Data protection

Quick guide to the employment practices code

Ideal for the small business

ico.

Information Commissioner's Office

Contents

Section 1

About this guidance

This guidance has been produced with the needs of small businesses in mind. It is designed to help them comply with the Data Protection Act when recruiting and employing workers. It is based on the Information Commissioner's 'Employment practices code'. The code itself contains, in full, the Information Commissioner's recommendations on how to meet the legal requirements of the Act. You can refer to the full code if you need more information. It is available free of charge from our office.

Section 2

What is the Data Protection Act?

- The Data Protection Act applies to information about living, identifiable people, such as job applicants and workers.
- Through the data protection principles, it regulates the way information about them can be collected, handled and used.
- It also gives them rights such as access to the information, and compensation if things go wrong.
- It applies to computerised information and to well-structured manual records, such as certain files about job applicants.

Section 3

Recruitment and selection

Q How does the Act affect recruitment and selection?

- If you collect or use information about people as part of a recruitment or selection exercise, the Data Protection Act will apply. For example, you might obtain information about people by asking them to complete an application form or to e-mail their CV to you.

- The Act does not prevent you recruiting staff effectively. What it does is help strike a balance between an employer's need for information and an applicant's right to respect for their private life.

- The Act requires openness. Applicants should be aware what information about them is being collected and what it will be used for. Gathering information about an applicant covertly is unlikely to be justified

Q If I want to collect or use information about job applicants, what must I do?

- Make sure that when you place a recruitment advert you identify your organisation properly – people should know who they are applying to. If you are using a recruitment agency, make sure the agency identifies itself.
- Use the information you collect for recruitment or selection only. If you are going to use the information for any purpose that goes beyond this, such as to add names to your company's marketing list, you must explain this clearly.
- Ensure that those involved in recruitment and selection are aware that data protection rules apply and that they must handle personal information with respect.
- Do not collect more personal information than you need. It is a breach of data protection rules to collect personal information that is irrelevant or excessive. Design your application forms with this in mind.
- Do not collect from all applicants information that you only need from the person that you go on to appoint, such as banking details, or information you only need from applicants for particular jobs, such as details of motoring offences.

- Keep the personal information you obtain secure; it should not normally be disclosed to another organisation without the individual's consent.

- Only ask for information about criminal convictions if this is justified by the type of job you are recruiting for. Don't ask for 'spent' convictions unless the job is covered by the Exceptions Order to the Rehabilitation of Offenders Act 1974.

- If you are going to verify the information a person provides, make sure they know how this will be done and what information will be checked.

- If you need to verify criminal conviction information, only do this by getting a 'disclosure' about someone from the Criminal Records Bureau (CRB). Make sure you are entitled to receive this information and that you follow the CRB's procedures strictly. Only keep a record that a satisfactory/unsatisfactory check was made; do not hold on to detailed information.

- Only keep information obtained through a recruitment exercise for as long as there is a clear business need for it.

Section 4

Employment records

Q How does the Act affect the keeping of employment records?

- The Data Protection Act will generally apply to information you keep about your workers.
- The Act does not prevent you from collecting, maintaining and using employment records. However, it helps to strike a balance between the employer's need to keep records and the worker's right to respect for their private life.
- The Act requires openness. Workers should be aware what information about them is kept and what it will be used for. Gathering information about a worker covertly is unlikely to be justified.

Q If I want to collect, keep and use information about workers, what must I do?

- You don't need to get the consent of workers to keep records about them, but make sure they know how you will use records about them and whether you will disclose the information they contain.
- Ensure that those who have access to employment records are aware that data protection rules apply and that personal information must be handled with respect.
- Check what records are kept about your workers, and make sure you are not keeping information that is irrelevant, excessive or out of date. Delete information that you have no genuine business need for or legal duty to keep.
- Be careful when disclosing information in a worker's employment record. Remember that those asking for information about workers may not actually be who they claim to be.
- Data protection doesn't stand in the way where you are legally obliged to disclose information, for example informing the Inland Revenue about payments to workers. You should nevertheless be careful not to disclose more information than required.

- In some cases you will not be legally obliged 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 apply in criminal or tax investigations or where legal action is involved. You will still need to take care if confidential or other sensitive information is involved.

- In other cases you could breach the Act if you disclose. Only disclose if, in all the circumstances, you are satisfied that it is fair to do so. Bear in mind that fairness to the worker should be your first consideration.

- Don't provide a confidential reference or similar information about a worker unless you are sure that the worker would agree to this. If in doubt, ask the worker concerned.

- Let workers check their own records periodically. This will allow mistakes to be corrected and information to be kept up to date.

- Keep employment records secure. Keep paper records under lock and key and use password protection for computerised ones. Make sure that only staff with proper authorisation and the necessary training have access to employment records.

- Where possible, keep sickness records containing details of a worker's illness or medical condition separate from other less sensitive information, for example a simple record of absence. This can be done by keeping the

sickness record in a sealed envelope or in a specially protected computer file. Only allow managers access to health information where they genuinely need it to carry out their job.

- If you collect information about workers to administer a pension or insurance scheme, only use the information for the administration of the scheme. Make sure workers know what information the insurance company or other scheme provider will pass back to you as the employer.

- If you collect sensitive information to help monitor equal opportunities, for example about workers' disabilities, race or sexuality, only use the information for that purpose. Where possible use anonymised information, that is information that does not allow particular workers to be identified.

- If you intend to use the information you keep about workers to send marketing material to them, give them a chance to opt out before doing so. If you intend to pass on their details to another organisation for its marketing, then get the worker's positive agreement before doing so (that is, you should ask them to indicate that they do agree, rather than assuming they agree unless they say they don't).

- When you no longer have a business need or legal requirement to keep a worker's employment record, make sure it is securely disposed of, for example by shredding it.

Section 5

Monitoring at work

Q How does the Act affect monitoring?

- If you monitor your workers by collecting or using information about them, the Data Protection Act will apply. This can happen, for example, when you video workers to detect crime, when you check telephone logs to detect excessive private use, and when you monitor e-mails or check internet use.

- The Act doesn't generally prevent monitoring. However, it sets out principles for the gathering and use of personal information. In short, data protection means that if monitoring has any adverse effect on workers, this must be justified by its benefit to the employer or others.

- The Act requires openness. Workers should be aware of the nature, extent and reasons for any monitoring unless, exceptionally, covert monitoring is justified.

Q If I want to monitor my workers, what must I do?

- Consider why you want to carry out the monitoring. This might mean asking what problem you are trying to solve, for example theft in the workplace.

- Once you are clear about the purpose, ask whether the particular monitoring arrangement will truly bring the benefit you are looking for and whether it is justified by this benefit.

- Remember:
  1. Monitoring is usually intrusive.
  2. Workers legitimately expect to keep their personal lives private.
  3. Workers are entitled to some privacy in the work environment.

- Consider whether alternative approaches or different methods of monitoring would deliver the benefits you want while being more acceptable to workers. Can you target the monitoring at an area of risk, for example the part of your premises where you think theft is occurring?

- Ensure your workers are aware that they are being monitored and why. You could tell them this by putting a notice on a notice-board or signs in the areas where monitoring is taking place. If your workers have computers, you could send them an e-mail about the monitoring. If you are open about it, they will know what to expect.

- If monitoring is to be used to enforce your rules and standards, make sure workers know clearly what these are.

- Only use information obtained through monitoring for the purpose for which you carried out the monitoring, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore, for example breaches of health and safety rules that put other workers at risk.

- Keep secure the information that you gather through monitoring. This might mean only allowing one or two people to have access to it. Don't keep the information for longer than necessary or keep more information than you really need. This might mean deleting it once disciplinary action against a worker is over.

Q Are there other points to consider for particular types of monitoring?

- Be particularly careful when monitoring communications, such as e-mails, that are clearly personal. Avoid wherever possible opening e-mails, especially those that clearly show they are private or personal. Monitor the message's address or heading only.

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

- Where video or audio monitoring is justified, target the monitoring, where possible, at areas of particular risk, and only use it where workers wouldn't expect much privacy.

- Ensure that if you use information for monitoring which is held by third parties, such as credit reference or electoral roll information, you can justify this. Take particular care with any information you hold about workers as a result of non-employment dealings with them, for example where they are also your customers.

- If you are justified in obtaining information about a worker's criminal convictions for monitoring, only do so through a 'disclosure' from the Criminal Records Bureau.

- If you monitor workers through information held by a credit reference agency, you must tell the agency what you will use the information for. Do not use a facility for carrying out credit checks on customers to monitor or vet workers.

Q Can I ever undertake secret monitoring?

- The covert monitoring of workers can rarely be justified. Do not carry it out unless it has been authorised at the highest level in your business. You should be satisfied that there are grounds for suspecting criminal activity or equivalent malpractice, and that telling people about the monitoring would make it difficult to prevent or detect such wrongdoing.

- Use covert monitoring only as part of a specific investigation, and stop when the investigation has been completed. Do not use covert monitoring in places such as toilets or private offices unless you suspect serious crime and intend to involve the police.

Section 6

Information about workers' health

Q How does the Act affect the collection and use of information about workers' health?

- If you collect or use information about your workers' health, the Data Protection Act will apply. This might be the case, for example, when you ask workers to complete a questionnaire about their health or where you test them to check their exposure to alcohol or drugs.

- The collection and use of health information brings the Act's sensitive data rules into play. These do not prevent the processing of such information but limit the circumstances in which it can occur. You must be able to satisfy one of the sensitive data conditions.

- The Act sets out principles for the collection and use of health information. If you wish to collect and hold information on your workers' health, you should be clear about why you are doing so and satisfied that your action is justified by the benefits that will result.

- The Act requires openness. Workers should know what information about their health is being collected and why. Gathering information about workers' health covertly is unlikely ever to be justified.

Q If I want to collect or use information about my workers' health, what must I do?

- Consider why you want to collect and use this information. This might mean identifying a problem you are trying to solve, for example work that is impaired due to drug or alcohol use.

- Make sure that you can satisfy a sensitive data condition. You are most likely to do this if:
  - collecting health information is necessary to protect health and safety; or
  - the collection is necessary to prevent discrimination on the grounds of disability; or
  - each worker affected has given explicit consent.

- Bear in mind that if you rely on consent it must be freely given. This means a worker must be able to say 'no' without a penalty being imposed and must be able to withdraw consent once given. A person is more likely to be in this position at the recruitment stage than when they are employed.

- Once you are clear about the purpose and that you can satisfy a sensitive data condition, check that the collection and use of health information is justified by the benefits that will result.

- In doing so, remember that:
  - gathering information about your workers' health will be intrusive, perhaps highly intrusive;
  - workers can legitimately expect to keep their personal health information private and expect that employers will respect this privacy.

- Consider whether alternative ways of collecting information about your workers' health would deliver the benefits you want while being more acceptable to them. For example, you might use health questionnaires rather than medical testing or at least use a questionnaire to select those to be tested.

- Collect information about as few workers as possible. Collect health information in areas of highest risk only; in other words, consider whether you can involve only a few individuals whose jobs are critical to safety or who work in a hazardous environment.

- Keep information about workers' health particularly secure. This might mean allowing only one or two people to have access to it, for example by password-protecting it, or keeping it in a sealed envelope in a worker's file.

- Don't keep information for longer than necessary or collect more information than you really need. This might mean deleting medical details once disciplinary action against a worker is over.

- Remember that, as an employer, your interest is mainly in knowing whether a worker is or will be fit to work. As far as possible it should be left to doctors and nurses to have access to and interpret detailed medical information for you.

- Let your workers know that information about their health is being collected and why. You could give out general information about this by putting a notice on a notice-board or sending a letter to workers. If your workers have computers, you could send them an e-mail about it.

- Where you are taking a specific action, for example where a worker is to undergo a medical test, ensure the worker is fully aware what, why and how much information is to be collected. Be particularly careful that if they are referred to a doctor or nurse, they know what sort of information you will receive as a result.

Q Are there any other points to consider when collecting information through drug and alcohol testing?

- Collecting information by testing workers for drug or alcohol use is usually justifiable for health and safety reasons only.

- Where testing is used to enforce the business' rules and standards, make sure the rules and standards have been clearly set out to workers.

- Follow these guidelines:
  - Only use drug or alcohol tests where they provide significantly better evidence of impairment than other less intrusive means.
  - Use the least intrusive forms of testing that will bring the intended benefits to the business.
  - Tell workers what drugs they are being tested for.
  - Base any testing on reliable scientific evidence about the effect of particular substances on workers.
  - Limit testing to those substances and the extent of exposure that will meet the purpose(s) for which the testing is conducted.
  - Ensure random testing is genuinely random. It is unfair and deceptive to let workers believe that testing is random if, in fact, other criteria are being used.
  - Do not collect personal information by testing all workers, whether randomly or not, if only workers carrying out a particular activity pose a risk. Workers in different jobs will pose different safety risks, so the random testing of all workers will rarely be justified.

Section 7

What rights do workers have?

- Remember that workers have a legal right of access to information you hold on them. This includes information about grievance and disciplinary issues, and information you obtain through monitoring. Normally you must give access when a worker requests it, but you can withhold information where providing it to the worker would make it more difficult to detect crime.

- Make sure you have arrangements in place to deal with access requests properly and within the 40-day time limit stipulated in the law.

- When giving access to employment records be careful with information about other people. It could be wrong, for example, to disclose the identity of someone alleging harassment to the person accused of carrying out the harassment.

- If there is a discrepancy between what an applicant tells you and what you learn by carrying out a check, give the applicant an opportunity to give their side of the story. Remember that the information you get from a check could be wrong, particularly if it comes from public records.

- Allow workers to comment on or object to the information you gather through monitoring where it might adversely affect them. It may be that equipment or system faults mean that the information obtained through monitoring is inaccurate or misleading. Information from third parties may simply be wrong.

- Allow workers to comment about the health information you gather where it might adversely affect them. It may be that a medical test has not been carried out correctly, so you are holding inaccurate or misleading information.

- If a worker objects to you holding or using information about them because it causes them distress or harm, delete the information or stop using it in the way complained about unless you have a compelling reason to continue.

- Workers can claim compensation if they suffer as a result of a breach of the Data Protection Act, so it is in your interests to make sure records are well managed and used responsibly.

For further information about the 'Employment practices code', please visit the Information Commissioner's website at:

www.ico.gov.uk

where the full code is available.

If you have any queries you can contact our helpline on 0303 123 1113 or write to us at:

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

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

www.ico.gov.uk

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

November 2011

ico.

Information Commissioner's Office