

Your right to Privacy at work



Everyone has the right to a private life – even when they're at work. But new technology is making it easier than ever for employers to snoop on their workers.

The law can protect you from unwarranted intrusion into your private life.

This leaflet tells you where you stand.

Employers intrude on the privacy of their workers in a number of different ways.

Although employers will need to collect and record some personal details – such as your address, telephone number and date of birth, other more controversial forms of intrusion can include:

- › monitoring emails, telephone calls and use of the internet
- › CCTV or video surveillance
- › drug testing.

The law sets some limits on how far your employer can intrude on your privacy. This leaflet explains what those limits are.

But the law is often complex and we cannot deal with every factor that might affect you in a leaflet like this.

If you think you have a case or need further information or advice you should contact your union or one of the organisations listed on the back page of this leaflet.

The Data Protection Act 1998

Employers' obligations

Under the Data Protection Act 1998 (DPA), your employer must make sure your personal data or information is 'processed' in a fair and lawful way.

Processing includes obtaining, recording, storing, sharing, deleting and otherwise using information.

Your personal data is any information from which you can be identified – either on its own or when taken together with other information your employer holds about you – and which affects your privacy, either in your personal or family life or in your working life.

Occasional references to you in a set of minutes from a team meeting, for example, are unlikely to count as personal information. Neither will information about the workforce that has been anonymised, in a way that makes it impossible to identify any individual.

Common examples of personal data or information that your employer may hold are:

- › information supplied in an application form
- › details of your salary and bank account
- › details of your sickness record
- › an email about an incident involving you
- › details of your disciplinary record
- › an assessment of your work performance in a staff appraisal form.



Personal data can also include your image on a CCTV or video recording; information about your use of your computer and your use of the internet at work; an opinion your employer has expressed about you; and a record of anything your employer intends to do in relation to you.

Your employer must tell you what personal information is being recorded, why it is being recorded, who is likely to have access to it and for what reason.

Unless you have willingly given your employer permission to do so, they must not reveal your personal information to people who do not have a legitimate reason for seeing it. Your employer must also make sure that the information kept about you is accurate, relevant and up-to-date, and that it is not kept for any longer than is necessary.

Data protection law places additional obligations on your employer to protect “sensitive personal information”. This is information about your:

- › racial or ethnic origin
- › political opinions
- › religious or other similar beliefs
- › trade union membership
- › mental or physical health
- › sexuality or sexual life
- › alleged or actual criminal offences.

Your employer can hold and use this type of information about you only in limited circumstances.

Legal requirements

Your employer is required to keep certain records by legislation (for example for health and safety reasons, to make sure it is not discriminating on grounds of race, religion, sex or sexuality, or to keep records of statutory sick pay).

With your permission

If you have given your employer clear-cut permission to store personal information – preferably in writing – knowing fully what is involved, and no pressure has been put on you to give that permission, then they can do so. You must also be able to withdraw your permission at any time.

Your right to know

The Data Protection Act 1998 (DPA) gives you important rights to ask your employer about the type of personal information they hold about you, how that information was obtained, how it is being or will be used and who is likely to have access to it.

If your employer refuses to give you this information, you can complain to the Information Commissioner (see page 6). If you are a union member, speak to your union first – it may be able to help you resolve matters without the need for a formal complaint.

Your right to request

You can also write to your employer to ask for a copy of the personal information held about you, provided this is held either on a computerised system or on paper and is organised into a “relevant filing system” (in other words is held in a fairly sophisticated, structured filing system, so that the information about you is easily located).

You may be asked to pay a fee of up to £10 for this.

Your employer must respond to your



written request promptly, and in any case within 40 days of receiving the request together with any fee you have been asked to pay.

Your employer can refuse your request if releasing the information would:

- › involve a breach of confidence owed to someone else
- › involve what the law refers to as a “disproportionate effort”
- › damage ongoing negotiations between you and your employer (for example about pay).

Inaccurate information

You can ask your employer to correct, delete or destroy any personal information held about you that is factually incorrect. This could be especially important in relation to disciplinary records or information about your health.

If the information is an opinion rather than a fact, it can be challenged only if the opinion is based on wrong facts. If you disagree with an opinion that is based on correct facts, it may be worth asking for your own views about the information to be added to the record. However, your employer does not have to agree to this.

References

The DPA does not allow you to ask your current employer for a copy of any references it has provided on your behalf to a prospective employer. You can, however, ask your employer for copies of references supplied by your previous employer(s).

The Information Commissioner

The Information Commissioner is responsible for making sure that organisations respect people's right to privacy under the DPA. If you are unhappy about the way your employer is processing your personal information; or if your employer has refused your request to see what personal information it holds about you; or if your employer has refused to correct inaccurate information, you can make a complaint to the Commissioner. Contact details are at the back of this leaflet. If you are a union member, it would be useful to seek advice from your union first.

The Commissioner has recently published an Employment Practices Code. Although the Code is not a legal obligation in itself, by ignoring it your employer may be breaking some of the laws on which it is based. The Code covers:

- › monitoring at work
- › information about workers' health
- › employment records
- › recruitment and selection.

You can find the Code of Practice on the Information Commissioner's website at www.informationcommissioner.gov.uk

Monitoring at work

Legitimate monitoring

There are legitimate reasons why employers may wish to monitor their workforce, for example to prevent theft or to make sure people work safely. But excessive or unjustified monitoring of staff can cause stress, loss of trust and low morale.

Data protection law does not prevent employers from monitoring workers, but where monitoring involves collecting, storing and using personal information, it needs to be done in a way that complies with the law and is fair to workers.

Before deciding whether to introduce monitoring arrangements, your employer should:

- › be clear about the reason for monitoring staff
- › identify any negative effects monitoring may have on staff
- › consider whether there are any less intrusive alternatives.

Your employer should also consult with the trade union or other staff representatives. Except in extremely

limited circumstances, employers must tell staff about any monitoring arrangements and the reasons why they are being or have been introduced.

Monitoring email, internet and phone use

Your employer has no legal obligation to allow you to use the phone, email or the internet for personal reasons. However, good employers trust staff with some private use of the phone, internet and email as long as this does not interfere with their work.

To comply with data protection law, your employer must tell you of any plans to monitor email or internet use, and the reasons for doing so. Simply telling you, for example, that your emails may be monitored is not enough. You should be left with a clear understanding of when information about you is being obtained, why it is being obtained, how it will be used and who will have access to it.

Your employer has the right to access your email inbox or voicemail while you are away from work to deal with any business communications in your



absence, so long as you have been told that this will happen. But your employer should take care not to access communications that are clearly non-business related.

Make sure you've read and understood your employer's policy on email and internet use. Talk to your union representative if you have one, as they are likely to know of any policies that do exist.

If your employer does not have a policy, do not assume that your emails and use of the internet are not being monitored. Ask your manager to clarify what personal use of the internet and email is permitted.

A good policy will:

- › Make clear the extent and type of private use allowed – for example, restrictions on overseas phone calls or limits on the size or type of email attachments.

- › Specify clearly any restrictions on internet material that can be viewed or copied. A simple ban on “offensive material” is unlikely to be clear enough for workers to know exactly what is and is not allowed. Employers should at least give examples of the sort of material that is considered offensive, for example material containing racist terminology or images of nudity.
- › Spell out any restrictions on what can be sent, for example bans on sending or receiving sexually explicit material and bans on offensive statements based on race, sex, sexuality, disability, age, or religion.
- › Lay down clear rules regarding personal use of communications equipment when used from home.
- › Explain the reasons for any monitoring, its extent and how it is being done.
- › Outline how the policy is enforced and the penalties for breaching it.

Employers may be concerned that email sent from their domain (the part after the @ sign in your email address) might appear to be an official communication from them. In this case, and to avoid difficulties in general, it might be sensible to use another email account that you can use via the web for personal email. And, of course, you can take this with you if you change jobs.

CCTV and video surveillance

CCTV surveillance is one of the more intrusive forms of monitoring that an employer can use.

Employers may want to use CCTV or video surveillance for security reasons, such as theft, vandalism or threats to the safety of their staff. Before introducing CCTV surveillance your employer should carefully consider whether this type of monitoring is justified, or whether the same results could be achieved by using other, less intrusive methods. Continuous CCTV monitoring of particular workers will rarely be justified.

If your employer is using CCTV surveillance that records the activities of staff, you should be told where and why it is being carried out. CCTV surveillance should be targeted at areas only where particular risks have been identified and should not be used in areas where staff have a legitimate expectation of privacy - for example in toilets, changing rooms and private offices.

There may, however, be exceptional instances where your employer is justified in carrying out secret CCTV or video surveillance.



Covert monitoring

Covert monitoring is deliberately carried out in secret so that you are unaware of it (for example, listening in to phone calls without telling staff). It should be used only in very exceptional circumstances.

Your employer must have genuine reasons to suspect that criminal activity is taking place and that telling staff about the monitoring would put the investigation at risk. The Information Commissioner's Code of Practice says that it will be rare for covert monitoring of workers to be justified.

The Code also says:

- › Covert monitoring must only be used as part of a specific investigation and must stop once the investigation is complete.
- › If audio or video equipment is to be used, it must not be used in places such as toilets or private offices.

Vehicle monitoring

Technology increasingly allows employers to monitor vehicles used by workers off-site, such as company cars or delivery vehicles. Devices can record or transmit information such as the location of a vehicle, the distance it has covered and information about the user's driving habits.

If a vehicle is allocated to a specific driver, and information described above can therefore be linked to a specific individual, this will count as personal information under data protection law.

If you are allowed private use of the vehicle, your private journeys should not be monitored, unless your employer has to do so by law, for example to comply with rules on drivers' hours.

Information about your health

Information about a person's health is highly private and the Data Protection Act classifies health information as "sensitive" personal information. This means that the rules about sensitive personal information (see page 4) come into play whenever an employer wishes to record or use information about workers' health.

Health information can include information about a worker's disabilities or special needs, the results of an eye test, or a medical assessment of fitness to work. But a casual inquiry about your health from your manager, where no formal record is made of your reply, will not count as personal information under data protection law.

The rules do not prevent your employer from processing (collecting, storing and sharing, etc.) health information, but they do further limit the circumstances in which your employer can do so.

Collecting health information may be important to monitor health and safety where workers are exposed to hazardous substances, or to carry out adjustments or adaptations in the case of disabled workers, for example.



But before deciding to do so, your employer should take particular care to make sure that it is legally necessary to collect and hold this type of information, and that there is no practical, less intrusive way of achieving the same result. You must be made aware of the extent to which information about your health is held and the reasons for which it is held.

Your employer does not have the right to access or see a copy of any of your medical records unless you have willingly given them permission to do so. If you have given permission, you have the right to ask to be given a copy of any medical report before it is provided to your employer and the right to withdraw your permission once you have seen the report. You also have the right to ask the doctor to amend the report if you believe it is incorrect or misleading. If this is refused, you can ask for a statement of your views to be attached to the report before it is sent to your employer.

You can object to your employer holding or using information about your health if this is causing you harm or distress. Your employer should then delete the information or stop using it in the way you have complained about, unless it is essential to continue to hold or use the information. If you are a union member, you may want to talk to your union representative before making a complaint.

Sensitive data rules and health information

The questions below do not represent a full list of the conditions imposed by the 'sensitive data' rules. However, in order to comply with rules, an employer should be able to answer 'yes' to at least one of these questions:

- › Is the processing necessary to enable your employer to meet its legal obligations, for example, by collecting information about workers' disabilities to ensure that any reasonable adjustments are made?
- › Is the processing for medical purposes, for example the provision of care or treatment by an occupational health doctor?
- › Is the processing in connection with any actual or potential legal proceedings?

Particular care should be taken to make sure that health information is kept secure. Medical information about workers should be separated from other personnel information, for example by keeping it in a sealed envelope, or subject to additional access controls on an electronic system.

Sickness and absence records

Sickness and injury records of particular workers will count as health information where they detail the type of illness or injury suffered by the worker. The sensitive data rules will therefore apply. Your employer may need to record this type of information for Statutory Sick Pay purposes, to monitor health and safety hazards, or to assess capability.

Absence and accident records, which merely state the reason for the absence – for example sickness – but do not refer to a specific medical condition or to a specific injury sustained by a particular worker will not count as health information.

Your sickness and injury records should be kept separate from your absence and accident records. This will make it easier for your employer to ensure that your sensitive health information is only revealed to the very few people who need it (for example, the occupational health

doctor), whilst still being able to use absence and accident records to monitor levels of attendance or health and safety risks.

Information from drug and alcohol testing

Testing workers for use of drugs and alcohol is particularly intrusive. Data protection laws do not apply to the testing itself, but where information from the testing is linked to a particular worker and is collected, stored and/or used, then this will be classified as sensitive personal information.

The collection of information through drug and alcohol testing is unlikely to be justified unless it is for health and safety reasons. Employers should not test simply to find evidence of illegal drug use.

Unless required to test by law, your employer should first assess whether:

- › there is a serious risk to be addressed
- › the testing will provide significantly better evidence than other less intrusive methods.

You should be told what drugs are going to be tested for and you should be given the right to challenge the accuracy of test results by having any sample taken independently analysed.



The Human Rights Act 1998

The European Convention on Human Rights and the UK's Human Rights Act say that you have the right to respect for your private and family life, home and correspondence.

This right extends to your life at work, as well as your life at home.

In 1997, an employer who tapped an employee's telephone line without telling them was found to have violated her right to respect for her private life.

The Data Protection Act takes account of the Human Rights Act and employers who stay on the right side of it will also stay on the right side of the Human Rights Act.



Contacts

Information Commissioner

The Information Commissioner can investigate complaints about misuse of personal information under the Data Protection Act 1998. If you are unhappy about the way your employer is using your personal information, you can contact the Data Protection helpline.

T: 01625 545 745

www.informationcommissioner.gov.uk

Advisory, Conciliation and Arbitration Service (ACAS)

ACAS is a public body that promotes good workplace relations. Its national helpline answers employment questions and provides general advice on rights at work for employees and employers.

T: 08457 47 47 47 (9am-4.30pm)

www.acas.org.uk

Health and Safety Executive (HSE)

The HSE can provide advice and information on health and safety issues.

T: 0845 345 0055

www.hse.gov.uk

Citizens Advice Bureau (CAB)

Your local CAB office will be listed in your telephone directory. You can also visit www.citizensadvice.org.uk to find advice and information online.

Discrimination

If you think your problem may have a discrimination aspect, you might find the following helpful:

Commission for Racial Equality

T: 020 7939 0000

www.cre.gov.uk

Disability Rights Commission

T: 08457 622 633

www.drc.org.uk

Equal Opportunities Commission

Advice and support on sex discrimination matters.

T: 08456 015 901

www.eoc.org.uk

Lesbian and Gay Employment Rights (LAGER)

Helpline 12-4pm

T: 020 7704 8066 (women)

T: 020 7704 6066 (men)

Unions today – your friend at work

The rights described in this leaflet – and many others, such as the minimum wage – have been won by union campaigning. Without union help and assistance many workers won't get the full benefit of new rights to work.

Every day unions help thousands of people at work. Last year unions won a record £330 million compensation for their members through legal action. They won £1 million in equal pay claims – an average of £15,000 per member.

And of course unions help negotiate better pay and conditions, including far better provisions for family friendly employment than the legal minimums.

To find out more about joining a union call the TUC *Know Your Rights* line on **0870 800 4 882**.

www.worksmart.org.uk is the one-stop website for everyone at work. It provides a range of information about working life and your rights at work – whether you are a union member or not. The full text of this leaflet, plus the whole range of rights materials, is on the site – just a click away.

1

Trades Union Congress

Congress House, Great Russell Street, London WC1B 3LS

Tel: 020 7636 4030

www.tuc.org.uk