Unite guide for members

Privacy at work

Published by Unite the Union
General Secretary Len McCluskey

Updated 2013

Unite House
128 Theobald's Road
Holborn
London WC1X 8TN
Tel: 020 7611 2500

This guide book is downloadable in PDF format from
www.unitetheunion.org

CONTENTS

■ INTRODUCTION

In modern employment practices there is an increasingly thin line between the needs of employers and workers rights to privacy. On the one hand employers claim the need for protection against liability for criminal activity and harassment by other employees, the need to monitor the performance of their workforce and the need for public protection. The monitoring and surveillance of employees including the monitoring of electronic communication, email and internet use, telephone calls, CCTV, workplace performance and medical testing (including drug, alcohol and genetic testing) is becoming more and more common place. This activity however, has been described as the 'new industrial tyranny,' that critics claim amounts to the unacceptable invasion of workers privacy at their workplace. Monitoring and surveillance can also be divisive and counter-productive to good employment relations within the workplace.

This research guide outlines some of the issues for employees concerning privacy at work and how trade unions should negotiate to maintain the balance between what is acceptable and what is not. It addresses:

- Monitoring and surveillance of employees
- Medical testing, including tests for drugs and alcohol
- Holding of information by employers
- Stop and searches by the employer.

■ LEGISLATION

The 2 major pieces of legislation concerning workers rights to privacy are:

• The Data Protection Act 1998

• The Human Rights Act 1998 (came into force in 2000)

In addition, there is a contractual duty implied between employers and employees of "mutual trust and confidence. " This may be breached if the employer is found to have invaded a worker's right to privacy.

The Human Rights Act, which brings the rights enshrined in the European Convention on Human Rights and Fundamental Freedoms into force in the UK, requires all public bodies to take these human rights into account in their procedures and actions. This means that employees of public authorities may be able to take their employer to a tribunal if they believe they are in breach of the convention. For employees in the private sector the situation is less clear, but they may be able to rely indirectly on the convention, as statutory or common law rights must be interpreted in a way that takes account of convention rights.

Article 8 (1) of the convention says; 'Everyone has the right to respect for his private and family life, his home and his correspondence.'

Article 8 (2) states: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health, or morals, or for the protection of the rights and freedoms of others.'

■ DATA PROTECTION ACT 1998

The Data Protection Act 1998, which replaced the Data Protection Act 1984, strengthens an individual's right to access to personal information held on them, as well as to know why it is being held and who it is being passed to. Personal records were extended by the Act to cover manual, as well as computerised, records and CCTV footage. An individual can approach their employer to ask for access to their files. The employer should reply within 40 days and is entitled to charge an administration fee of up to £10.

There are eight data protection principles which state that data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the data subject's (worker's) rights
- Secure, and
- Not transferred to countries outside the European Economic Area without adequate protection for the individual.

The Act gives special protection to 'sensitive' personal data. This includes data on race or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sex life and criminal proceedings or convictions.

The Information Commissioner is responsible for enforcing the Act and can prosecute the data controller (person holding the information) for non-compliance. Employees are entitled to seek compensation through the courts for any damage caused as a result of the employer not complying with the requirements of the DPA.

■ CODES OF PRACTICE

The Information Commission has issued a code of practice, The Employment Practices Data Protection Code, published in four parts:

- Recruitment and Selection (part 1)
- Employment Records (part 2)
- Monitoring at Work (part 3)
- Medical Information (part 4)

The code explains the law in relation to data processing and sets out good practice recommendations for employers to help them comply with the law. It is not legally enforceable but can be used in evidence in any enforcement action against an employer. The code also contains important recommendations that can be used by union representatives in negotiations with employers on the issues below.

■ MONITORING AND SURVEILLANCE

Unions have becoming increasingly concerned by monitoring and surveillance techniques used by employers to record their every activity and monitor their performance in the workplace. Supervision and accountability have been replaced by video surveillance, smart cards, telephone eavesdropping, scrutiny of email and Internet access and productivity monitoring e.g. counting the number of keyboard strikes.

Monitoring and surveillance not only undermines worker's rights to privacy, it can also create high levels of stress and anxiety leading to ill health and poor performance. Performance monitoring (e.g. key board strikes) can also lead to physical health problems such as Repetitive Strain Injury and Carpal Tunnel Syndrome.

Not every workplace will be subject to CCTV or intensive performance monitoring but with the predominant use of technology in the workforce, more and more workers are likely to be affected by this issue. Unions therefore must engage with employers about monitoring and surveillance in the workplace.

■ LEGAL SITUATION

The legal situation in general is that surveillance or monitoring of employees is permissible as long as they have been informed that it is taking place. However, any form of secretive surveillance in the workplace, including CCTV, monitoring or interception of email or internet use, might be incompatible with the Human Rights Act, unless it can be justified for one of the reasons allowed by Article 8(2). This qualifies the right to privacy on certain grounds such as national security, public safety, and the economic wellbeing of the country, the prevention of crime or for the protection of health or morals. In the case of McGowan v Scottish Water [2005] IRLR 167 EAT, it was held that covert surveillance leading to dismissal for timekeeping fraud did engage Article 8 (right to privacy) but it did not breach it because the surveillance was not disproportionate given the nature of what was being investigated. However it must be emphasised that this area of law is largely untested so far.

NEGOTIATING A WORKPLACE CODE OF PRACTICE

One way of safeguarding privacy in the workplace is to agree a wide-ranging code of practice with the employer on surveillance and monitoring at work. This will let workers know what they can expect and what their rights are in relation to the information gathered about them. It will also commit the employers to certain basic principles protecting the privacy of employees and set out the precise form in which any monitoring is to be carried out.

The Data Protection Code part 3 sets out some core principles in relation to monitoring. These are:

- It will usually be intrusive to monitor your workers
- Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified; and
- In any event, workers' awareness will influence their expectations

The ITPA section of Unite has developed a draft code of practice for protection of privacy at work that is available at the end of this guide. (Appendix 1) It states clearly that the circumstances where surveillance and monitoring will be permitted are, 'to protect the safety, security and integrity of the organisation'. It should not be used to monitor workforce performance or hours of attendance.

The code recommends that employers should undertake an 'impact assessment' to decide whether the adverse impact of monitoring on individuals is justified by the benefits to the employer and others. The assessment should help decide if and how to carry out monitoring and whether monitoring is a proportionate response to the problem it seeks to address.

The impact should also:

- Clearly identify the purpose of the monitoring and the benefits it is likely to achieve
- Identify any adverse impact of the monitoring arrangements
- Consider alternatives to monitoring or different ways in which it might be carried out, e.g. investigation of specific incidents, spot checks, more training

- Take into account the obligations that arise from monitoring, e.g. how the information will be kept securely and handled in accordance with the DPA
- Judge whether the monitoring is justified

Trade unions should work with the employers to undertake the impact assessment and to consider alternatives to monitoring. The code recommends that if information gathered from monitoring is likely to have an adverse impact on workers, they should be presented with the information and allowed to make representations before any action is taken. This will of course be of particular importance where the action may be deemed relevant to disciplinary action within the meaning of the Employment Act 2008 which changed the way dispute resolution would be dealt with. Trade unions should ensure that the information gathered from monitoring should be used only for the purpose for which it was intended, e.g. to provide security or prevent crime. It should not be used for other purposes such as disciplinary procedures for other unrelated matters. Unions and employers should also be aware that video and audio systems can malfunction and provide misleading or inaccurate information. Information can also be misinterpreted or even deliberately falsified. Unions therefore must ensure that in the event of any disciplinary/grievance procedures, workers have the right to see the evidence and challenge it if necessary.

■ COVERT SURVEILLANCE

Under the Human Rights Act, secret surveillance of employees can be an infringement of their rights to privacy. It is only likely to be justifiable in extreme circumstances relating to national security, public safety or crime prevention. Secret surveillance relating to employees work performance, rather than any potential criminal activity, is therefore unlikely to ever be justified. Note however the decision of McGowan v Scottish Water detailed at page 7.

Union reps should be involved where any covert monitoring is suggested or put in place. They should ensure that the need for covert monitoring is justified and intended to deal with a specific threat to the organisation's safety, security or integrity. It should also be time-limited. The Unite ITPA code states, Covert monitoring or surveillance will only be permitted with the prior agreement of Unite representatives. The circumstances in which such monitoring could take place would normally be where there are serious grounds for suspicion of criminal activity or serious wrongdoing. Where covert monitoring or surveillance is agreed Unite representatives will have the right to audit such usage once the particular exercise has been completed.

The Employment Practices Data Protection Code provides the following guidance:

- Covert monitoring should not normally be considered. It will be rare for covert monitoring of workers to be justified; it should therefore be used in exceptional circumstances.
- Deploy covert monitoring only as part of a specific investigation and cease once the investigation has been completed: and
- If embarking on covert monitoring with audio or video equipment, ensure that this is not used in places such as toilets or private offices. There may be exceptions to this in cases of suspicion of serious crime but there should be an intention to involve the police.

■ MONITORING ELECTRONIC COMMUNICATION

E-mail and Internet are now in general use in most work places and indeed is encouraged by the government. Most employers now expect their workers to be familiar with electronic communication and to be able to use the Internet for business purposes. However the monitoring of web access and email content is also prevalent and there have been a number of cases where employees have been dismissed for inappropriate use of the systems. In April 2005 Unite lodged a complaint with the Information Commission on behalf of staff at the Association of Head Teachers concerning the unauthorised and possibly unlawful monitoring and interception of employee's emails.

As stated earlier, secret monitoring of email and Internet use is unlikely to be justified by the employers unless there are extreme circumstances. However, employers will want to protect themselves from legal liability if employees send defamatory or offensive emails using the company system. They will also want to limit Internet use, not only to restrict time spent on non-work activities, but also so they are not liable for the harassment of other staff caused by the display and downloading of pornographic or offensive material.

The Data Protection Code advises employers who wish to monitor their employees' use of electronic communications, including telephone, fax, voice-mail, Internet access and email should establish a policy on their use and communicate it to their staff. The policy should inform staff that their email and Internet use will be monitored and ensure that they know what is considered acceptable use and what is not. In a claim where the employer's written policy allowed staff to make 'limited and reasonable' personal use of email, a number of employees successfully claimed unfair dismissal following their dismissals for

abuse of the email system because it was unclear what 'limited and reasonable' meant and different managers applied the policy in different ways. [Lang v SP-Dataserve Ltd ET 103200].

To satisfy data protection requirements, a company's policy for the use of electronic communications should as a minimum:

- Set out clearly the circumstances in which employees may or may not use the employer's phone systems (including mobile phones), email system and the internet access for private communications
- Make clear the extent and type of private use that is allowed, for example any restrictions on overseas phone calls or limits on the size or type of email attachments
- Specify clearly any restrictions on Web material that can be viewed or copied. A simple ban on "offensive material" is unlikely to be sufficiently clear for workers to know what is and is not allowed. Employers should at least give examples of the sort of material that is considered offensive, e.g. material containing racist terminology or images of nudity.
- Advise employees what personal information they are allowed to include in particular types of communication, or the alternatives that should be used, e.g. communication with the company doctor should be sent by internal mail rather than email
- Lay down clear rules regarding personal use of communication equipment when used from home, e.g. facilities that enable external dialling into a company network
- Explain the purposes of any monitoring, its extent, and the means used
- Outline how the policy is enforced and the penalties for breaching it

A policy that clarifies the situation for staff is usually welcome and unions should be involved in drawing up the guidelines. It is inevitable that employee's private lives will encroach on their working lives and it is important that the policy recognises this and allows for reasonable personal use of the telephone, email and Internet. Local managers in conjunction with Unite reps should determine the definition of 'reasonable use'. Email and Internet are also very useful tools for union representatives for communicating with members and gathering information for union business. Access to this should also be included in any negotiations over electronic facilities. The ITPA sector of Unite has developed a model e-facilities agreement that is attached at the back of this guide (see Appendix 2). The Data Protection Code says that automated systems for monitoring may be preferable and less intrusive than monitoring of communications to or from workers. It also says that, wherever possible, employers should avoid opening emails, especially ones that clearly show they are private or personal. It encourages workers to mark any personal emails as such.

The code also says that employees should be informed that their mail boxes may be checked when they are off sick and that they should also be aware of the extent to which information about their internet access and emails is retained in the system and for how long. Unite recommends that any monitoring or retrieval of messages should only take place if the employer is legally obliged to do so or has a reasonable reason to believe that an employee has committed a criminal or seriously disciplinary offence. In such cases, e-mail will be monitored and retrieved only in the presence of union reps.

■ TELEPHONES

Workers in call centres almost always have their calls monitored. Employers argue that this type of qualitative monitoring is done to ensure that customers are given the correct information, to protect workers from false complaints from the public and for training purposes. However it can also be used to monitor performance and may even determine performance related pay in some places.

Secret recording and monitoring of employee's private telephone conversations has been held to be a breach of individual's right to privacy (Halford v UK [1997] IRLA 471). However, it may be permissible for employers to monitor telephone calls where staff have been informed that this is taking place. As with other forms of monitoring it is very important that unions and staff are informed and consulted over its operation.

The Data Protection Code says that like other forms of monitoring, telephone monitoring should only be used when the benefits justify the adverse impact.

If it is to be carried out, the following should be considered:

- If telephone calls or voice mails are monitored, or will be monitored in the future, consider carrying out an impact assessment
- If voice mails need to be checked for business calls when workers are away, make sure they know this may happen and that it may be unavoidable that some personal messages are heard, and
- In other cases, assess whether it is essential to monitor the content of calls and consider the use of itemised call records instead.

The code also says that workers should be made aware of the extent to which the employer receives information about the use of telephone lines in their homes or mobile phones provided for their personal use, for which the business pays partly or fully.

■ LOCATION TRACKING

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

Monitoring vehicle movements where the vehicle is allocated to a specific driver and information about the performance of the vehicle can be linked to them is allowed but regulated by the Data Protection Act.

Unite recommendations:

- Unite Representatives have been able to successfully argue in several cases that a less intrusive method of monitoring than fitting vehicle and other tracking devices manage to achieve the aims of performance management the employer wishes to see but are more 'privacy friendly' to the employee. For example, often it will not be the employer themselves that are collecting and monitoring the information it will be a contracted company. How can the employer be sure that any information collected on the employee will be secure? Who will have access to the information? On occasion employers have argued that they wish to introduce vehicle and other tracking devices under health and safety considerations, for example, to be alerted if an employee has an accident. It may be that a system of regularly checking in with an employer by mobile phone is a more 'privacy friendly' way of achieving this aim rather than constantly tracking someone.
- As mentioned above, any introduction of a vehicle or other tracking device should only take place after a clear and detailed policy on its use has been agreed with Unite and clearly and simply communicated to the workforce. Unite Representatives should ensure that such a policy includes the following points;
  - That prior to implementation, sufficient paid training will be provided to all employees on the use of the tracking system,
  - That the employer will clearly and simply explain to employees what information will be collected and how it will be used (this should include the current workforce but also any new joiners in the future),
  - That the employer will not use the tracking system to make any changes to productivity agreements between Unite and the employer,
  - That at no time (without the express authority of the employee or employees concerned) should any information from the tracking system be provided to an outside authority or authorities unless required by law,
  - The employer will verify that those asking for information about workers are who they claim to be and have the authority to request this information

before passing on this information. If this information is required to be provided by law then the employee or employees will be notified by the employer as to who has been provided with that information and given copies of the information. The employer will not disclose more information than is legitimately requested by the authority or authorities. If the information requested by an outside authority or authorities is available from another source other than the tracking system, this should be used rather than the information obtained by the tracking system,

- The employer will provide prior evidence that information from the tracking system will be held securely once the tracking system is introduced. If the employer contracts out this function to a third party to carry out the tracking system monitoring on their behalf then they will have clear contractual agreements governing the data collected, how it is used and that it is stored securely. This will be agreed with Unite representatives before it is contracted out to the third party,
- Those employees that use works vehicles privately for their own use in the evenings and at the weekend should be able to switch off the tracking system.
- Discussions must be had, and rules drawn up, about how the information will be used in disciplinary matters. Unite reps should try to ensure that the tracking data should not be used in this manner; if this cannot be agreed strict parameters about what is appropriate use, the full disclosure of information in such circumstances and other checks must be negotiated at the outset.

■ MYSTERY SHOPPERS

This is where the use of human 'spies' to go into a shop, bank or post office and pretend to be a customer, usually a difficult one, is used to test the staff. Unite does not see the need for mystery shoppers and has condemned the use of them. The union argues that managerial supervision and genuine customer feedback should provide the information that is needed. If they are to be used, it should be for training purposes only and any evidence gathered from a mystery shopper should not be used to initiate disciplinary procedures against staff.

■ MEDICAL TESTING

Employers have used medical testing for the following purposes:

- Screening of potential new employees
- Drug and alcohol testing of current employees
- Genetic testing (examination of DNA samples to determine whether there is a predisposition to a disease or condition.)
- HIV testing

■ DRUG AND ALCOHOL TESTING

Recent reports indicate that drug and alcohol testing has become more widespread in the UK over the last decade. In the US, testing has developed into a rapidly expanding industry where most major companies routinely test workers for drugs. Clearly employers will have legitimate concerns about worker's impairment due to drugs and alcohol, particularly in the safety critical industries (such as transport and engineering) where under the Transport and Works Act 1992 it is a criminal offence for certain workers to be unfit through alcohol or drugs. However, evidence suggests that testing is not effective in eliminating the problem and there are serious issues of privacy concerning the information that is gathered as a result. Testing is also by its nature intrusive and for those reasons, unions have in general resisted drug and alcohol testing unless there are overwhelming reasons for it that are supported by the staff.

Part 4 of the Information Commissioner's Office (ICO) code concerns medical testing. It says that drug testing at work can only be justified on health and safety grounds, and employers who test for drugs should have a proper system in place to ensure testing is done fairly. It also demands that employers should 'gather information through testing designed to ensure safety at work rather than to reveal the illegal use of substances in a worker's private life.'

The ICO code covers sickness and injury records, occupational health scheme, information from medical examinations and testing and drug, alcohol and genetic tests. It applies to job applicants, former applicants and former and current employees, agency staff, casual staff and contract staff. Others in the workplace, e.g. volunteers are also covered. Information concerning workers health is classified as 'sensitive data' and as such is given special protection by the ICO code.

Sensitive data can only be processed under strict conditions, which includes:

- Having the explicit consent of the individual
- Being required by law to process the data for employment purposes e.g. to ensure health and safety
- Needing to process the information in order to protect the vital interests of the data subjects or another, or
- Dealing with the administration of justice or legal proceedings.

Employers must identify who within the organisation can authorise or carry out the collection of information about a worker's health on behalf of the organisation and ensure they are aware of their employer's responsibilities under the Act. The employer should ensure that anyone involved in health information collection or medical testing is properly trained and the interpretation of medical information should be left to properly qualified personnel.

The ICO code advises that sickness and injury records should be kept separate from absence and accident records and that sickness or injury records should not be used for a particular purpose when records of absence could be used instead.

The code advises employers that, before obtaining information through drug or alcohol testing, they must ensure that the benefits justify any adverse impact, unless the testing is required by law.

It recommends that the employer should undertake an impact assessment, on similar lines to monitoring and surveillance, to identify the possible adverse impacts such as:

- The intrusion into the private life of staff and others
- Whether health information will be seen by those who should not, such as IT staff
- The impact on trust and confidence between employer and worker
- Whether the collection of health information will be oppressive or demeaning, e.g. collection of urine samples

The code effectively undermines blanket drug testing, stating that it is unlikely to be justified except on health and safety grounds. Random testing of all workers will also not be justified if in fact it is only workers engaged in particular activities that pose a risk. This applies even to safety critical businesses such as transport as workers in different jobs will pose different risks. For example, a train driver or signal engineer whose actions were impaired through exposure to alcohol or drugs would pose a significantly greater risk than a ticket inspector or administrator.

The code is clear that employers should have a drugs and alcohol policy that is accessible to all staff and spells out the consequences for workers of breaching the policy. Given legitimate concerns about the need to support workers who misuse alcohol and drugs, unions welcome alternatives to testing. The TUC has called on employers to draw up drug and alcohol policies in consultation with unions with an emphasis on confidentiality and assistance for workers who have drug or alcohol problems. The TUC's "Drunk or disordered" guide says that a workplace policy on drugs and alcohol should be comprehensive and should ensure that workers feel confident to report rather than hide problems.

The Health and Safety Executive's model policy on drug misuse contains the following elements:

- A statement of the policy's aims, and to whom it applies
- An indication of who is responsible for carrying out the policy
- A definition of drug misuse
- Rules about how employees are expected to behave

- Safeguards, making it clear that absence for treatment and rehabilitation is covered by normal sickness absence, and recognition that relapses may occur
- Assurance that employees with drug problems will be treated in confidence, subject to the law
- A description of support available to employees with drug problems, and a statement encouraging employees with drug problems to seek help voluntarily
- A commitment to providing all employees with general information about drugs and their impact on health and safety
- Details of the disciplinary procedures, for example stating that possession/ dealing will be automatically reported to the police.

Drugs and alcohol are not the only factors that may affect worker's health and impair their ability to do the job. Excessive working hours, work-related stress, bad working conditions, health and sleeping problems may have a greater impact on safety and should be included in any occupational health scheme.

MEDICAL TESTING TO SCREEN POTENTIAL APPLICATIONS

For job applicants, medical tests are only justified where there is a likelihood of appointment. Tests are only appropriate if they are needed to determine whether a person is fit or likely to remain fit to do a job, meet any legal testing requirements, or to determine eligibility to join a pension or insurance scheme. On employees the ICO code says, 'Only obtain information through a medical examination or medical testing of current workers if the testing is part of an occupational health and safety programme that workers have a free choice to participate in, or you are satisfied that it is a necessary and justified measure to:

- Prevent a significant risk to the health and safety of the worker or others, or
- Determine a particular worker's fitness for carrying out his or her job, or
- Determine whether a worker is fit to return to work after a period of sickness absence, or when this might be the case, or
- Determine the worker's entitlement to health related benefits, e.g. sick pay
- Prevent discrimination against workers on the grounds of disability or assess the need to make reasonable adjustments to the working environment, or
- Comply with other legal obligations

Information obtained in the course of medical tests that is not relevant to the purpose of the test must be permanently deleted.

■ GENETIC TESTING

Genetic testing has the potential to provide employers with information predictive of the likely future health of workers or with information about their genetic susceptibility to occupational diseases.

It has caused some concern to unions whose general policy has been to resist genetic testing in the workplace. Although there is little evidence so far that UK employers are using it to screen employees, such testing is on the increase in the US, so there are fears that the practice could follow here. The ICO code says clearly, 'only seek information through genetic testing as a last resort, where: it is not practicable to make changes to the working environment or practices so as to reduce risks to all workers, and it is the only reasonable method to obtain the required information.'

The Human Genetics Commission advises that employers should not demand that an individual take a genetic test as a condition of employment. It should therefore only be introduced after very careful consideration, if at all.

■ ACCESS TO MEDICAL RECORDS ACT 1988

Protection for employees for the use of confidential medical records by their employer without their consent is already enshrined in the Access to Medical Records Act 1998. It also gives employees the right to see a medical report before it is given to the employer and enables the employee to ask for changes to be made to it.

Section 3 of the Act provides that an employer must notify the employee before applying to a medical practitioner for a medical report to be used for employment or insurance purposes, and get the employee's written consent for this to be done.

A medical report is defined as "a report relating to the physical or mental health of the individual prepared by a medical practitioner who is or has been responsible for the clinical care of the individual." This definition would generally exclude any report prepared by a company doctor after a one-off examination, but if an employee has previously received treatment from a company doctor, i.e. "clinical care," then the employee will have access to any subsequent reports.

■ HOLDING OF INFORMATION BY EMPLOYERS

The Data Protection Act places responsibilities on any organisation to process personal data that it holds in a fair and proper way. Failure to do so can lead to a criminal offence being committed. The Information Commissioner's Code sets out some good practice recommendations on managing data protection. It says: "It is important to develop a culture in which respect for private life, data protection, security and confidentiality of personal information is seen as the norm."

Its advice to employers includes the following:

- Identify the person within the organisation responsible for ensuring that employment policies and procedures comply with the Act
- Assess what personal information about workers is in existence and who is responsible for it
- Eliminate the collection of personal information that is irrelevant or excessive to the employment relationship. If sensitive data are collected ensure that a sensitive data condition is satisfied
- Ensure that all workers are aware how they can be criminally liable if they knowingly or recklessly disclose personal information outside their employer's policies and procedures. Make serious breaches of data protection rules a disciplinary matter, and
- Consult workers and/or trade unions or other representatives, about the development and implementation of employment practices and procedures that involve the processing of personal information about workers.

Part 1 of the ICO code deals with recruitment and selection. It provides benchmarks on:

- Advertising
- Applications
- Verification
- Short listing
- Interviews
- Pre-employment vetting
- Retention of recruitment records
- Disclosure of criminal convictions.

■ CRIMINAL RECORDS

The Rehabilitation of Offenders Act 1974 allows individuals whose convictions are regarded as 'spent' after a period of rehabilitation the right not to have to declare their convictions when applying for a job. The period of rehabilitation varies according to sentence and age when convicted, although sentences in prison, youth custody or a young offender's institution of thirty months or more are never spent. Some jobs however are considered exempt from the Rehabilitation of Offenders Act and convictions have to be disclosed, whether spent or not. These include teachers, social workers, nurses and those involved in upholding the law. The government established the Criminal Records Bureau (CRB) to provide information to employers about applicant's criminal records. It applies to posts exempted from the Rehabilitation of Offenders Act and relates particularly to certain sensitive areas of employment such as posts involving regular contact with children or vulnerable adults.

■ EMPLOYMENT RECORDS

Part 2 of the Employment Practices Data Protection Code deals with employment records and aims to help employers strike a balance between the employer's need to keep records and the worker's right to respect for his or her private life.

■ SICKNESS RECORDS

The code says that sickness and accident records will include information about worker's physical or mental health and will therefore involve the processing of personal data.

It recommends that:

- Sickness and accident records should be kept separately from absence records (i.e. those that may give the reason for absence as sickness, but contain no medical information) and should not be used for a particular purpose when records of absence could be used instead;
- Employers should only disclose information from sickness or accident records about a worker's illness, medical condition or injury where there is a legal obligation to do so, where it is necessary for legal proceedings or where the worker has given explicit consent to the disclosure; and
- Employers do not make the sickness, accident or absence records of individual workers available to other workers, other than to provide managers with information about those who work for them in so far as this is necessary for them to carry out their managerial roles

■ DISCIPLINE, GRIEVANCE AND DISMISSAL

The Data Protection Act applies to personal data processed in relation to discipline, grievance and dismissal proceedings.

The ICO code recommends that employers:

- Do not access or use information kept about workers merely because it might have some relevance to a disciplinary or grievance investigation if access or use would be either: incompatible with the purpose(s) the information was obtained for, or disproportionate to the seriousness of the matter under investigation
- Ensure that there are clear procedures on how 'spent' disciplinary warnings are handled, and
- Ensure that when employment is terminated the reason for this is accurately recorded and that the record reflects properly what the worker has been told about the termination

■ RETENTION OF RECORDS

The Data Protection Act does not specify a period for which data may be held, it merely requires that the personal data in a record shall not be kept for longer than is necessary for a particular purpose.

The ICO code recommends that:

- Retention times for information should be standardised and based on business need
- Data should be anonymous where practical
- Any information on criminal convictions of workers is deleted once the conviction is 'spent' under the Rehabilitation of Offenders Act
- Records that are to be disposed of are securely and effectively destroyed

■ STOP AND SEARCHES OF EMPLOYEES

Situations may arise when employers want to conduct searches of employees and their property, for example in cases of suspected theft or where there is concern about employees using or dealing in illegal drugs on the premises. Under the Misuse of Drugs Act 1971 an employer may be committing a criminal offence if an employee supplies drugs prohibited by that Act on the employer's premises.

Prior to the Human Rights Act 1998, employees did not have a statutory right to privacy. However, under Article 8 of the Human Rights Act, the courts now apply the concept of a 'reasonable expectation of privacy' as a basis for determining whether Article 8 has been infringed in the workplace. Public sector employees can now bring a direct claim against their employer if their right to privacy at work has been infringed under Article 8.

Interference with the employee's right to privacy may be justified where the employer can make out three conditions:

1. That in conducting the search he was acting in 'accordance with the law'
2. That his actions were in pursuit of a legitimate aim
3. That the measure according a right to search was 'necessary in a democratic society' and proportionate

However, case law in this area has not developed sufficiently to determine the extent and breadth of these qualifications to an employee's rights to privacy in the workplace.

An employer is entitled to make provision in the contract of employment for those circumstances in which he/she intends to stop and search employees. Any employee who enters into a contract on those terms may therefore be presumed to have consented to the employer's exercising that right and the employee refuses the search, he/she may be in breach of contract.

However, an employer must take care not to breach the duty of mutual trust and confidence implied in every contact by the manner is which the search is carried out, particularly if a body search is carried out.

If there is no provision in the contract of employment authorising an employer to stop and search an employee, the employer may still evade liability based on breach of contract if a search is carried out and the employee willing consented to it. However if an employee refuses to provide their consent, he/she will not be in breach of contract. The law in principle protects everybody against any form of physical molestation and any infringement of that right constitutes the common law offence of battery. Where an employer conducts a forcible search of an employee's body, such action might also constitute assault and false imprisonment.

Where an employer catches an employee in the act of committing a crime or suspects that he or she is in the act of doing so, the employer has the 'citizen's power of arrest,' contained in S.24(4) of the Police and Criminal Evidence Act 1984. Any employer may therefore stop and detain any person who is in the act of committing an arrestable offence or whom he has reasonable grounds to suspect is committing an arrestable offence. The purpose of the arrest is to detain the person until the police arrive. The citizen's power of arrest does not include a power to search.

Stop and search checklist

- A policy on stop and search should make clear the reasons for the search; who will carry out the search, where searches will take place, what the employer is looking for and how employees will be chosen
- Staff carrying out searches, especially random searches must be trained so that they do not discriminate on grounds of race, gender, religion etc.
- Employers should consider non-invasive methods of searching. Where this is not possible, someone of the same gender should carry out searches in private
- Employee consent is crucial even where the employer has a contractual right. Without consent, a search could amount to a criminal assault and the employee may be entitled to bring a civil claim for personal injury against the employer and/or the person who conducted the search

APPENDIX 1

■ DRAFT CODE OF PRACTICE FOR PROTECTION OF PRIVACY AT WORK

Objectives

1. The objectives of this code of practice are to define the manner in which any personal data relating to employees is permitted to be processed and the circumstances where surveillance and monitoring of employees of the organisation will be permitted in order to:

a. Protect the safety, security and integrity of the organisation as employer.

b. Protect the privacy of the employees of the organisation.

General principles

2. Personal data includes all information held about identified or identifiable employees and includes, but is not limited to information in electronic or hard-copy, expressions of opinion about and intentions towards an employee, photographic film, video and sound material.

3. Personal data relating to an identified or identifiable employee or group of employees shall not be processed, collected, stored, combined or communicated except in accordance with this code of practice.

4. Data processing including the collection, storage, combination, communication or any other use of personal data will be carried out with the aim of minimising the collection of personal data and maximising the privacy of employees.

5. Personal data will only be processed in a way which is compatible with the original purpose for which it was collected.

Individual rights

6. Employees will be regularly notified of personal data held about them, have the right of access and to obtain a copy of any records of personal data without charge and the right to correct or destroy any incorrect or incomplete personal data.

7. Where any personal data is processed which may give rise to criminal or disciplinary proceedings, the data will be made available to the employee and his/her Unite representative in connection with such proceedings if requested for the purposes of representation.

8. Medical personal data will only be collected if needed:

    1. To establish whether an employee is fit for a particular job or area of work.

    2. To fulfill the requirements of occupational health and safety.

    3. To determine entitlement to and/or to grant social insurance, pension or sickness/ill-health benefits and such data will only be collected with the agreement of the employee and in accordance with medical confidentiality and general principles of occupational health and safety.

9. No personal data will be collected in connection with membership of Unite or Unite the Union activities except with the agreement of the employee and the union.

10. The normal rules on the making and receiving of personal telephone calls will apply.

Collective rights

11. Unite representatives will be consulted with a view to seeking agreement on:

    1. The introduction or modification of automated systems that process employees' personal data.

    2. The introduction of any overt electronic monitoring of employees' behaviour in the workplace in advance of any such monitoring being introduced.

    3. The purpose, contents and manner of administering and interpreting any questionnaires and tests concerning the personal data of employees.

12. Alcohol and drugs testing will only be carried out with the prior informed consent of the employee and must form part of an explicit health information, education and rehabilitation policy except where explicitly authorised by legislation or regulatory authority.

13. Genetic screening will not be permitted except where explicitly authorised by legislation or regulatory authority.

Communication of personal data

14. No personal data will be communicated to a third party without the consent of the employee except where this is:

    1. Necessary to prevent serious and imminent threat to life or health.
    2. Required by law or regulatory authority.
    3. Necessary for the conduct of the employment relationship.
    4. Required for the enforcement of criminal law.

Monitoring and surveillance of employees

15. Surveillance means the use of any device or person to record the location, movement and/or behaviour or identifiable individuals and includes the use of computers, video and closed circuit TV, sound devices, telephones, systems for establishing identity and location and undercover clients/ customers and private investigators.
16. Continuous overt monitoring or surveillance will be carried out only if required for health and safety, training or the protection of organisational assets or property.
17. Covert monitoring or surveillance will only be permitted with the prior agreement of Unite representatives. The circumstances in which such monitoring could take place would normally be where there are reasonable grounds for suspicion of criminal activity or other serious wrongdoing. Where covert surveillance is agreed Unite representatives will have the right to audit such usage once the particular exercise has been completed.

APPENDIX 2

■ MODEL E-FACILITIES AGREEMENT

Access to electronic mail

1. Unite representatives have the right to use the corporate email system for works council/trade union purposes, to send and receive emails both internally and externally. This shall include the right to send email communications to all employees, subject to this right being exercised reasonably. There shall be a further right to operate electronic bulletin board or discussion list services within the corporate email service, provided such facilities are technically possible.
2. Employees have the right to use the corporate email system to communicate with their Unite representatives and officials.
3. Employees are permitted to use the email service for non-business use during business hours to send and receive individual emails both internally and externally provided that this is not detrimental to their job responsibilities.
4. The employer undertakes that email will not be routinely read or monitored. Email will be monitored and retrieved only if the employer is legally obliged to do so or has reasonable reason to believe that an employee has committed a criminal offence or serious disciplinary offence or is in breach of this agreement. In these situations, email will be monitored and retrieved only in the presence of Unite representatives.
5. The right of employees to send and receive emails is subject to the following conditions:
    1. Email sent must be lawful and not include defamatory or libellous statements.
    2. Email shall not be used as a means of sexually harassing other members of staff. Email shall not be used for sending offensive comments based on an individual's gender, age, sexuality, race, disability or appearance.
    3. If required by the employer, personal email sent both internally and externally shall include a disclaimer to the effect that the views expressed are those of the author's alone and not necessarily those of the company.

Access to the internet

1. Unite representatives have the right to access the internet through the company server.
2. Unite representatives have the right to create their own website using facilities on the company's intranet or internet server, provided such facilities are technically available. Unite will have the right to include such material as it feels is appropriate on its website.
3. Limited non-business use of the internet by employees is permitted during business hours, provided that it does not interfere with job responsibilities.
4. The employer reserves the right to monitor use of the internet by employees and, if necessary, prevent them having access to it if they feel that it is being used excessively for purposes unconnected to work and/or if it is interfering with job responsibilities.
5. Employees have the right to access intranet or internet sites run by Unite and other sites which are concerned with employment issues, health and safety, equality issues or other matters relevant to their rights at work. Employees have the right to participate in internet based newsgroups (such as Usenet newsgroups) relating to these issues.
6. It is not permitted knowingly to access websites with sexual or pornographic material, or those which promote or encourage racism or intolerance.

Unite the Union
Unite House
128 Theobald's Road
Holborn
London WC1X 8TN
Tel: 020 7611 2500
www.unitetheunion.org

ES/3641-11/RG PRIVACY AT WORK