is the case for both public and private sector businesses. An interception occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. It therefore includes access to e-mails before they have been opened by the intended recipient, but does not include access to stored records of e-mails that have been received and opened. Bear in mind that in many cases, for example customer enquiries, the intended recipient of a communication will be the business itself rather than a specific individual. Monitoring of such incoming communications by the business will not involve an interception. There are though likely to be incoming communications, including but not limited to private ones, where the intended recipient is a specific individual. Monitoring that extends to the content of these before they have been opened by the intended recipient is likely to involve an interception.

See Page 58, on the Lawful Business Practice Regulations, for more information about this.

3.2.3 Where practicable limit monitoring to that necessary to ensure the security of the system, e.g. protection from intrusion and from malicious code such as viruses or Trojans, or detection of the misuse of passwords.

Take account, particularly in any impact assessment, of the ability of automated monitoring to reduce the extent to which extraneous information is made available to any person other than the parties to a communication. For example, monitoring to protect the security of a system can generally be automated. Monitoring to detect references to matters of particular sensitivity, for example the name of a company involved in a merger negotiation, might also be automated. Automated monitoring systems are becoming increasingly sophisticated and their capabilities should be exploited to assist data protection compliance, for example through the ability to target monitoring at suspicious patterns of activity.

3.2.4 Do not introduce monitoring or the recording of the content of calls in all cases. If recording is necessary to provide evidence of business transactions, e.g. in telephone banking, and it is undertaken only for this reason it will not be monitoring' within the scope of this part of the Code. Recording should though be limited to those calls involving, or likely to involve, transactions. Take into account, particularly in any impact assessment, the possibility that acceptable benefits might be achieved by the use of an itemised call record. If the itemised call record alone is insufficient, assess whether it can be used to help ensure that monitoring is strictly limited and targeted. For example, there might be evidence that commercial secrets are being passed to a competitor. By examining itemised call records it might be possible to narrow down those under suspicion and target monitoring accordingly.

See How Intrusive is Your Monitoring?' on page 56 for more information about this.

3.2.5 Although this Code of Practice is primarily concerned with information about workers rather than external callers, employers should bear in mind that monitoring workers will often involve collecting information about those people who make calls to or receive calls from the organisation as well as about workers themselves. Where monitoring goes beyond simply listening-in in real time on calls without recording them and so involves the processing of personal data, these people should also be told that monitoring is taking place and why. Unless it is self-evident that monitoring is taking place and why, provide this information, where reasonably practicable, through the use of recorded messages on telephone systems. Don't forget that those who might be making personal calls to workers are less likely to expect that their calls may be monitored, or to understand why, than, for example, customers who might expect some recording to take place. If there is no better way of providing information, instruct workers to inform callers that their calls may be recorded and to explain why this is the case.

3.2.6 Where employers pay for mobile phones which workers may use for personal calls or for land lines in their homes, they may receive itemised bills directly or via their workers. Employers should bear in mind that workers' expectations of privacy are likely to be significantly greater at home or outside the workplace than in the workplace. This distinction should be reflected in making an impact assessment. If bills are received directly, workers should be made aware of the extent of information about personal use received by the employer. In either case, information about personal calls should not be used for monitoring. It may be used for billing or in exceptional circumstances, where there is evidence of work related criminal activity, accessed as part of a specific investigation.

3.2.7 In an impact assessment of e-mail monitoring you should consider the following;

- Can analysis of e-mail traffic rather than monitoring the content of messages be used? If the traffic record alone is not sufficient, can the traffic record be used to narrow the scope of content monitoring, for example to restrict any examination of the content of messages to those that are being sent to a rival organisation?
- Is it feasible to use an automated monitoring and detection process that for example detects malicious code such as viruses or Trojans, or limits the size of attachments that can be received?

- Is there a risk that monitoring the content of messages will breach a duty of confidence owed to workers or customers?
- Are there secure lines of communication, for example for the transmission of sensitive information from the worker to an occupational health advisor or for trade union communications that will not be subject to monitoring? Some systems can be set up so that messages to and from particular individuals or sections of the organisation are not subject to monitoring or are monitored differently to others.
- Is there a system that allows workers to mark personal communications as such?
- What would be the implications of making adjustments to the system, for example to provide facilities that allow messages to be sent that do not bear the employer's official' heading? The provision of such facilities should reduce the risk of employers' liabilities in respect of personal e-mails sent using the employer's equipment.
- Can any monitoring be confined to external rather than internal e-mail messages? In some cases monitoring of internal messages might be more intrusive for workers whereas the benefits of monitoring might come mainly from external messages.
- Can e-mails that are marked personal, or which there are other grounds to believe are personal, be excluded from monitoring or treated differently? Apart from automated monitoring which rejects or returns unacceptable messages for security reasons messages that are personal should only be opened in exceptional circumstances, for example where a worker is suspected of using e-mail to harass other employees.
- Is there a ban on personal use of the e-mail system or a restriction on the types of messages that can be sent? Such a ban or restriction does not in itself justify the employer knowingly opening messages that are clearly personal. However an employer designing monitoring is entitled to work on the assumption that messages in the system are either all likely to be business ones or, if personal, are only likely to be of a particular type. If personal use is prohibited it may be possible to detect personal messages from the header or address information and take action against the sender or recipient without opening them.
- Are workers provided with a separate e-mail account or an encryption capability? Are they allowed access to web-based mail services for personal use?
- Are systems for recording information about e-mail use reliable? Employers should bear in mind that e-mails and associated records can be misleading or even falsified, and if cited in court could be challenged.

In an impact assessment of internet access monitoring you should consider the following;

- Can monitoring that prevents rather than detects misuse be used, for example by blocking access to inappropriate sites or material by using web-filtering software? Consider the capabilities of the latest technology, for example, products are available that, it is claimed, can undertake complex analysis of images and thereby prevent the display of sexually explicit material without disrupting normal business activity.
- Is it possible to prevent misuse of systems by recording the time spent accessing the internet rather by monitoring the sites visited or the contents viewed?

- Is it possible to limit the use of the information collected? For example, if the issue is that a worker has been spending too much time on the internet for purposes that are not work-related, is it necessary for the worker's manager to be told exactly what sites have been visited?
- Can private internet access be separated from business access, perhaps by having a different log-on for private use and then limiting the collection of information on private use to the length and time of the session?
- Can monitoring be done on an aggregated basis, for example examining logs of which sites have been accessed from which departments and only focussing on specific workers if it is apparent there is a problem?

See How Intrusive is Your Monitoring?' on page 56 for more information about this.

3.2.8 Accessing the contents of a worker's personal e-mails or other correspondence will be particularly intrusive. This should be avoided wherever possible. It is particularly important if the worker has a genuine expectation of privacy. This might be confined to e-mails where the words private' or personal' have been included in the message header if workers have been clearly instructed to mark personal e-mails in this way. If the content of personal e-mails is to be accessed, the employer must have a pressing business need to do so, e.g. grounds to suspect the worker of work-related criminal activity. This must be sufficient to justify the degree of intrusion involved and there must be no reasonable, less intrusive alternative. It is recommended that the impact assessment approach is used to determine whether this is the case. An employer is, of course, entitled to take into account anything workers may have been told about the likelihood and extent of monitoring in its assessment.

3.2.9 Monitoring external e-mails will mean processing information about those people who send e-mails to or receive e-mails from the organisation, as well as about workers. Unless it is self-evident, these people are also entitled to be told, where practicable, that monitoring is taking place and why. This may not be easy to achieve. Employers would not, for example, be expected to inform external senders of e-mails that messages will be virus checked even though this may involve processing their personal information. However, if information about external contacts is to be used in ways they would not expect, then they should be told. If e-mail responses are solicited, for example, when job applicants are asked to send in their applications by e-mail, it should be possible to provide any necessary information beforehand, for example in the job advertisement. If e-mails are unsolicited, the information could be provided in any response.

3.2.10 The purpose for doing this should be to ensure the business responds properly to its customers and other contacts during a worker's period of absence. Workers should be aware that communications addressed to them will be opened in their absence. Employers may wish to encourage the use of a marking system to help protect personal communications when the intended recipient is absent. Only in exceptional circumstances should e-mails that are clearly personal be opened, for example if the worker is suspected of using the employer's communication system to engage in criminal activity.

3.2.11 There are a variety of ways in which workers can be told about the retention of information about their e-mail or internet usage. This might be done by giving them an information pack addressing this when they are given access to the office's internet or e-mail systems, or by displaying on-line information on their computer. It is important to ensure that workers are aware of retention periods and, in particular, that they are not misled into believing that information will be either deleted or retained when this is not the case.

3.3 Video & audio monitoring

3.3.1 Continuous video or audio monitoring is particularly intrusive for workers. The two combined are even more intrusive. The circumstances in which continuous monitoring of individual workers is justified are likely to be rare, for example work in particularly hazardous environments such as refineries or nuclear power-stations, or where security is a particular issue, for example in the premises of a precious stone dealer. This is different from the security monitoring of public or semi-public areas where workers may pass from time to time, e.g. corridors or car-parks. Depending on how and why it is set up, such monitoring may not fall within the scope of this part of the Code. It is in any case much more likely to be justified, particularly if one of its purposes is to protect workers or their property.

In an impact assessment of video and/or audio monitoring you should consider the following;

- Can video and audio monitoring be targeted at areas of particular risk, for example where there is a risk to safety or security?
- Can monitoring be confined to areas where workers' expectations of privacy will in any case be low, for example areas to which the public have access?
- Can video and audio capability be treated separately?
- Will the employer be in a position to meet its obligations to provide subject access to and, to the extent that it might be necessary, remove information identifying third parties from audio and video recordings?

3.3.2 Employers carrying out monitoring should make it clear to workers that monitoring is taking place and where and why it is being carried out. This could be done by ensuring that in areas subject to monitoring, a prominent sign is displayed that identifies the organisation responsible for the monitoring and why is it being undertaken, and says who to contact regarding the monitoring. Simply telling workers that from time to time they may be subject to video or audio monitoring is not sufficient. A good rule of thumb for fairness is for the employer to consider whether workers, at the point at which they are subject to monitoring, would be aware that it is taking place. Although in limited circumstances the Data Protection Act allows for covert monitoring, for example where telling workers about the monitoring would be likely to prejudice the detection of crime, workers should normally be told clearly when monitoring is taking place.

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

3.4 Covert monitoring

3.4.1 Where the carrying out of monitoring results in the collection or other processing of personal information, those who are subject to it should be made aware that it is being carried out and why it is being carried out. The more intrusive the monitoring the more precise the information given to workers needs to be. Where video or audio monitoring takes place workers should have specific information such as the location of cameras or microphones. Where communications are monitored the information may be less specific but workers should know when to expect that information about them will be collected. In any other case the monitoring is likely to be covert.

Covert monitoring is monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place. Employers should ask themselves if the workers about whom they are collecting information would be likely to know the collection is taking place. If the answer is no', the monitoring will be covert. Covert monitoring may take place inside or outside the workplace. The covert watching of a worker by another person is not in itself subject to the Data Protection Act, but once it results in a record being kept about the worker, the Act will apply.

Covert monitoring will only be justified in a particular case if openness would be likely to prejudice the prevention or detection of crime or equivalent malpractice or the apprehension or prosecution of offenders. There may be cases where one of the other exemptions in the Act could apply, but these are unlikely to arise in the employment context. It is therefore essential that the employer makes a considered and realistic assessment of whether such prejudice is likely. A reliable test of whether covert monitoring is justified is to consider whether the activity being monitored is of sufficient seriousness that it would be reasonable for the police to be involved. This does not mean, though, that the employer need necessarily involve the police. However, the implications of covert monitoring are such that senior management authorisation ought to be a prerequisite.

3.4.2 No further guidance on this recommendation.

3.4.3 It is hard to see circumstances where an employer would be justified in installing secret video cameras or other covert monitoring devices in areas where workers would have a genuine and reasonable expectation of privacy. This would include toilets. It is also likely to include closed offices allocated to individual workers for their exclusive use, although the extent to which particular parts of the workplace can genuinely be regarded as private will vary from employer to employer. Whilst in exceptional circumstances covert monitoring in private areas might be justified, for example where there is evidence of drug-dealing on the premises, any such monitoring should take place with the intention of involving the police.

3.4.4 An employer does not avoid its obligations by engaging a private investigator or other agent to collect personal information about workers on its behalf. If an employer engages a private investigator to collect information covertly on workers the private investigator will be a data processor'. The employer retains responsibility for data protection compliance. This can be discharged through the contract the employer must have with the private investigator and under which data protection obligations must be placed on the investigator.

3.4.5 Limit the number of staff involved in covert monitoring and identify clearly who has authorisation to be involved. Clear rules should be set down limiting the disclosure of and access to personal information obtained. Information about workers who are not the target of the investigation should be deleted as soon as practicable. The type of activities that an employer could not reasonably be expected to ignore might include criminal activity, gross misconduct or practices that jeopardise the safety of others.

3.5 In-vehicle monitoring

3.5.1 In an impact assessment of monitoring of vehicles used by workers you should consider the following;

- Can the monitoring be conducted without yielding information that relates to the private use of vehicles? Information about the location of the vehicle will be the most intrusive.
- Is private use of vehicles supplied by, or on behalf of, the employer, allowed? Where private use of vehicles is allowed, monitoring their movement when used privately, without the freely given consent of the user, will rarely be justified. (Note: this means that if the vehicle is used for both private and business use there ought to be a privacy button' or other arrangement that enables the monitoring to be disabled. However where an employer is under a legal obligation to monitor the use of vehicles, even if used privately, for example by fitting a tachograph to a lorry, then the legal obligation will take precedence.)
- Is monitoring of workers' own vehicles to take place? Monitoring of such vehicles will only be justified where the vehicle is being used for business purposes, the worker has freely consented to the installation and use of any monitoring device, and the information collected by the employer is strictly necessary for its business purposes, for example to reimburse the worker for the cost of business use.

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

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

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

3.6 Monitoring through information from third parties

3.6.1 An impact assessment should be based on the presumption that workers are entitled to keep their private lives private and that employers should not intrude into this unless they face a real risk to which the intrusion is a proportionate response. As part of the

assessment, consider whether there is evidence that the monitoring is justified. For example, a worker's financial circumstances should not be monitored unless there are firm grounds on which to conclude that a worker in financial difficulties in the job in question actually poses a significant risk to the employer. One area where this might be the case is in some parts of the financial services industry where there are particular opportunities for fraud.

3.6.2 Workers can be told about the sources that will be used to carry out checks on them in a variety of ways. General information can be put in a staff handbook, displayed on a notice board or delivered on-line to workers with access to computer systems. However, where a specific check is to be carried out, the worker should be directly informed of this unless to do so would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

3.6.3 Section 55 of the Act makes it a criminal offence to obtain personal information without the authority of the data controller. Credit reference agencies hold a range of information about individuals. Some can only be used for credit decisions. An employer using a facility for employee monitoring that is provided to assist it in making credit decisions about customers is likely to be obtaining information without the authority of the agency.

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

3.6.4 Do not monitor workers through information you have as a result of a different relationship with them, e.g. as a customer or client, unless it is based on a condition of employment and the intrusion caused by the monitoring is justified by the risk faced. This is only likely to be so in special cases, for example a bank must not routinely monitor the bank accounts of all workers. If monitoring can be justified it must be targeted at particular individuals and particular information that poses a risk. For example monitoring to detect serious indebtedness by bank workers with a particular opportunity for fraud might be justified on the basis that preventative action can then be taken. This would not however justify examining the details of payments made by these workers unless criminal activity was suspected.

3.6.5 As with any worker records, steps should be taken to ensure the reliability of staff that have access to monitoring information. This is especially important where private or confidential information is likely to come into their hands. This is not simply a matter of carrying out background checks; it also involves instruction or training and ensuring that workers understand their responsibilities in respect of such information. Consider placing confidentiality clauses in the contracts of employment of relevant staff.

3.6.6 Once information has been obtained through monitoring and any necessary evaluation of this made, do not retain the information unless there is an overriding reason for doing so. Usually it will be sufficient to record that the evaluation has been carried out and its result. As a general rule, unless there is a legal or regulatory obligation to do so, the information should not be retained for more than 6 months. There might however be some exceptions, for example where the information has ongoing relevance to the placement of the worker, such as might be the case with an employment agency that routinely places its workers in a variety of short-term assignments with its clients.

How intrusive is your monitoring?

The table opposite gives guidance on the degree of intrusiveness involved in monitoring the content of various types of communication that are likely to take place in a typical workplace. It is intended to illustrate that the more personal the nature of the communication, the higher the threshold for monitoring it. The table should help employers to carry out the impact assessment referred to throughout this section of the Code.

Low Intrusiveness

Pure business communications

These are the types of communications that only deal with business matters. Typically they would include letters sent out on a business' headed paper or electronic equivalents. The communication contains no information of a particularly personal or intimate nature.

Example	Guidance on monitoring
1: An e-mail from a company accountant to a supplier querying why an invoice has been submitted for goods that have not been supplied. **2: Work contact details submitted by a health and safety officer to a website so that information about fire safety equipment can be returned.**	Disclosure of its contents would be unlikely to cause damage or distress to any worker. To the extent to which it is not obvious, it is sufficient that workers are aware in general terms that the work they do is likely to be monitored or checked. It is difficult to envisage how monitoring these communications could be considered to be a disproportionate infringement of privacy.

Business communications including personal information

These are communications taking place in the workplace that are clearly for genuine business reasons but contain information that is of a personal nature. Many personnel' type communications will fall into this category and in many instances the worker identified in this type of communication would object to the information being made widely available in the workplace.

Example	Guidance on monitoring
1: A report submitted by e-mail from a worker to a line manager requesting leave of absence from work because of serious sickness in the family. **2: A report submitted for a disciplinary hearing relating to a worker's alleged misconduct.**	A worker must not be misled into thinking that a communication is private if this is not the case. Whether monitoring these communications is a proportionate response will depend very much on the circumstances of the case. Those carrying out any monitoring should be clear on procedures and fully trained. They have responsibilities to ensure that information obtained through monitoring is kept secure, only used for the purpose for which it was obtained and is deleted once the purpose for carrying out the monitoring is complete.

Personal communications

This Code makes it clear that there is no obligation under the Act for employers to provide communications equipment for workers' own personal use. However, many employers choose to do this. Although employers may provide such facilities, they will need to manage any risks to the business arising from such usage. For example, a worker might use internet access facilities to download pornography in the workplace. It follows, therefore, that even where personal use of communications systems is allowed, there may be exceptional circumstances where monitoring is necessary. There will in any case be a need to check for malicious code to ensure security of the system.

Example	Guidance on monitoring
1: A worker visiting a patient support group website to seek advice on a condition not related to his or her employment. **2: An e-mail between two workers complaining to each other about how they are treated by their employer.**	These are circumstances in which workers might reasonably expect that their communications will be private, unless workers have been told clearly that monitoring will take place. Even if workers are told this, it will be intrusive and must be kept to the minimum necessary to address risks. A ban on personal communications does not in itself justify monitoring of the content of such communications. Such a ban and the existence of alternative facilities for personal communications are relevant factors but the monitoring must still be a proportionate response to the problem it seeks to address.

High Intrusiveness

Lawful business practice regulations

This section provides guidance to employers who wish to monitor electronic communications (e.g. telephone calls, fax transmissions, e-mails, internet access) on how they can meet the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations.). The RIPA and LBP Regulations cover a complex series of situations, of which monitoring in the workplace is only one. This guidance is designed to assist businesses, including public authorities, when they act as employers, but not in other situations. It is intended to cover all the main points but is necessarily simplified. It is not a complete statement of the law but employers following it are unlikely to find themselves on the wrong side of the law.

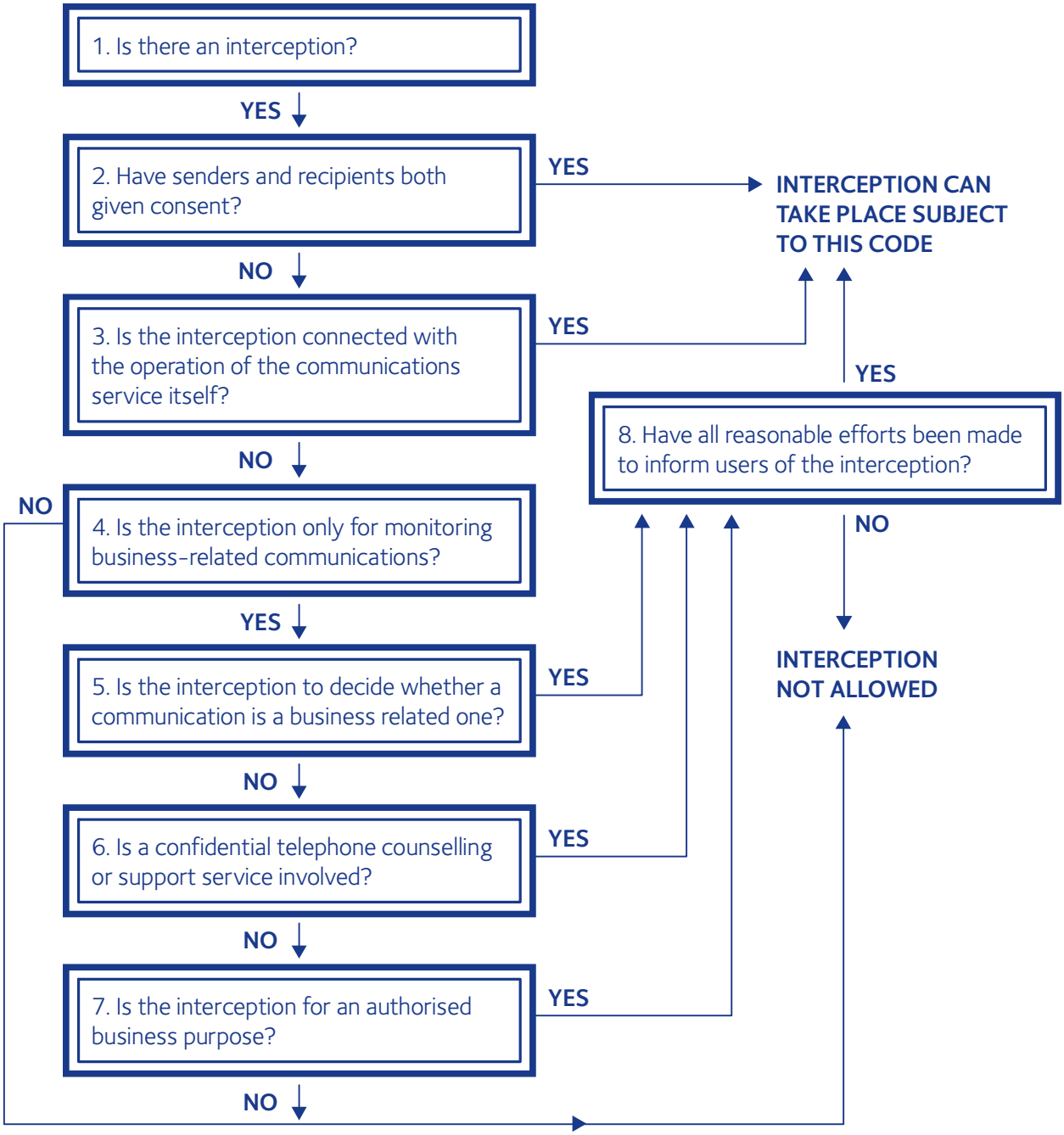
Under RIPA it is against the law for a business to intercept an electronic communication on its, or anyone else's, system. There are some exceptions. Most of the exceptions contained in RIPA itself are unlikely to apply to the monitoring of communications by employers, for example where an interception is authorised under a warrant. The RIPA exceptions that may be relevant are:

- where the interception takes place with consent
- where the interception is connected with the operation of the communications service itself.

In addition to the exceptions in RIPA itself, the Lawful Business Practice Regulations set out further exceptions where, in connection with the carrying on of a business, an interception will not contravene RIPA. These exceptions will be particularly relevant to employers. They set out the circumstances in which a business is authorised to carry out an interception for the purpose of running its business. The regulations are designed to meet the legitimate needs of businesses to manage their information systems, making use of the capabilities of modern communications technology, but in a way that is consistent with high standards of privacy. It must be remembered though that they are not exemptions from the Data Protection Act.

An interception of communications that does not come within the exceptions in the LBP Regulations or in RIPA itself is against the law. It is irrelevant whether or not the monitoring associated with the interception would satisfy the other provisions of this Code. On the other hand, if the interception does come within the exceptions, the monitoring cannot proceed regardless. The collection, storage, and use of personal information that is involved in the monitoring must still satisfy Data Protection requirements.

This diagram may assist employers in checking whether the requirements of RIPA and the LBP Regulations are met. Explanatory notes follow on the next page.



Explanatory notes

1. Is there an interception?

Interception takes place if the contents of a communication are made available, during the course of its transmission, to someone other than the sender or intended recipient. Depending on the nature of the communication the intended recipient may be simply a business or a specific individual. Examples where interception may take place include a supervisor listening in to calls, a business opening e-mails stored on a server before they have been opened by the intended recipient, and an automated system that opens e-mails and/or their attachments to check them for viruses. Examples that do not involve interception include a business accessing a stored collection of e-mails that have been received and opened or deleted by the intended recipient, and a business accessing a stored collection of sent e-mails.

2. Have senders and recipients both given consent?

Interception is allowed if the business has reasonable grounds for believing that both the sender and recipient have consented to the interception. Interception is also allowed in certain other circumstances without the consent of the sender or recipient. However, if a business is to rely on consent in order to legitimise an interception, there must be some action from which consent can be inferred, for example, the caller saying yes when asked or proceeding with a telephone call after hearing a message saying that calls are recorded. Consent must be freely given. Businesses might choose to rely on consent to cover the interception of telephone calls or internal e-mails but it is hard to see how consent can readily be obtained from external senders of e-mail.

3. Is the interception connected with the operation of the communications system itself?

Interception without consent is allowed if:

- it is undertaken by or on behalf of a business that provides a telecommunications service, and
- it takes place for purposes connected with the provision or operation of that service.

Providing a telecommunications service means providing access to and facilities for making use of an electronic communications system. Employers will often be providers of a telecommunications service in respect of their own networks. They might rely on this provision where, for example, incoming e-mails are intercepted by the IT department in order to divert them so as not to block up an e-mail gateway.

4. Is the interception only for monitoring business-related communications?

Interception without consent is not allowed by a business unless the interception is solely for monitoring (or recording) communications which:-

- involve the business entering into transactions, or
- relate in another way to the business, or
- take place in some other way in the course of carrying on the business.

These categories cover most business communications but they do not include personal communications by workers unless they relate to the business. Interception will not be allowed if it is carried out wholly or partly to gain access to the contents of personal communications sent to or by workers that do not

relate to the business. This does not prevent interception which is carried out only to gain access to the contents of business communications but which may incidentally and unavoidably involve some access to other communications on the system.

5. Is the interception to decide whether a communication is a business related one?

Interception without consent is allowed if it is to monitor, but not record, communications to check whether they:-

- involve the business entering into transactions
- relate in another way to the business

For example, an employer may open e-mails in an absent worker's in-box if this is necessary to see whether there are business communications that need to be dealt with in the worker's absence. However, the employer should not open e-mails that in their unopened state appear not to relate to the business, e.g. e-mails that are marked personal' in the header, unless there are convincing grounds on which to believe they are in fact business related.

6. Is a confidential telephone counselling or support service involved?

Interception without consent is allowed if it is to monitor, but not record, communications to a confidential, free, telephone counselling or support service operated in such a way that users can remain anonymous. This is to enable help-line workers to receive appropriate supervision and support.

7. Is the interception for an authorised business purpose?

Interception without consent is allowed if it is part of monitoring (or recording) business communications for one of the following purposes:

- To establish the existence of facts (e.g. to collect evidence of transactions such as those involved in telephone banking or to keep records of other communications where the specific facts are important, such as being able to prove that a customer has been given certain advice).
- To check that the business is complying with regulatory or self-regulatory procedures (e.g. to check that workers selling financial services are giving customers the health warnings required under financial services regulation).
- To check the standards that workers are achieving (e.g. to check the quality of e-mail responses sent by workers to customer enquiries).
- To show the standards workers ought to achieve (e.g. for staff training).
- To prevent or detect crime (e.g. to check that workers or others are not involved in defrauding the business).

- To investigate or detect unauthorised use of the telecommunications system (e.g. to ensure that workers do not breach the employer's rules on use of the system for business purposes, for example by sending confidential information by e-mail without using encryption if this is not allowed. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised).
- To ensure the security of the system and its effective operation (e.g. to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

8. Have all reasonable efforts been made to inform users of the interception?

The requirement of the LBP Regulations is to make reasonable efforts to inform users of the system that an interception may take place. Workers, including temporary or contract staff, will be users of the system but outside callers or senders of e-mail will not be. Where, as will usually be the case, interception involves the collection, storage or use of personal information, the requirements of the Data Protection Act to provide information to those whose data are processed will come into play. Information required under both the LBP Regulations and the Data Protection Act overlaps and can of course be provided at the same time.

Part 4: Information About Workers' Health

Good Practice Recommendations Part 4: Notes and Examples

4.1 Information about workers' health: general considerations

4.1.1 There are risks that the Act will be breached if, for example, line managers institute testing of their workers without authority and without taking into account the provisions of this Code. Anyone authorising testing should have received the necessary training. Business practices should be designed to ensure that testing or other collection of health information does not take place without careful consideration of the requirements of the Act and the recommendations in the Code.

Managers and human resources staff are not generally qualified to interpret medical details. Medical diagnosis and the interpretation of the effect of particular medical conditions on a worker should be left to doctors, nurses or other appropriate health professionals. For this reason those who are not health professionals are unlikely to need access to the details of medical conditions as opposed to information on the impact of those conditions on a worker's ability to work.

4.1.2 Other circumstances in which a sensitive data condition may be satisfied include:

- where the collection of health information is necessary to defend a tribunal claim or for other legal proceedings.
- where a public sector body needs to collect health information to discharge its statutory functions.
- where the collection of health information is undertaken by a confidential occupational health service and is necessary for preventative medicine, diagnosis or care and treatment.
- where the collection of health information is necessary for important, non-intrusive research.
- where the worker has deliberately made information about his or her health public.

See page 72 for more details.

4.1.3 No further guidance on this recommendation.

4.1.4 The level of security applied to personal data must be appropriate' to the nature of the data to be protected and the harm that might result from misuse or loss. Given that health information is sensitive data', the appropriate' level of security is a high one. Unless a particularly high level of security is applied to all employment records it is likely that health information will need to be singled out for special treatment. Depending on the nature of the organisation, it may be possible to keep information about workers' health on a separate database or subject to separate access controls. In other cases it may be possible

to separate health information from the other contents of a worker's personnel file by putting it in a sealed envelope.

The principle of need to know' access should be applied strictly. As far as practicable, access to information on medical conditions should be confined to health professionals, such as doctors and nurses. Managers should only have access to information that is necessary for them to undertake their management responsibilities. Very often this can be limited to information about a worker's current or likely future fitness to work. In some cases it may be necessary for managers to know more about a worker's state of health in order to protect that worker or others. If it is necessary for others to have access they should be subject to contractual conditions of confidentiality equivalent to those imposed on a health professional by their professional standards.

Safety representatives have a legal right of access to information that they need to fulfil their functions. However the employer should not provide information identifying an individual worker unless that worker has consented to this. The law does not prevent an employer from providing anonymised information to a safety representative. Where the disclosure of identifiable information is required by law, (such as might be the case under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995), the Data Protection Act 1998 does not prevent the disclosure taking place.

Where an employer offers a private medical insurance scheme, only in exceptional circumstances should it be necessary for the employer to have access to medical information about a particular worker or about family members and others included in the cover. In general medical information should be kept in confidence by the hospital or clinic responsible for providing the healthcare. It should normally be sufficient for the employer to be provided with information about the financial and other administrative aspects of the scheme.

See Part 2 Employment Records, page 31, for more information on security requirements.

See Part 2 Employment Records, page 35 for more information on insurance schemes.

4.1.5 Health questionnaires should be designed to ensure they only elicit information that is relevant and necessary. This implies they should be designed by health professionals. It also implies that they should be interpreted by those who are qualified to draw meaningful conclusions from the information supplied. Questionnaires need to be checked to ensure they do not lead to discrimination in contravention of the Disability Discrimination Act 1995.

If it is necessary to commission a medical report on a sick worker, for example to assess his or her suitability for continued employment, only relevant information should be sought. This means that the author of a medical report should not be asked to provide medical details of the worker's condition. Instead the report's author should be asked to provide an assessment, for example, of whether or not that worker is fit to return to employment, whether he or she should be redeployed, or whether adjustments need to be made to the workplace to accommodate his or her disability.

The Access to Medical Reports Act 1988 applies when an employer seeks a report from a worker's general practitioner or any other medical practitioner who is or who has been responsible for the clinical care of the worker. In summary, the obligations on the employer are to:

- Notify the worker of his intention and obtain the worker's consent to the application for a report
- Inform the worker of his or her right to:
  - withhold consent to the application being made
  - access the report before it is supplied to the employer by telling either the employer or the medical practitioner of his / her wish to do so
  - withhold consent to supply of the report to the employer once he / she has seen it
  - request amendments to the report before it is supplied
  - access the report for up to 6 months after it has been supplied by the medical practitioner

Workers should not normally be asked to consent to the disclosure of their entire general practitioner records or other comprehensive care and treatment records such as those held by a hospital. Although on occasions an occupational health physician may need access to the full record, such records contain more information than the employer is ever likely to need. Where it is necessary to seek information the general practitioner should be asked specific relevant questions to elicit the information needed by the employer.

4.2 Occupational health schemes

4.2.1 Information could be provided to workers who are part of the scheme by giving them clear written information about what health information will be collected, who will have access to it and in what circumstances. It is particularly important to ensure that workers are aware of the circumstances, if any, in which their line managers will have access to the information that they supply to a health professional. This should be kept to a minimum.

Employers offering an occupational health scheme should consider carefully what information they need to have access to in order to administer the scheme. In most cases only statistical or anonymised information is needed to administer the scheme.

Medical details about individual workers should only be made available to managers in so far as it is necessary to enable them to discharge their management responsibilities. As far as possible an occupational health advisor should hold the medical information about a worker, only telling the worker's manager the results of the health assessment, for example whether or not there's a legitimate reason for a worker's absence from work. It is difficult to see how the disclosure to an employer of information about the health of a worker's family members can be justified.

It should be remembered that the disclosure of medical information given by a worker to an occupational health doctor, nurse or other health professional is restricted not just by the

Data Protection Act but also by a duty of confidence. Other than in exceptional circumstances consent will be needed for the release of such information to non-medical personnel. It is advisable that such consent is given in writing.

4.2.2 It is important that any monitoring of e-mails, telephone calls, internet usage or similar activities by an employer is designed not to compromise any confidential communications between workers and health professionals or non-clinical counselling staff. If, as part of a general monitoring programme, a confidential conversation or other communication is unintentionally picked up, information relating to that conversation or communication should be deleted at the earliest opportunity and no record should be kept of it.

See Part 3 Monitoring at Work page 64 for more information about monitoring electronic communications.

4.2.3 Understanding and acting in a way that is consistent with the principles set out in the Guidance on Ethics for Occupational Physicians will assist compliance with the Data Protection Act 1998. The Guidance is published by the Faculty of Occupational Medicine 5th Edition May 1999 ISBN 1-86016-112-X.

See page 84 for contact details for the Faculty of Occupational Medicine.

4.3 Information from medical examination and testing

4.3.1 If the obtaining of information through medical testing is to be justified on the basis that it is necessary to enforce the organisation's rules and standards, these rules and standards must be known and understood by workers. In some cases the standards may be obvious, for example that it is unacceptable to use illegal drugs in the workplace, but in others they may not. Rules and standards, for example in relation to acceptable levels of alcohol use, should be specific and be set out in a policy that is made known to and accessible by all workers affected. Such a policy may address only drug and alcohol use or may be drawn more widely. Either in this policy or separately, the employer should go on to set out the circumstances in which medical testing may take place, the nature of the testing, how information obtained through testing will be used, and the safeguards that are in place for workers who are subject to it.

Workers employed on overseas contracts may be expected to undergo a degree of medical examination and testing that is substantially more intrusive than that carried out on workers in the UK. For example, workers contracted to work in certain countries may be exposed to particular risks or there may be a legal requirement for testing in the country concerned. In such cases employers should make workers aware of any examination or testing that they will be expected to undergo at an early stage.

4.3.2 Medical examination and testing is intrusive. It should only be used to obtain information where necessary. Employers should not subject all applicants for a job or even all those short-listed to examination or testing. Ideally only where there is an intention to appoint, subject to satisfactory examination or test results, should such examination or testing be undertaken. It is though recognised that practical considerations may dictate that medical

examination or testing is undertaken in parallel with other pre-employment checks, e.g. the obtaining of a disclosure' from the Criminal Records Bureau.

4.3.3 An example of other legal obligations is the obligation on an employer under the Control of Asbestos of Work Regulations 2002 to keep workers who are exposed to asbestos under adequate medical surveillance.

4.3.4 When obtaining information through the testing of workers, employers must be clear about what substances or conditions the testing is designed to detect and about why the testing is being carried out. An impact assessment should be carried out to determine whether testing is a proportionate response to a particular problem. Testing should be designed to only reveal information relevant to the purpose for which the test is being undertaken. Those being subjected to the test should be made aware of this. If an employer intends to carry out a test on an existing sample that the worker has not been told about and has not consented to, the employer must tell the worker about the intention to carry out additional testing and must obtain the worker's freely given consent for this. It would be unfair to the worker, for example, to test a blood sample for the presence of alcohol when the worker has only been told the sample would be tested to check for the presence of a particular chemical to which the worker might have been exposed. It would also be unfair to obtain information by performing a drug test on a sample of a worker's hair without the worker's knowledge.

4.3.5 Information that is obtained in the course of a medical examination or test that does not have a significant bearing on the purpose for which the testing is conducted should be permanently deleted. For example, information obtained during drug testing that happens to indicate that a worker is pregnant should be neither recorded nor used; tests should be designed, as far as possible, not to detect this in the first place.

4.4 Information from drug and alcohol testing

4.4.1 Take particular care when carrying out an assessment of whether the obtaining of information through drug testing is justified on health and safety grounds. Bear in mind that:-

- the employer's interest is usually in detecting drug use that puts at risk the safety of those to whom they owe a duty of care. This can arise from drugs that are legal as well as illegal. Employers should not test merely to find evidence of the use of illegal drugs.
- the drug testing used must address the risk. It must be capable of providing real evidence of impairment or of potential impairment at work that is sufficient to put at risk the safety of others.
- other than in the most safety critical areas, regular drug testing is unlikely to be justified unless there is a reasonable suspicion of drug use that has an impact on safety.
- drug testing must provide significantly better evidence of impairment that puts safety at risk than less intrusive alternatives such as a test of cognitive ability.
- drug testing should only be carried out as part of a post-incident investigation where there is evidence that workers' conduct has had some bearing on the incident.

4.4.2 This can be done by limiting the number of substances being tested for, or by using tests that only detect recent exposure to the substances being tested for. A variety of techniques for carrying out alcohol and drug testing are available to employers. They vary in intrusiveness, depending on the range of substances that can be detected and the time scales involved. For example, some tests are only designed to detect the use of a particular drug within, for example, the previous eight hour period, whilst others are designed to detect the use of a wide range of substances over a much longer period. Employers intending to carry out testing should use the least intrusive methods practicable to deliver the benefits to the business that the testing is intended to bring.

Note that there are tests (assisted performance tests) and equipment that can be used to measure hand-eye coordination and response time. These do not involve any invasive medical procedures and are more justifiable for first instance tests.

Assisted performance tests may be more reliable for the employer in providing evidence of impairment and less intrusive for the worker.

4.4.3 No further guidance on this recommendation.

4.4.4 Even in safety-critical businesses such as public transport or heavy industry, workers will pose a different safety risk through their use of alcohol or drugs depending on the type of work that they carry out. For example, a train driver or signal engineer whose actions are impaired through exposure to alcohol or drugs would generally pose a significantly greater safety risk than would a ticket inspector or rail enquiries clerk. This difference in risk should be reflected in carrying out an impact assessment. Information about ticket inspectors or rail enquiries clerks should not be obtained through testing simply on the basis that fairness' somehow requires that if drivers or signal engineers are tested, they should be tested as well.

4.4.5 No further guidance on this recommendation.

4.4.6 In some contexts attempts have been made to obtain information by collecting urine or other samples covertly, or by testing existing samples in a manner that workers have not been told about. This is deceptive and misleading to workers, and in so far as such practices involve the processing of personal data, they are likely to lead to a breach of the Data Protection Act. Although covert medical testing may be carried out in exceptional circumstances, it is hard to envisage these arising without the police being involved.

4.4.7 The reliable interpretation of test results can require a high level of technical expertise. In order to satisfy their legal duty to ensure results are adequate for the purpose(s) for which the testing was carried out, employers may need to seek appropriate technical advice and use an approved laboratory to analyse samples, such as one operating to the UK Laboratory Guidelines for Legally Defensible Workplace Drug Testing. It is not though necessary to employ health professionals to undertake tests for alcohol using breath analysis equipment.

Although simple kits that can be used to test for various substances are available over-the-counter, employers should not assume that the tests are infallible and should be able to

deal adequately with disputes arising from their use. Some test kits may fail to differentiate between an illegal drug and a legitimate pharmaceutical, or between a pharmaceutical that causes impairment and one that does not.

In order to meet the data protection requirements of adequacy and accuracy in the processing of personal data, for example by ensuring a secure chain of custody for samples, it may be necessary for employers to use a professional service with qualified staff to carry out the testing and interpret its results.

4.5 Information from genetic testing

Note: Most of this supplementary guidance is extracted from an opinion on Ethical Aspects of Genetic Testing in the Workplace by the European Group on Ethics in Science and New Technology, July 2003.

4.5.1 Although there are many diseases with a recognized genetic component resulting from a defect in a single gene (monogenic diseases), as a general rule the incidence of such diseases is low. Monogenic diseases include cystic fibrosis, sickle cell anaemia, Huntington's Disease and haemophilia.

In contrast to the above examples of diseases resulting from defects in a single gene, other human diseases with a genetic component are thought to result from interactions between several genes (polygenic diseases). The incidence of some polygenic diseases is very high. In most of these cases the genetic basis is incompletely understood and is complicated by influences of environment, diet and lifestyle. Examples of such polygenic diseases are heart disease, several cancers and some allergies.

Even for monogenic diseases, predictive value of genetic testing may be limited. There is always a possibility that the disease in question might not manifest itself during the working life of the individual and it is not always possible to predict the severity of the future disease.

The situation is even more complex where diseases with a polygenic basis are concerned. At the present time it is virtually impossible accurately to predict, using genetic tests, either whether the disease will develop at all or, if it does, its timing and severity. Even if the genetic basis of such diseases becomes fully understood, environmental and lifestyle factors, which may themselves be unpredictable, will limit the predictability of disease development.

4.5.2 No further guidance on this recommendation.

4.5.3 Genetic screening for susceptibility to workplace environmental hazards clearly has some precautionary relevance but in many cases the link between a particular genetic status and susceptibility to a particular hazard has only a theoretical basis at present.

The Human Genetics Commission is the statutory body responsible for monitoring and advising on issues to do with genetics.

See page 85 for contact details for the Human Genetics Commission.

4.5.4 At the present time, very few genetic tests are available that give information to either an employer or a worker which could validly be used in the context of decisions concerning employment. It is likely that this situation may change in the future although it is difficult to predict the pace of such change. Validity of a genetic test would require demonstration of:

1. its relevance to health protection of workers
2. the reliability and reproducibility of the test and
3. the level of predictive value for the test.

In such a sensitive area, it is obviously extremely important that procedures for genetic testing are as reliable as possible, as provision of incorrect information to an employer or a worker could have far reaching consequences. All stages of a scientifically satisfactory testing procedure should have built in negative and positive controls to ensure the reliability of the test result. Good laboratory practice should be observed at all times, including detailed documentation of procedures and results. Even when testing procedures are optimised, false negatives and false positives will emerge and validation procedures for the tests may be required.

Conditions for Processing Sensitive Data

When can sensitive personal information 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 information. The conditions which are most likely to be relevant are:-

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

Note: This condition can have quite wide application in the context of employment. 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;

- check the entitlement of workers to work in the UK
- ensure the health, safety and welfare at work of workers
- select safe and competent workers
- ensure a safe working environment
- not discriminate on the grounds of race, sex, disability, religion or sexual orientation
- ensure the reliability of workers with access to personal data
- protect customer's property or funds in the employer's possession
- consider reasonable adjustments to the workplace to accommodate workers with disabilities
- maintain records of statutory sick pay and maternity pay
- supply information on accidents where industrial injuries benefit may be payable
- prevent workers working on a transport system when unfit through drink or drugs
- not continue to employ teachers who do not have the necessary health or physical capacity for employment
- not dismiss workers when it unfair to do so
- ensure continuity of employment under TUPE Regulations

Thus an employer may be able to collect and use sensitive data if this can be shown to be necessary to enable the employer to meet its legal obligations, for example in relation to the safety of its workers, in relation to others to whom it owes a duty of care, or to prevent unlawful discrimination. The collection and use of sensitive data must however be necessary for exercising or performing a right or obligation that is conferred or imposed by law. This condition would, for example, be satisfied if:-

- there is evidence that a worker is using the employer's e-mail system to subject another worker to racial harassment, and there is no reasonable alternative to monitoring the worker's e-mail if the employer is to ensure it meets its obligations not to discriminate on the grounds of race.

It would not though be satisfied if:-

- an employer obtains information on the criminal convictions of all applicants for a particular job in order to protect its staff or customers but the protection could equally be provided by obtaining this information only on the successful applicant prior to confirmation of appointment.
- an employer holds information on the driving convictions of all its workers on safety grounds but safety could equally be ensured by holding this information only on those workers who drive the employer's vehicles.
- a bus operator undertakes drug or alcohol testing of all its workers but the safety of its passengers and others could be ensured by confining tests to the drivers of its vehicles and anyone else employed in a safety-critical role.

This condition might also be relied upon to enable an employer to keep more general sickness records on the basis that these are necessary if the employer is to ensure that it does not dismiss workers on the grounds of absence when it would be unfair to do so.

- **The processing is necessary**
  - **to protect the vital interests of the worker or another person where consent cannot be given or the data controller cannot reasonably be expected to obtain it, or**
  - **to protect the vital interests of another person where consent is unreasonably withheld.**

Note: This condition is most likely to apply when there is a medical emergency and the worker or another person is at risk of serious harm.

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

Note: This condition is most likely to be relevant in the context of prospective or actual tribunal or court proceedings. It might, for example, be relied on to enable an employer to process sensitive personal information to defend itself against a claim for unfair dismissal or unlawful discrimination.

- **The processing**
  - **is of information in categories relating to racial or ethnic origin, religious beliefs or other beliefs of a similar nature, or physical or mental health or condition, and**
  - **is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment, and**
  - **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 information has been made public as a result of steps deliberately taken by the data subject.**

Note: Examples would be where a worker's trade union membership is known because the worker has appeared on local television as a spokesperson for the trade union or where a worker has chosen to tell colleagues at work about his or her condition or disability without any implication that the information should be kept confidential.

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

Note: This condition will be mainly relevant to public sector bodies that may have specific legal duties placed on them in relation to the qualifications, attributes, background, health 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 information such as criminal convictions relating to workers, or in exceptional cases, their family or close associates. It is therefore most likely to be relevant to the employment of groups such as police or prison officers.

- **The processing is necessary for medical purposes including preventative medicine and medical research and is undertaken by a health professional or someone else subject to an equivalent duty of confidentiality.**

Note: This condition is likely to apply where information is held by a company doctor, nurse or similar health professional. It will also cover non-medical staff provided they have an equivalent duty of confidentiality imposed on them, for example through their contract of employment. Whilst this condition will be applicable to the operation of an occupational health service it will not generally extend to information on workers' health when it is in the hands of human resources professionals or other managers unless they need to hold it for medical rather than employment purposes.

- **The processing is in the substantial public interest, is necessary for research purposes, does not support decisions about individuals and is unlikely to cause substantial damage or distress.**

Note: This condition is most likely to be relevant in the context of research into occupational disease or illness.

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

Note: This condition will cover situations where allegations of work-related criminal offences by workers arise, for example, as a result of audit investigations or complaints from customers. In the context of monitoring it will cover situations where monitoring is necessary to detect criminal activity and where seeking the consent of the workers involved would amount to a tip off. Unlawful acts' include not only criminal matters but also acts that breach other statutory or common law obligations.

- **The processing is in the substantial public interest, is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or other service and is carried out without the consent of the data subject because the processing**
  - **is necessary in a case where consent cannot be given by the data subject**
  - **is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or**
  - **must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.**

Note: This condition will be relevant to the monitoring of calls to confidential counselling, advice or support lines such as those run by some charities, for example The Samaritans. It will cover the position of the caller but not of the worker taking the call.

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

By no penalty we mean that consent will not be valid if the employer imposes a punishment on the worker for refusing consent. For example consent to the employer obtaining a doctor's report on a sick worker will not be valid if the worker faces dismissal simply for refusing to give consent.

This does not necessarily mean that declining consent has to be a risk-free option for the worker. It is possible to envisage a situation where, with the benefit of the information in the doctor's report the employer would have been persuaded to continue the worker's employment, but without it the employer, acting on the limited information available, decides that dismissal on the grounds of sickness absence is appropriate. Consent obtained in these circumstances will still be valid.

The need for consent to be freely given means that the extent to which consent can be relied upon in the context of employment is limited. 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 the opportunities to obtain valid consent are likely to be reduced. If, for example, the consequences of not consenting is the automatic withdrawal of a job offer the consent is unlikely to be freely given.

Frequently Asked Questions

1. Aren't paper files exempt from the Data Protection Act are we OK if we don't computerise our workers' health records?

Not necessarily. As well as computerised records manual data held within a relevant filing system are covered by the Act. This is defined as any set of data which is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible. An example of a relevant filing system would be a personnel file with a worker's name or individual reference number on it and in which there are internal dividers which make it easy to find information about the worker such as starting date, performance mark at last appraisal, absence record etc. Other examples might be a file of applications for a particular vacancy in which the individual forms are kept in alphabetical order, or a file of the results of drug tests in which the individual results are kept in alphabetical order. Less obviously structured records, particularly those where the information is kept merely in date order, are unlikely to be caught.

2. Do I have to get a worker's consent to keep records about him or her?

Consent to hold personal information 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 personal information such as health records rather than non-sensitive personal information. In the case of sensitive personal information the consent must be explicit . However, even then, sensitive personal information 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. Information about the racial or ethnic origin of workers may therefore be held in order to comply with the law relating to racial discrimination, and personal information about their health may be held in order to comply with health and safety law. Similarly, sickness records of workers may be kept in order to enable employers to meet both the requirements imposed on them by the law in relation to statutory sick pay and the requirement not to dismiss workers unfairly on the grounds of absence.

See page 72 for the conditions for processing Sensitive Data.

3. What about sickness records?

Sickness records will almost certainly contain information about workers' physical or mental health. They will therefore include sensitive data. Where they are kept in order to enable employers to meet the requirements imposed on them by the law in relation to statutory sick pay it is clear that a sensitive data condition can be satisfied and consent will not be needed. With more general sickness records the position is less clear-cut. The Commissioner recognises that employers need to keep some sickness records and it is unsatisfactory if they have to rely on the consent of workers to do so. He also understands the argument that without sickness records employers will be unable to ensure that workers are not dismissed unfairly on the grounds of absence. He therefore takes the view that an

employer keeping and using sickness records in a reasonable manner can rely on the condition that the processing is necessary in order to enable the employer to comply with any legal obligation associated with employment. The Data Protection Act, as it currently stands, does not place the question beyond doubt but the Commissioner understands that Government is considering changes to the law that will do so. Even though consent is not needed, employers should of course ensure that workers are aware of what information about them is kept in sickness records and how it is used.

4. 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.

5. 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.

6. 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.

7. 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?

You should approach the Criminal Records Bureau or Disclosure Scotland who operate a system of police checks for staff working with children or vulnerable adults. The Act does not stop you using this channel. What it will do, when the relevant parts are brought into force is prohibit enforced subject access' in connection with employment or recruitment.

See page 17 for more information on the Criminal Records Bureau and Disclosure Scotland.

8. 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.

9. Is a worker entitled to access to all our confidential records, including references?

There is no general exemption from the worker's right of access to information about him / her simply because the information is confidential'. 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 may though be entitled to take steps to withhold information that reveals the identity of other individuals such as the author of the reference. This would not usually justify withholding the reference in its entirety.

10. How do I deal with requests by workers for access to information where the information identifies someone else? We get this problem a lot when workers want access to disciplinary files and similar documents.

Such requests require careful handling and there is no simple solution to your problem. Employers should be prepared to disclose information to a worker that identifies work colleagues, provided that the information is about colleagues acting in a business capacity and is not of a particularly private or sensitive nature. However, there are cases where information should be withheld. This might be the case where, for example, giving access would allow a worker accused of bullying to find out the identity of his or her accuser.

See page 40 for the process to follow for access when information about third parties is involved.

11. 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 therefore recommended.

12. We are looking at centralising our group's employment records at our headquarters in the USA. Can we do this?

Personal data must not be transferred outside the European Economic Area (EEA) unless adequate protection is provided in the destination country. Some countries provide adequate protection by virtue of their data protection law. The USA is not one of these. In the USA a special arrangement known as the safe harbor' has been created. If your company is a member of the safe harbour transfer is allowed. There are also other alternatives such as providing adequate protection through the terms of a contract between your company in the UK and its parent in the USA. Detailed guidance on international transfers of personal data is provided on the Data Protection: Your Legal Obligations section of the Commissioner's website.

13. Can we disclose personal information to prospective purchasers of our business?

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

14. We own the equipment workers use for communications and they've been told we are going to monitor them. Isn't that enough?

You may well own the equipment, but the rules of data protection still apply to personal information processed on it. Telling workers about the monitoring is important, but telling them about it in general terms is unlikely to be sufficient. Workers should be told about the specific circumstances in which messages they send or receive may be seen by others. Even if workers have been told about monitoring, the other rules of data protection still apply. This means, for example, that the information obtained through monitoring mustn't be irrelevant or excessive. The benefits monitoring brings should be sufficient to justify carrying it out. The Code recommends the use of an impact assessment to check whether monitoring is justified.

15. But what if we completely ban private e-mail use and internet access?

A ban can be an important factor but is not necessarily an over-riding one. A ban on private use doesn't in itself allow the employer to access messages that are clearly private. The intrusion involved in accessing such messages must still be justified by the benefits gained. It might, for example, be possible to identify an e-mail as private from its header and take action against its sender or recipient for breach of the rule without reading the message's content. In any case there might well be genuine business messages, for example ones sent by a worker to his or her occupational health advisor that a worker has legitimate grounds for wishing to keep private.

16. Is it right that we can never open private e-mails in the course of monitoring?

There is no absolute ban on an employer accessing the content of private e-mails, but any such access ought to be carefully considered. Much depends on the reasons for access, any rules the employer might have for private use of the system, what workers have been told about monitoring and what steps are taken to keep the intrusion to a minimum. There is, for example, likely to be little to prevent an employer who suspects a worker of engaging in criminal activity in the workplace and who reasonably believes that this may involve the sending or receipt of e-mails from accessing the contents of his or her messages. The opening of e-mails that are clearly private should not be undertaken lightly though.

It is unlikely that opening private messages merely on the off chance that evidence of wrong-doing will be found will be justified if this involves revealing their contents to an individual other than the sender or intended recipient.

17. The Lawful Business Practice Regulations allow a wide range of monitoring. Don't they override the Data Protection Act?

No. When carrying out monitoring both pieces of legislation must be complied with, one doesn't override the other. The Lawful Business Practice Regulations deal with the interception of electronic communications. Not all monitoring involves interception. Even where it does, the Regulations work in tandem with the Data Protection Act. An interception, if it is not done with the consent of the parties to the communication, must satisfy one of the conditions in the Lawful Business Practice Regulations. In so far as it then involves the recording and use of personal information it must also comply with the Data Protection Act. Although the conditions in the Lawful Business Practice Regulations allow for interception of business related communications in a range of circumstances, monitoring that involves interception and is targeted on the contents of personal communications that are not business related is not permitted.

18. How does the Act affect virus checking?

The Act does not prevent employers monitoring their systems to check for viruses or other forms of malicious code. In fact the Act requires those handling personal information to use technical means to safeguard their systems. Virus checking should though be conducted in the least intrusive way possible consistent with achieving good security. It is preferable, for example, from a privacy viewpoint, for suspect messages to be rejected or quarantined for collection by the intended recipient rather be opened and read by a systems administrator.

19. Does the Code really require us to provide our workers with separate e-mail accounts for private messages?

No, this is a misunderstanding. The Code says that if an employer chooses to provide a separate facility for private messages this will be an important factor in deciding what monitoring of the business related account is justified. If a separate account is provided for private messages this will help limit any intrusion that results from monitoring the business account.

20. We have to prevent sexual and racial harassment of workers. Are we justified in checking e-mail and internet access to do so?

Employers have legal obligations on them that require them to take active steps to prevent racial or sexual harassment in the workplace. Nevertheless it is hard to see a justification for randomly or routinely accessing the content of e-mail messages, particularly private ones, sent to of from workers or checking which websites they have visited in the course of private internet use on the off-chance that evidence of harassment will be found. Where there are grounds to suspect that a particular worker or workers are using e-mail to harass others or are downloading inappropriate material from the internet then targeting monitoring at those workers' e-mail or internet use may well be justified.

21. We undertake work as a contractor for a bank and they insist we monitor our workers' creditworthiness. If they require us to do this does this mean we can do it regardless of what the Data Protection Act says?

No. As you are monitoring the creditworthiness of your workers you must be satisfied that the intrusion they face is justified by the benefits the monitoring brings to you and the bank. You are obviously entitled to take the bank's circumstances into account in assessing what monitoring is justified, but the assessment should be yours. You are also entitled to take into account the extent to which workers genuinely have a free choice whether or not to subject themselves to the monitoring, i.e. are they able to choose not to work on the bank's contract without suffering any detriment? Incidentally, you must not use a facility provided to you by a credit reference agency for checking your customers to check your workers without the agency's knowledge and agreement.

22. Is it acceptable for us to install hidden video cameras? We told all workers some months ago that we might do this.

Video cameras are particularly intrusive. The notice you have given to workers will not be sufficient unless it is the case that providing more specific information would be likely to prejudice the prevention or detection of crime or equivalent malpractice, for example because the camera has been set up to monitor a worker you suspect of theft. Because video cameras are intrusive workers should generally be aware of exactly where they are located and what they are being used to detect.

23. We collect a lot of information about workers through monitoring e-mails and internet access. What do we have to do when one of them makes a subject access request?

If a worker makes a subject access request he or she is entitled to access to all the information of which he or she is the subject. This will include internet access logs and e-mail records. Remember though that a worker will not be the subject of a message simply because he or she is its sender or recipient. Clearly the more information that is amassed about workers through monitoring, the more onerous employers may find it to respond to subject access requests. Systems that are designed with subject access in mind are though likely to reduce the burden considerably.

24. We encourage our managers to take responsibility for managing sickness in the workplace. Doesn't the Code stand in the way of this?

No. The Code does not try to limit the responsibilities an employer gives to its managers. What the Code seeks to ensure is that managers have access to no more information about their workers' health than they need to carry out their responsibilities. The broader their responsibilities the more information they are likely to need. However managers' concern will primarily be with the impact of a medical condition on a worker's fitness for work rather than with the medical details.

25. We are required to undertake health surveillance for workers exposed to particular health risks. Does the Code mean that this can only be undertaken by health professionals?

According to the Health and Safety Executive (HSE) health surveillance is about systematically watching out for early signs of work-related ill health in workers exposed to certain health risks. There is nothing in the Code that would prevent a supervisor, with appropriate training, having a limited role in the collection of basic health information and associated record keeping, for example carrying out skin inspections to look for signs of rashes on the hands of workers working with detergents. This is the role of responsible person' identified by the HSE. What is important is that supervisors are trained for any role that they might have in the collection of basic health information, are aware of its possible sensitivity and the need to keep it securely and do not try to interpret the information by, for example, attempting to diagnose the possible cause of symptoms. More intrusive collection of health information, its interpretation and associated record keeping should be carried out by a qualified person such as an occupational health nurse or doctor.

26. As a train operator we must ensure the safety of our passengers. We therefore have a rule that the drivers we employ must not come to work when under the influence of alcohol. To support this, we plan to introduce random testing. We want to treat all our workers equally so we intend to apply the same rule to our office based staff. We also plan to extend the random testing to them. Is this in accordance with the Code?

The Code does not affect your decision to apply a no alcohol rule to all your workers. This is not a data protection issue. However the gathering of information about your workers through random testing is. You need to be sure that the intrusion involved is justified by the purpose you are trying to achieve. The collection of information on drivers through random testing may well be justified on safety grounds, particularly if you have suspicions that your rule is being breached. However, the random testing of office based workers is unlikely to be justified because its purpose appears to be to ensure equality of treatment rather than the safety of the public. The Code advises employers to conduct an impact assessment to help them determine whether the collection of information through testing is justified.

27. Why does the Code include a section on genetic testing? Isn't the Information Commissioner encouraging the use of highly intrusive and unproven techniques by even mentioning genetic information in the context of employment practices?

We are aware that there is little, if any, evidence that information obtained through genetic testing is currently being used by employers in the UK. The Code takes a very cautious approach to genetic testing. Nevertheless, the Code is intended to be forward looking. There is no doubt that genetic testing techniques are developing quickly and that some employers may seek to take advantage of the opportunities that they provide. Although a cautious approach should be taken and any advice from the Human Genetics Commission should be borne in mind, there may in time be exceptional circumstances where the obtaining of some information about some workers through genetic testing is both justified and desirable.

28. We place great value on our corporate reputation and believe it will be damaged if any of our workers are involved with illegal drug taking outside work. Are we allowed to obtain information through drug testing in order to prevent this? If we have included a drug testing term in workers' terms of employment, will this cover us?

Obtaining information about workers' conduct outside work through drug testing is particularly intrusive. It is only likely to be justified where there are compelling grounds. Employers are advised to undertake an impact assessment to help them determine whether this is the case but obtaining information through drug testing is unlikely to be justified on the basis of maintaining corporate reputation. An exception is with organisations that are themselves charged with enforcing anti-drugs laws. If workers have genuinely given their consent to the collection and use of information through drug testing this can be taken into account in an impact assessment but it does not guarantee compliance with the Data Protection Act. Any information collected must still be relevant and not excessive. Furthermore, informed freely given consent is not guaranteed merely because a relevant term of employment is in place.

Useful Addresses

1 Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545745 (for information and copies of the Code) or
01625 545740 (for notification)

Fax: 01625 524 510

E-mail: mail@ico.gsi.gov.uk (for information and copies of the Code) or
notification@ico.gsi.gov.uk (for notification)

Website:
www.ico.gov.uk
(for information, to download the Code and for notifications)

Regional Offices

Northern Ireland

Information Commissioner's Office – Northern Ireland

3rd Floor
14 Cromac Place
Belfast
BT7 2JB

Telephone: 0289 027 8757

Fax: 028 9051 1584

E-mail: ni@ico.gsi.gov.uk

Scotland

Information Commissioner's Office – Scotland

45 Melville Street
Edinburgh
EH3 7HL

Telephone: 0131 244 9001

E-mail: scotland@ico.gsi.gov.uk

Wales

Information Commissioner's Office – Wales

2nd Floor, Churchill House
Churchill Way
Cardiff
CF10 2HH

Telephone: 029 2067 8400

Fax: 029 2067 8399

E-mail: wales@ico.gsi.gov.uk

2 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

3 British Psychological Society

St Andrews House
40 Princess Road East
Leicester
LE1 7DR

Telephone: 0116 254 9568

Fax: 0116 247 0787

Website: www.bps.org.uk

4 BSI (British Standards Institute)

BSI-DISC
389 Chiswick High Road
London
W4 4AL

Telephone: 020 8996 9000

Fax: 020 8996 7001

E-mail: cservices@bsi-global.com

Website: www.bsi.org.uk

5 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

6 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

7 Confederation of British Industry

Centre Point
103 New Oxford Street
London
WC1A 1DU

Telephone: 020 7395 8247

Website: www.cbi.org.uk

8 Criminal Records Bureau

PO Box 110
Liverpool
L69 3EF

Telephone: 0870 9090811

Website: www.crb.gov.uk

9 Department of Trade and Industry

Communication and Information Industries Directorate
151 Buckingham Palace Road
London
SW1W 9SS

Telephone: 020 7215 5000

Website: www.dti.gov.uk/cii

10 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

11 Disclosure Scotland

PO Box 250
Glasgow
G51 1YU

Telephone: 0870 609 6006

Website: www.disclosurescotland.co.uk.

12 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

13 The Faculty of Occupational Medicine

The Royal College of Physicians
6 St Andrew's Place
Regents Park
London
NW1 4LB

Telephone: 020 7317 5890

Website: www.facoccmed.ac.uk

14 Health & Safety Executive

Rose Court
Southwark Bridge
London
SE1 9HS

Telephone: 08701 545500

Fax: 02920 859260

Website: www.hse.gov.uk

15 Human Genetics Commission

Department of Health
Area 652C, Skipton House
80 London Road
London
SE1 6LH

Telephone: 020 7972 1518

Fax: 020 7972 1717

E-mail: hgc@doh.gsi.gov.uk

Website: www.hgc.gov.uk

16 The Stationery Office

PO Box 29
Norwich
NR3 1GN

Telephone: 08700 600 5522

Fax: 08700 600 5533

E-mail: customer.services@tso.co.uk

Website: www.tso.co.uk

17 Trades Union Congress

Congress House
Great Russell Street
London
WC1B 3LS

Telephone: 020 7636 4030

Fax: 020 7636 0632

Website: www.tuc.org.uk

Publications Line
t: 08453 091 091
f: 0870 600 8181

Helpline
t: 0303 123 1113 or 01625 545745
f: 01625 524510

e: mail@ico.gsi.gov.uk
w: ico.gov.uk

June 2005

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

DP/EPCSG/0605

Information Commissioner's Office