

**EMPLOYMENT LAW UPDATE FOR CHARITIES SEMINAR
10 JUNE 2008**

Data Protection and Employment Codes of Practice
Presented by Malcolm Lynch, Partner

Data Protection Act 1998

What does the Act do?

The Act seeks to protect data in two ways. First it requires those who record and use data (known as the data controller) to be open about their use and follow the 8 data protection principles of good information handling. Secondly, it gives the individuals identified by the data (known as the data subjects) certain rights including access to the data and rights to have that data corrected.

What does the Act cover?

The Act is concerned specifically with personal data. The definitions of both personal data and data are set out in the list of basic interpretive provisions at the end of this document, but can be summarised as data which relates to a living individual who can be identified from the data or from other information held by the data controller and includes expressions of opinion about the individual and any actions that may be taken that relate to the individual. Data includes information which is held electronically or in hard copy format in a filing system, or is part of an accessible record such as health records, some educational records and some public records.

Notification

As processors of personal information employers are data controllers and as such are obliged to register with the Information Commissioner's Office. This process is known as notification. There are a number of exemptions from notification for individuals and organisations who make only limited use of personal data but it must be remembered that these exceptions are limited and even if you are exempt from notification, you are still required to comply with the data protection principles.

What is data processing?

Generally whatever you can think of doing with data will amount to processing including obtaining it, recording or storing it.

Failure to notify

Unless you are exempt, failure to notify is a criminal offence.

Offences under the Data Protection Act can be committed not only by the organisation themselves but also by the officers. Breaches of the data protection principles and data subject rights can be made by managers and individual workers, rendering them liable to prosecution and fines (section 61 Data Protection Act 1998).

The Information Commissioner's Office has powers to prosecute those who fail to register and is now actively pursuing those who have failed to register and exercising these powers. Recently two sole-practitioner solicitors in London were prosecuted and fined for failure to register.

Exemptions

Two exemptions which may be relevant to charitable employers relate:-

First to a not-for-profit organisation if all of the data processing is only for the purposes of establishing or maintaining membership or support for your organisation or providing or administering activities for individuals who are either members or have regular contact with it;

Secondly, you do not have to notify if the only process you carry out is for one or more of the following core business purposes of staff administration, advertising, marketing and public relations or accounts and records.

These two exemptions will not cover organisations who obtain personal data from a third party or who may process data for another organisation, for example, undertaking payroll duties or if you are marketing goods and services for others.

Again, although you may be exempt from notifying the Information Commissioner's Office you must still comply with data protection legislation and the principles of good data handling.

Data Protection Principles - the rules of good data handling

The precise wording of the data protection principles are set out in Schedule 1. In summary, they are:-

1. Personal data must be fairly and lawfully processed and shall not be processed unless:
 - (a) At least one of the Schedule 2 conditions is met; and

WRIGLEYS

— SOLICITORS —

- (b) In the case of sensitive personal data at least one of the Schedule 3 conditions is also met.

The Information Commissioner has confirmed that in assessing whether or not processing is "fair", the most important consideration is the interest of the data subject. The Act makes it clear that with some limited exceptions, processing will not be fair unless the data subject has been provided with basic information which will include the purpose for which the data is to be processed and a description of any person to whom the data may be disclosed.

As employers you will generally be covered by one or more of the conditions in schedules 2 and 3 allowing you to process the data, but the processing must still comply with the other data protection principles. The conditions are attached for your convenience.

2. Personal data shall only be obtained for specified and lawful purposes and not processed in any manner incompatible with that purpose.

It is essential that as an employer you are clear about the purposes for which the data will be processed and clearly explain these purposes to the data subjects. The data must then be used only for those limited, clear and well explained purposes. Such purposes may be those which you have notified to the Commissioner, or which are included in any fair processing code you have issued to staff.

3. Personal data must be relevant to your organisation's need and not excessive in detail.

These terms are not defined but the intention is that you should monitor the reasons why you require information to ensure that you hold only the data that you actually need.

To use an employment application form as an example, details of National Insurance numbers will only be required for a successful applicant, details of whether an applicant holds a current driving licence, or their religious denomination may be irrelevant.

4. The data must be accurate and kept up-to-date.

The remedy for breach of this fourth principle is simply to correct any errors in the data. The Act also contains a special provision to take account of the situation where an employer has accurately recorded inaccurate information received from the employee or any third party so that the employer should ensure that such data indicates this, but does not in itself require deletion.

5. Data should be kept no longer than is necessary.

WRIGLEYS

— SOLICITORS —

Guidance has been issued by the Commissioner which confirms that the length of time appropriate will depend upon the information. Clearly data should not be kept indefinitely. The Code of Practice on Recruitment and Selection suggests that vetting information relating to unsuccessful job applicants should be deleted within six months.

6. The data must be processed in accordance with the rights of the individual.

These include a right to receive a copy of the information, rights in relation to automated decision taking and to prevent information provided being used for direct mailing purposes. See below for further discussion of the data subject's rights.

7. The data must be securely stored to prevent unlawful or unauthorised processing, loss, destruction, damage or disclosure.

The Act specifically states that an employer must take reasonable steps to ensure the reliability of staff who have access to personal data this identifies a requirement for training and restricting access to information held, rather than questioning the honesty of staff.

This principle also applies to your use of third parties' services, for example, outsourced functions such as payroll and pensions and includes a requirement to have in place a written contract ensuring appropriate security.

8. The eighth principle restricts transfers of data to countries outside the European Economic Area.

The EEA presently consists of the twenty seven EU member states together with Iceland, Liechtenstein and Norway. It does not include the Channel Islands or the Isle of Man.

A number of countries outside the EEA with their own data protection laws have been designated as "adequate" by the European Commission.

The European Commission have also found data transfers to the USA are "adequate" provided the US business has signed up to a "safe harbour" arrangement. Such arrangements may be extended to other countries which have no general data protection law.

Even where a country has not been designated as adequate, a data controller is entitled to form their own conclusion that an adequate level of protection for a particular transfer exists. Such an assessment, however, is only anticipated to be practical for a business that routinely transfer large volumes of data to a particular country.

The Information Commissioner has established a model contract for such transfers.

An example of a transfer would include where an employee travels abroad with a laptop containing personal data connected with their employment. The employer in the UK remains the data controller. Whilst abroad the employee works on that data it will amount to processing. Provided the data remains in the possession of the employee and the employer has an effective procedure addressing security and other risks posed by the use of laptops (e.g. theft or loss of the laptop), the conclusion that there is adequate protection is likely to be reasonable.

Data Subject Rights

The Data Protection Act 1998 provides the following rights for individuals:-

1. Subject Access

Upon making a request in writing upon paying any fee required (to a maximum of £10) an employee is entitled to receive all information constituting personal data of which he or she is the data subject.

This includes not only information about the employee held in computer records but also manual data held in relevant filing systems whether this is in a central human resources or personnel department or elsewhere in the organisation for example information which may be held by line managers or department heads.

The information to be disclosed would also include emails and other documents which may have been although having been deleted from a live system are still capable of recovery, for example in archive or back-up systems.

The Act specifies that a data controller is not obliged to comply with the request ... unless he is supplied with such information as he may reasonably require in order to ... locate the information which that person seeks (section 7(3)).

A particular problem arises for employers who may find that in complying with a request they will disclose information relating to another individual. This for example may include references or complaints received whether or not they have formed part of a disciplinary process.

Where an employer is satisfied that the information can be disclosed without identifying any other individual, this will include deleting names or other relevant parts of any documents, then the information must be disclosed.

Where such steps cannot be reasonably taken, the employer will only be required to comply with the access request where the other individual has consented to the

disclosure of the information or whether it is reasonable in all the circumstances to comply with the request without the consent of the other.

These will require the employer to give consideration:

- to any duty of confidentiality owed to the other;
- steps which he may reasonably take with a view to seeking their consent;
- whether the other individual is capable of giving consent; and
- any express refusal to give consent.

In circumstances where the data subject may be aware that information has been withheld, they must rely upon their rights either to seek an assessment from the Information Commissioner or pursue a complaint through the Courts.

This does not mean that all third party identification must be removed. The data controller is required to consider what other information the data subject may have. For example, if the document refers to a discussion between the data subject and another individual, then the data subject will already know the identity of that individual. This may apply, for example, to records of discussions with line managers.

2. Rights in relation to automated decision taking

By written notice, individuals can require a data controller to ensure that no decisions that will have significant affect on them is based solely on the processing by automatic means of personal data of which they are the subject. Exemptions apply to assist certain decisions provided:

2.1 The decision must be taken in the course of steps taken:

- for the purposes of considering whether to enter into a contract with the data subject; or
- with a view to entering into such contract or in the course of performing such contract; or
- the decision must be authorised or required by or under any enactment; and

2.2

- the effect of the decision must be to grant a request of the data subject; or
- steps must be taken to safeguard the legitimate interest of the data subject, for example, by allowing them to make representations.

For this right to apply the automated decision taken must be based on matters relating to the individual.

An example given in the Code of Practice is where an automated job application scan excludes employees who specify a particular minimum salary. That information does not identify the individual.

3. The right to rectify, block, erase or destroy incorrect data (Section 14);
4. Compensation may be payable to an individual who suffers damage or distress as a result of any contravention of the requirements of the Act where the data controller is unable to prove that they have taken such care as is reasonable in the circumstances to comply with the relevant requirements.
5. An assessment as to whether processing is likely or unlikely to comply with the Act (section 42).

Where the Information Commissioners considers that a breach of the data protection principles has occurred then an enforcement notice can be issued against any responsible organisation. An appeal can be made to the Independent Information Tribunal in respect of an enforcement notice.

A breach of the data protection principles itself is not a criminal offence. However, if an organisation fails to comply with an enforcement notice or continues to break the data protection principles, a criminal offence is committed.

Exemptions

The Act includes a number of exemptions which are likely to be relevant in the employment context. These may be divided into two groups:

Subject information exemptions. This includes where for example other individuals may be identified from the data which would otherwise be required to be disclosed.

There are also specific non-disclosure exemptions which restrict the nature of information which a data controller would otherwise be required to provide.

Dealing with these two groups in more detail:-

WRIGLEYS

— SOLICITORS —

1. Subject information exemptions include:-

- (i) personal data processed for crime and taxation purposes; namely prevention or detection of crime, apprehension or prosecution of offenders or the assessment or collection of any tax or duty. Such data is exempt from the duty to disclose but only to the extent where such disclosure would be likely to prejudice any of the crime or taxation purposes.
- (ii) to protect confidentiality of personal data processed for the purposes of management forecasting or management planning but again subject to the extent which disclosure of such information would prejudice conduct of the business or other activity of the employer.

Such information will clearly be time-sensitive and once the time covered by relevant forecasts has passed or a plan has been put into effect or discarded, it is difficult to see how this exemption could continue to be relied upon.

- (iii) where the data consists of records of intentions of the employer in relation to any negotiations with the employee or potential employee. Again this is subject to the exemption only applying to the extent to which the application of the disclosure requirements would likely prejudice such negotiations.
- (iv) where the data is processed for the purposes of, or in connection with, a "corporate finance service" provided by a "relevant person". This will only apply to information which could, in the reasonable belief of the data controller, effect the price or value of particular instruments of a price sensitive nature and would apply, for example, on company take-overs and mergers.
- (v) Confidential references given by an employer for specified purposes (education, training or employment, appointment to office or provision of any service) are exempt from the subject access rights. This only applies to references in the possession of the employer giving the reference and not in the hands of a recipient.

2. Non-disclosure exemptions

There are exemptions from the main provisions of the Act which restrict the disclosure of personal data by the data controller. These exemptions apply to circumstances where disclosure is required, and to the extent that it is required

- for any of the crime and taxation purposes; or

- may otherwise be required by any rule of law or by the order of a Court; or
- where such disclosure is necessary for the purposes of or in connection with legal proceedings or obtaining legal advice.

The purpose of these provisions is to enable the data controller to release the information in relevant circumstances without being in breach of the provisions of the Act and the rights of the individual data subject.

It must be noted that nothing in the Data Protection Act itself will require such disclosure or provides any third party, including the police, rights to obtain access to personal data in the possession of a data controller.

Enforced Subject Access

Section 56 provides that it is a criminal offence for any employer to require an employee or prospective employee to supply them or produce a "relevant record" in connection with their recruitment or continued employment.

The term "relevant record" relates to records of cautions, criminal convictions, National Insurance contributions and certain social security benefits.

Section 55 of the Data Protection Act also makes the unlawful obtaining and unlawful disclosure of personal data a criminal offence.

A person must not knowingly or recklessly, without the consent of the data controller:-

- (a) obtain or disclose personal data or information contained in personal data, or
- (b) procure the disclosure to another person of the information contained in personal data.

There is a specific exception to liability where the person can show:-

- (a) that the obtaining, disclosing of or procuring,
 - (i) was necessary for the purposes of preventing or detecting crime or;
 - (ii) was required or authorised by or under any enactment by any rule of law or by the order of a Court
- (b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person, or

WRIGLEYS

— SOLICITORS —

- (c) that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing, or procuring and the circumstances of it, or
- (d) in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

There are statutory exceptions to liability where the employer acts by authorisation of law where in particular circumstances conducting checks is justified as being in the public interest. This retains protection for employers in sensitive areas such as child care. The volume and complexity of the law in this area is beyond the scope of this paper and indeed is set to change, but by way of example there is a legal requirement for "child care organisations" to carry out checks on prospective workers who work in "child care positions".

The definition of "child care organisation" is limited to organisations:

- which provides accommodation, social services or health care services to children or supervise children; and
- whose activities are regulated by certain prescribed statutes (which largely relate to the type of activities in paragraph 'a' above;

The definition of a "child care position" is broad and includes:

- a position whose normal duties include work in:-
 - (i) a hospital exclusively or mainly for children,
 - (ii) a home, care home, or private hospital exclusively or mainly for children ,
 - (iii) an educational institution which is a care home exclusively or mainly for children,
- a position whose normal duties include work on day care premises,
- a position whose normal duties include caring for, training, supervising or being in sole charge of children,
- a position whose normal duties involve unsupervised contact with children,
- the position of charity trustee of a children's charity,

- a position whose normal duties include supervising or managing an individual in his work in one of the above positions.

So this particular obligation to obtain checks only applies to a narrow section of charities, but to many positions though not all within such charities.

Where you are in any doubt as to whether checks should or can be made we would advise you to seek specific advice.

Sensitive data

The definition of sensitive personal data is set out in the definitions at the back of this document. This includes information as to the data subject's racial or ethnic origin, political opinions, religious beliefs, physical and mental health, and sexual life.

The Act sets out a series of conditions, at least one of which has to be met before an employer can process sensitive personal data.

The Code of practice recognises that consent may be more freely given in the recruitment process where an individual will usually have a free choice whether or not to apply for a particular job.

Explicit consent must still be obtained and blanket consents are unlikely to be acceptable. The applicant must have been told clearly what personal data is involved and the use that will be made of it.

As the recruitment process progresses, consent is less likely to be freely given, for example, where a job offer may be withdrawn if the information is not provided.

It is therefore important for an employer to ensure that it obtains consent early in the recruitment process and give applicants the opportunity to opt in or opt out of giving such data. For example, an employer may confirm that an appointment is subject to the satisfactory criminal records bureau disclosure, but such a request for disclosure would only be made in the latter stages of the recruitment process.

There is a code of practice issued by the Criminal Records Bureau that sets out an employers obligations in respect of the use of information obtained through standard and enhanced disclosures. It is the Information Commissioner's position that many of the principles of the CRB code of practice will be equally applicable to the basic disclosure and that any failure to comply with the Code is likely to be a breach of the data protection principles.

Data protection principles and employment relationships

WRIGLEYS

— SOLICITORS —

Much of the information held by an employer relating to their workers will not require worker's consent and the Information Commissioner's position is that it may have been misleading to seek consent where workers have no real choice.

Equally, processing of sensitive data may not require explicit consent in a number of circumstances, for example, where the processing is necessary to enable the employer to comply with any legal obligation. An employer may retain information about the racial or ethnic origin of workers in order to comply with the law relating to discrimination and may keep sickness records in order to maintain records in relation to statutory sick pay.

An employer must remember that whilst they may be permitted to process that information, such processing must comply with the data protection principles. In such cases, information about racial or ethnic origin may be anonymised and still satisfy equal opportunities monitoring requirements. Holding information about sickness absence would not permit an employer to produce league tables or require retention of records once an individual employee has exhausted their SSP entitlement. There may be other reasons to justify holding the information but it is important that the employer has made a proper assessment.

Exemptions available after 23 October 2001 but before 24 October 2007

The exemptions for manual data which was held immediately before 24 October 1998 and which was not or which is not intended to be automatically processed or which is not recorded or intended to form part of a relevant filing system which is a health record, education record or accessible public record are no longer applicable.

The Employment Practices Code

The Employment Practices Code on Data Protection issued by the Information Commissioner is intended to help employers comply with the Act and encourage good practice. It is aimed primarily at larger businesses where employment constitutes a significant activity, but much of the Code will be applicable to any employer. The Code was originally issued in four separate parts. The first of which was issued in 2002 and the subsequent parts over the following few years. The Code has since been updated and is now published as a single volume.

The Code seeks to issue guidance on points that an employer will need to check and what action if any they will need to take in order to ensure compliance with the data protection principles. The Code forms the Information Commissioner's recommendations and does recognise that employers may have alternative ways of meeting the legal requirements of the Act.

Relevant provisions in the Code are likely to be cited by the Information Commissioner in connection with any enforcement action that arises in relation to the processing of personal data. The Information Commissioner's view is that disregard for the data protection requirements and particular benchmarks within the Code designed to assist organisations is likely to mean that an employer will not comply with the Act.

The Code is issued in four parts:-

Part 1: Recruitment and Selection

Part 2: Employment Records

Part 3: Monitoring at Work

Part 4: Information about Workers' Health

Throughout the Code, the term "worker" is used in a wide sense and will extend beyond those in a traditional "employment" relationship. The Code covers:-

- a. successful and unsuccessful applicants, including former applicants;
- b. current and former employees;
- c. current and former agency workers;
- d. current and former casual workers;
- e. current and former contract workers;

The Act will also apply to volunteers, work experience placements and others in the workplace.

It must be remembered that the data protection principles apply to all individuals and are not restricted to employees.

Part 1 - Recruitment and Selection

The initial recruitment and indeed subsequent internal recruitment of workers to new roles inevitably requires the processing of data. Much of the information is of the type generally considered to be personal and private and some will be sensitive data for the purposes of the Act. The Act does not restrict the ability of an employer to carry out an effective recruitment exercise, but aims to strike a balance between the needs of the employer and the rights of the individual.

1. Advertising

Adverts should show the name of the organisation which will be collecting the information and how it will be used, unless this is self-evident. This is particularly relevant where a recruitment agency is concerned; in which case the employer should check the agent is identifying itself and informing the applicant how their information will be used. As soon as you receive applicant's details from an agent you must inform the applicant that you are holding their data if this has not already been done by the agent.

2. Job applications

Ensure that all information obtained is relevant to the decision. National insurance details should not be collected at this stage as they will only be required of a successful applicant. This also applies to any information about previous convictions, which again may only be obtained if this is relevant to the role.

You should explain to applicants any sources from which and how other information about the candidate may be sought.

Employers should also ensure that there is a secure process for receiving and processing an application. Steps should be taken to avoid applicants details being seen throughout an office or discussed between staff who are not involved in the selection process, and even then only to the extent necessary within the selection process.

If you are collecting sensitive data at this stage you should ensure at least one of the sensitive data conditions is satisfied.

Secure methods for dealing with applications should be used at each stage. Online applications should be securely transmitted, e.g. by using encryption software and

as soon as hardcopy applications are received these should be kept securely and access restricted to the relevant personnel only.

3. Verification

In the Code this is referred to as the process of checking that details supplied by an applicant are accurate and complete. The verification process should be open. All applicants should be informed of what information will be verified and how this will be done as early on in the process as possible. Verification will include confirmation of qualifications and taking up references, which for example may be stated on the job advertisement or application form.

As stated above enforced subject access is a criminal offence. Where evidence of previous convictions is a genuine requirement of the post, an enquiry should be made of the Criminal Records Bureau (or Disclosure Scotland) under the provisions of the Police Act 1997.

If documents for verification are to be obtained from another organisation you must obtain a consent signed by the applicant.

Where information obtained as part of the verification process differs from that provided by the applicant, care must be taken not to simply assume that the applicant has been dishonest or misleading. Under the data protection principles it is the data controller's responsibility to ensure that data is accurate and processed fairly. As part of this process, the applicant should be asked to provide an explanation of any discrepancy before any decision is taken.

4. Shortlisting

In shortlisting the employer's main concern should be that the selection criteria is applied in a way that is both consistent and fair.

The Code does not seek to address practices where selection criteria may amount to unlawful discrimination on the grounds of sex, sexual orientation, race, religion or belief, age, or disability, although such actions will also breach the data protection requirement that personal data is processed fairly and lawfully. Methods used for shortlisting should be compared with good practice sources such as the Equality and Human Rights Commission.

The Act contains specific provisions on automated decision making. In order to fall within the provisions of the Act, the automated process must evaluate matters relevant to the individual, or the identification of the individual.

Where a decision is made by an automated process, for example, psychometric testing, then an applicant will have the right to have the logic involved in making

such a decision explained and also to have the decision itself reconsidered or retaken on different terms, including a non-automated process.

5. Interviews

The collection of personal data at interview, its recording, storage and use, will all represent processing within the scope of the Act. Again all personal information collected must be relevant to the position.

Applicants will normally be entitled to have access to interview notes about them which are retained by the employer, whether or not the applicant is ultimately successful in employment and this should be borne in mind when designing interviews, during the interviews and also as part of defending the application process against any challenge. Interview notes should be destroyed after a reasonable time, generally six months from completion of the selection process.

6. Vetting

In the Code this means actively making enquiries from third parties about an applicant's background and circumstances and goes beyond verification as described above.

The vetting process is particularly intrusive and should therefore be confined to areas of special risk. Limited vetting may be a legal requirement for some jobs, for example, under the Protection of Children's Act 1999. The Data Protection Act does not prohibit the use of vetting, but regulates how it may be carried out.

Routine vetting of all applicants will be hard to justify. Where possible, information should instead be gathered from the applicant and verified. Information revealed by vetting will only ever be relevant to a successful applicant.

Confirmation that vetting will be used must be made known to an applicant at the earliest opportunity. Preferably, this would mean noting that vetting will take place in the job advertisement.

As with the verification process, the employer should take steps to ensure that the information it receives from third parties is reliable and any discrepancy with information provided by the applicant should be investigated before a decision based on the vetting information is made.

Where information about third parties who may be associated with the applicant is to take place, those third parties must be made aware of the processing of their personal data, including information as to the purposes for which it will be processed. Where such third party information is not to be held, the Code

confirms that there would be no obligation to act on the basis that notification would be either impractical or disproportionate.

7. Retention of recruitment records

There must be a clear justification for retaining recruitment records once the process has been completed. Indefinite retention is unlikely to be justified. If the reason for retention is that the records may be necessary for the organisation to defend against any legal action arising from the recruitment, for example, discrimination this should only be to the statutory limitation period for bringing the action. An employer should establish a policy for the retention of any recruitment records based on a clear business need. In many cases information may be anonymised and identifiable details deleted. Such processes would be applicable in monitoring equal opportunities in the recruitment process and the success of specific recruitment campaigns for future reference.

Where an application is to be retained, for example, for future vacancies or opportunities other than a specific job advertised, the applicant must be made aware of this and given the opportunity to have their details removed. By this stage the employer should already have confirmed its procedures for the retention or deletion of applications.

Information gathered as part of the verification or vetting process should not be retained unless there is a clear legal obligation to do so. Where appropriate, confirmation that information has been verified or the vetting process has been successful will be all that is required for employment purposes.

Any information retained should be kept securely and regularly reviewed for relevance and accuracy in accordance with the charity's data protection policy.

Part 2 - Employment Records

For this part of the Code it is necessary to distinguish records containing sensitive data from those which do not. In this part of the Code the term 'sickness record' is used to describe a record of the details of an illness or condition responsible for a worker's absence; 'injury record' is used to describe a record of the details of an injury suffered and 'absence record' to describe a record of absence which may give the reason as either sickness or injury, but not the details of such sickness or injury.

Employers should restrict their records to absence records rather than sickness or injury records so far as possible.

1. Collecting and keeping records

It is not ordinarily necessary to obtain consent to keep employment records, but workers should be aware that records are being kept and given an explanation of the purposes they are kept for. Consent may be necessary for collecting sensitive data.

New workers should be informed and existing workers should be reminded from time to time of their rights under the Act. A sensible time for doing this might be with an annual personal details update, giving workers the chance to check the accuracy of their personal information.

2. Security

There is a security standard (ISO 27002:2005 "Code of Practice for Information Security Management") providing guidance on the main security risks relating to data records. Not all the recommendations will be relevant for all organisations, but the principles are generally applicable.

There should be a system of secure filing cabinets, access controls and passwords on computerised records so that only staff with a legitimate business need to access the information can do so.

Staff who do have access to such records must be reliable and background checks, such as references from previous employers, should be taken up for these staff. Their contracts should also contain confidentiality clauses concerning the use and confidentiality of such data.

There should also be systems for transferring such data and taking it off site.

3. Sickness and injury records

Check that where possible only absence and accident records are kept rather than any sickness and injury records. Where sickness and injury records are kept, these should be physically separate from other employment records and must satisfy one of the sensitive data conditions.

Absence, sickness and injury records should only be available to those who need access for their jobs. It is recognised that managers may need some access to enable them to manage their staff.

Information from sickness and injury records about an identifiable worker should only be disclosed where there is a legal obligation to do so or the worker has given their written consent.

4. Pension and insurance schemes

WRIGLEYS

— SOLICITORS —

These are often offered by external providers, but administered in house. The information gathered for such a scheme should only be used for that purpose and not general employment purposes. Only the minimum information required should be exchanged with the scheme provider. Workers should be told who will hold information and how it will be used.

5. Equal opportunities monitoring

Information about ethnic origin, disability, religion, and sexual orientation is sensitive data and so must satisfy a sensitive data condition. Where practicable the information collected should be anonymised and again should not be excessive. Forms should also be devised to ensure individuals are given adequate opportunities to describe themselves.

6. Marketing

If you use personal details for marketing or advertising purposes workers must be given an opportunity to opt-out.

You must not give workers' details to third parties for marketing or advertising purposes unless they have specifically opted-in. Also if it is intended to use details for a new purpose or a purpose that has not been previously explained to the worker the details should not be used unless workers have specifically opted-in.

7. Fraud or crime detection

Information about workers should not be disclosed unless there is a legal requirement to make the disclosure, you consider that non-disclosure would be likely to prejudice the prevention or detection of crime or the worker's contract of employment allows for such disclosure.

8. Subject access

Workers have a right of access to information about themselves held by their employer. You should have a system in place to recognise information access requests and respond to them promptly and at least within 40 calendar days of receiving the request.

Information relating to the worker may also relate to third parties, such as other workers, and you will need to balance the worker's right to information about themselves with any other person's rights such as an expectation that their information will be private. This will be particularly relevant to managers, for example the line manager of a worker who has conducted an appraisal of the worker.

Information should be given in hard copy form together with the sources of information. Any codes or abbreviations used should be accompanied with an explanation.

Perhaps the most important advice is to have a system which allows for production of information relating to a particular worker efficiently and quickly.

9. References and disclosure requests

References, including references to new employers, character references and financial references, generally disclose personal data.

It is important to have a clear policy on when and how references will be given and that references will only be given with the subject's consent.

As with all information which may identify third parties it will be necessary to consider a third party's rights before disclosing, or indeed withholding a reference from a worker.

With disclosure requests, you should only disclose when there is a legal obligation to do so. All the information requested should be judged separately. If the disclosure is to be made overseas, you should check there is a proper legal basis for making the disclosure.

Generally you should inform the subject if an unusual disclosure request has been made, unless this is prevented by law. For example, there are particular criminal offences of "tipping-off" persons in relation to money laundering, tax and some other criminal investigations.

Where publishing information about workers ensure there is a legal obligation to do so, that the information is not intrusive and does not allow the identification of individual employees without their consent.

Information should only be given to a trade union with the worker's consent.

10. Merger, acquisition and business re-organisation

Mergers, acquisitions and business re-organisation will inevitably involve disclosure of information about workers. To the extent possible such information should be anonymised. Personal information should only be released after confidentiality and non-disclosure agreements have been agreed.

Following a merger or acquisition the newly acquired records should be checked to ensure they do not hold excessive information.

11. Discipline, grievance and dismissal

Subject access rights apply equally to any disciplinary and grievance processes and matters. Records should be of sufficient quality to support any decisions made. Such information should be kept securely.

General employment records should not be used in consideration of disciplinary and grievance matters. Only records of substantiated matters should be kept unless there is an exceptional reason for keeping such information.

12. Outsourced processing

Many organisations outsource all or some of their HR functions. When outsourcing you should be satisfied that the service provider has sufficient security measures in place. The contract should provide that information is only processed in accordance with your instructions and will be held securely.

Part 3 - Monitoring at work

Before considering the Code itself it is advisable to consider the law applicable to monitoring. The Act does not prevent monitoring workers, but any monitoring must be done in a way that is consistent with the Act. However, the Regulation of Investigatory Powers Act 2000 also applies to employers as much as it applies to anyone else. It is primarily against the law to intercept an electronic communication, however there are exceptions for legitimate business aims.

Interception takes place if the contents of the communication are made available, during the course of its transmission, to someone other than the sender or intended recipient. Accessing stored collections of emails that have been received and opened or deleted by the intended recipient or accessing a stored collection of sent emails and checking telephone call logs showing the duration of telephone calls and telephone numbers does not amount to interception and are therefore not subject to RIPA.

The Telecommunications (Lawful Business Practice) (Interceptions of Communications) Regulations 2000 provides some exceptions relevant in the context of employment. The regulations set out when an employer is authorised to carry out an interception for the purposes of running its business.

Interception is allowed if the employer has reasonable grounds for believing that both the sender and recipient have consented. For this to apply there must be some action from which consent may be inferred, for example, proceeding with a telephone call after hearing a message saying that the call will be recorded.

Interception is not permitted by a business unless it is solely for monitoring (or recording communications) which:-

WRIGLEYS

— SOLICITORS —

- i. involve the business entering into transactions; or
- ii. relate in any other way to the business; or
- iii. take place in some other way in the course of carrying on the business.

These categories cover a very wide range of business communications but they will not include personal communications by an employee unless they relate to the business. The regulations

- do not permit an employer to open emails that can be identified as personal without opening them, and
- do not permit interception targeted at private communications regardless of whether or not the use of the system for such communication is permitted.

Where for example an employer seeks to monitor a policy prohibiting personal communication, this does not provide justification for interception and any interception will be unlawful.

The Code itself recognises that there are various good reasons for monitoring workers, not least to comply with legal obligations, but such monitoring can have a detrimental affect on the trust and confidence between employer and worker which is fundamental to the relationship. Any adverse affects on the worker must be justified by the benefits to the employer or others by conducting an impact assessment. Many employers do make some checks on the quantity and quality of work produced and most workers expect this.

1. General approach

Any monitoring is intrusive to workers who have a legitimate expectation to some privacy in their working environment and keep their private lives private.

Before introducing any monitoring you should be clear what benefit of such monitoring will bring and do an impact assessment to judge how workers will be affected. Where monitoring is used for quality purposes this should be made clear in a policy which workers are aware of outlining the extent and nature of such monitoring.

As with all other personal information, information collected through monitoring must be kept securely and if it involves sensitive data must be justified by satisfaction of at least one sensitive data condition. If information gathered through monitoring may have an adverse impact on workers you should allow them to make representations before taking any action.

2. Monitoring electronic communications

As described above, monitoring has to comply with Regulation of Investigatory Powers Act 2000. Before monitoring any communications you should carry out an impact assessment. Consider whether any less intrusive methods could be used to achieve the aim, for example automated systems for virus checking.

If you wish to monitor electronic communications, including telephone, fax, email and internet access or use, you should establish a clear policy covering the nature and extent of the monitoring and make sure it is implemented. Any policy should cover personal use of such facilities. Where workers are permitted to use email for personal messages your policy should include the marking of such emails as personal in the subject line. The policy should also cover situations when workers are out of the office; if their email or voicemail is to be checked, say so and alert them that personal messages may also be opened.

The policy should cover retention of records and statistics, including personal use. Include details of how the policy will be enforced and what penalties there are for breaches.

If any communications with customers are monitored make sure that the customer is aware of it and the purpose for such monitoring.

3. Video and audio monitoring

If any CCTV or other video and audio monitoring is considered conduct an impact assessment to check the purpose outweighs any negative impacts. Give workers and any visitors clear notice of where, how and why such monitoring is taking place.

4. Covert monitoring

Covert monitoring should only be used in the rarest circumstances, for example where there are grounds to suspect criminal activity or gross malpractice and that notifying individuals about such monitoring would prejudice its prevention or detection.

Any such monitoring should be limited in duration to the specific investigation and not of indefinite duration. You should not use such monitoring in areas which workers would reasonably expect to be private.

Any investigation should be subject to specific rules made for use of and access to the information. Any information found that does not relate to the investigation should be ignored and deleted or destroyed unless it is of another crime or malpractice or of a nature that no employer could reasonably ignore it.

5. Information gathered from third parties

You should tell workers what sources will be used to carry out checks and why the checks are being carried out. Notification will generally be by way of the application process or staff handbook for those engaged.

Workers conducting such checks should be properly trained in the use of such information and compliance with data protection rules. There should be as small a number of workers conducting such work and with access to the results as possible.

Information should not be retained unless there is a particular legal requirement. A record that a check has been conducted is sufficient.

Part 4 - Information about workers' health

Information recorded about workers' health will always be sensitive data for the purposes of the Act and so a sensitive data condition must be satisfied. Employers should also consider workers' rights to respect for private and family life under the Human Rights Act, where applicable.

There are a number of sensitive data conditions that will apply allowing information about workers' health to be collected. The most likely of these is to comply with legal obligations such as health and safety and not to discriminate. The condition that data can be collected with consent may well be met, but the relevance of such information may be questionable if none of the other conditions are met. Any consent given must be explicit and of their own free will, i.e. there can be no penalties for refusal to give consent.

Employers should remember that the Act requires review to ensure it is relevant, up to date and accurate.

1. General considerations

Before gathering any information about workers' health consider why the information is needed and conduct an impact assessment. Ensure that a sensitive data condition is met. Blanket consents should not be relied upon.

Information should be limited to fitness to work rather than general health matters. Where medical reports are required these should be focused on the ability of the worker to work rather than the medical details. Information that is collected for insurance or pension matters should only be used for those purposes.

Any information about workers' health should be kept securely and preferably separate from other personnel information.

2. Medical testing

Medical testing should only be used for enforcing rules and standards that are set out in a clear policy covering the purpose and sensitive data condition that is satisfied. The testing should be carried out at a time that the information gathered will be necessary and justified, for example it should only be carried out on applicants who are likely to be appointed.

There are limited justifications for carrying out testing, including whether the worker is fit to work, fit for the particular role, to meet legal requirements or for meeting pension or insurance scheme admission criteria. Where possible a less intrusive method, such as a health questionnaire, should be used.

Delete all information which is not relevant or up to date.

3. Drug and alcohol testing

Conduct an impact assessment before implementing any drug and/or alcohol testing policy. This is unlikely to be justifiable except for health and safety reasons. The policy should be clearly set out, including substances that are unacceptable together with levels which are unacceptable or zero-tolerance, and implemented and cover the consequences of failure to provide tests or failing a test.

Criteria for selecting workers to be tested should be clear and non-discriminatory. If testing is random ensure it is genuinely carried out at random. Random testing should also only be carried out on those persons whose work has a safety critical element. Random testing of all workers is unlikely to be justified. Random testing is less likely to be justifiable than post-incident testing where drug or alcohol use appears to be a factor.

Testing should be scientific and limited to substances that would have an affect on the functions for which the testing is carried out. Workers should also have a right to have a sample retested or dispute the findings of any test.

Freedom of Information Act 2000

The Freedom of Information Act 2000 was passed on 30 November 2000. The Act falls under the remit of the Information Commissioner and adds a dual role to the Data Protection Act functions.

The Freedom of Information Act gives a general right of access to all types of "recorded" information held by public authorities, and those providing services. The Act also sets out exemptions from the rights and places a number of obligations on public authorities.

Only public authorities are covered by the Act but this is widely defined to include Government departments, local authorities, NHS bodies (including doctors, dentists, pharmacies and opticians treating NHS patients), schools, colleges and universities. It also includes a long list of other public bodies ranging from various expert committees to regulators and organisations. It is intended to broaden the scope of those covered to include those who are carrying out services of a public nature, particularly in relation to care services, so in the near future will apply directly to many charities.

Other charities will come across freedom of information through contracts with public authorities. When a freedom of information request is made of the public authority they may well require information held by charities to be passed to them for consideration and disclosure, all within the same tight timescales as any other information held by them.

Under the Act public authorities have two main responsibilities.

First is a requirement to produce a "publication scheme" which is intended as a guide to the information that they hold which is publicly available. All public bodies should now have their publication schemes in place.

The second responsibility will be to deal with individual requests for information. The Freedom of Information Act extends the subjects access rights of the Data Protection Act 1999 to individuals to permit access to all the types of information that the public bodies hold, regardless of whether that information is personal or non-personal.

Anyone can make a request for information recorded both before and after the Act was passed. The Act gives an applicant the right to be told whether the information exists and the right to receive a copy or summary or the right to inspect a record of that information.

There are some twenty-three exceptions to the Act, some of which will be familiar from the Data Protection Act, for example, national security or law enforcement. Some exemptions apply to wide categories of information, for example, Court records and trade secrets and information relating to investigations or proceedings conducted by public authorities.

WRIGLEYS

— SOLICITORS —

In most cases where information is exempt, a public authority must consider the public interest in providing the information. This requires a consideration of the circumstances of each particular case and the exemption that covers information. There is an overriding rule that the information may only be withheld in the public interest if withholding it is greater than the public interest in releasing it. The most controversial decision to date involves the order for disclosure of cabinet minutes at which the Attorney General's legal advice on military action against Iraq was discussed. The Information Commissioner decided that the public interest in the information, including the accountability and transparency of government decisions was such that it outweighed the exemptions of formulation of government policy and ministerial communications. The Cabinet Office has appealed the decision to the Information Tribunal.

Freedom of information and data protection laws come together at a point where personal information is considered for disclosure.

A request by an individual for information about himself will be exempt under the Freedom of Information Act and will continue to be handled as a subject access request under the Data Protection Act.

There is some degree of tension between the two regimes, which has been the focus of legal debate for some years. The 2003 decision of *Durant v Financial Services Authority* gave a very narrow definition of personal data, which accordingly gave a broader scope to freedom of information provisions.

However, where an applicant specifically requests information about a third party or where responding to a request would involve the disclosure of personal information about a third party, the request falls within the remit of the Freedom of Information Act. In considering the application, the authority must however apply the data protection principles and therefore must not release third party information if to do so would mean breaching one of the data protection principles.

The Future

It is anticipated that there will be some substantial changes to the Data Protection Act. Following a successful freedom of information request it has come to light that the European Commission considers 11 of the Articles of the European Data Protection Directive have not been correctly implemented in the UK by the Data Protection Act; nearly one third of the Articles of the Directive.

For sometime lawyers have anticipated that a wider interpretation should be given to the definition of personal data. However, following the recent revelations it is also expected that there will be amendments to provisions covering the application to manual files, conditions for processing sensitive data, rights for data subjects, transfer of data, fair processing notices, exemptions, powers of the Information Commissioner and the

WRIGLEYS

— SOLICITORS —

penalties and remedies available. The Ministry of Justice have acknowledged that the European Commission has raised issues, but maintain that UK law and the Data Protection Act is compliant with the requirements of the Directive.

This note is prepared on the basis of The Information Commissioners:-

Employment Practices Code on Data Protection.

Further information available at www.ico.gov.uk and 01625 545745

Tim Wrigley
Trainee Solicitor

Malcolm Lynch
Partner

Chris Billington
Partner

Wrigleys Solicitors LLP
9 Cookridge Street, Leeds LS2 3AG
Tel: 0113 244 6100
Fax: 0113 244 6101
Email: tim.wrigley@wrigleys.co.uk

www.wrigleys.co.uk

This material does not give a full statement of the law but is intended for guidance and discussion purposes only. It is not a substitute for professional advice. No responsibility for loss occasioned as a result of any person acting or refraining from acting on the basis of the contents of this document is or can be taken by Wrigleys Solicitors.

DATA PROTECTION ACT 1998

SCHEDULE 1

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

DATA PROTECTION ACT 1998

SCHEDULE 2

**CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF ANY PERSONAL DATA**

1. The data subject has given his consent to the processing.
2. The processing is necessary-
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary-
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under any enactment,
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6.
 - (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
 - (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

DATA PROTECTION ACT 1998

SCHEDULE 3

**CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:
PROCESSING OF SENSITIVE PERSONAL DATA**

1. The data subject has given his explicit consent to the processing of the personal data.
2.
 - (1) 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.
 - (2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary-
 - (a) in order to protect the vital interests of the data subject or another person, in a case where-
 - (i) consent cannot be given by or on behalf of the data subject, or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing-
 - (a) is carried out in the course of its legitimate activities by any body or association which-

WRIGLEYS

— SOLICITORS —

- (i) is not established or conducted for profit, and
 - (ii) exists for political, philosophical, religious or trade-union purposes,
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing-
- (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
 - (b) is necessary for the purpose of obtaining legal advice, or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- 7.
- (1) The processing is necessary-
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under any enactment, or
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
 - (2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

WRIGLEYS
— SOLICITORS —

- 8.
- (1) The processing is necessary for medical purposes and is undertaken by-
 - (a) a health professional, or
 - (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
 - (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
- 9.
- (1) The processing-
 - (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
 - (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
 - (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
 - (2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

DATA PROTECTION ACT 1998

Basic interpretative provisions.

1.

(1) In this Act, unless the context otherwise requires-

"data" means information which-

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- (b) is recorded with the intention that it should be processed by means of such equipment,
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

"data subject" means an individual who is the subject of personal data;

"personal data" means data which relate to a living individual who can be identified-

- (a) from those data, or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

WRIGLEYS

— SOLICITORS —

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

"relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set 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.

"sensitive personal data" means personal data consisting of information as to:

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.