Data protection, surveillance and privacy at work

Member resource

The law is stated as at 02 April 2009
Please click on the individual questions below to see the answers.

- **What legislation governs data protection, surveillance and privacy at work?**

The main legislation governing data protection is the Data Protection Act 1998 (DPA) which came into force on 1 March 2000.

The DPA implements an EU Directive (the Data Protection Directive 95/46/EC) and both the Act and the Directive aim to give individuals rights in connection with the processing of manual and computerised personal data and on the movement of such data.

Other important statutory provisions concerning data protection include the following:

- Human Rights Act 1998
- Freedom of Information Act 2000 (FOI Act) (only applicable to public authorities)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/2905)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- The Environmental Information Regulations 2004 (SI 2004/3391)
- The Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI 2006/2068.
- Criminal Justice and Immigration Act 2008.

Information and guidance is available from the Information Commissioner's Office (ICO) website - see question below on where guidance and help on the DPA can be found.

- **What is the Information Commissioner's Office?**

The Information Commissioner's Office is a UK independent supervisory authority reporting directly to the UK Parliament which ensures that organisations which process data do so in compliance with the Data Protection Act 1998 (DPA), Freedom of Information Act 2000, (FOI Act) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and the Environmental Information Regulations 2004 (SI 2004/3391). Among other responsibilities the Information Commissioner’s office does the following:

- publishes guidance and develops codes of practice designed to assist individuals and organisations comply with the legislation
- maintains a public register of Data Controllers under the DPA and the list of public authorities with approved publication schemes under the FOI Act
- prosecutes persons in respect of offences committed under the legislation.
- Vist the Information Commissioner's Office website

- **Where can guidance and assistance on interpretation of the Data Protection Act be found?**

The website of the Information Commissioner is the most comprehensive source for guidance as to good practice.

The Information Commissioner has published codes of practice, good practice notes, technical guidance notes and other guidance. The guidance evolves and develops over time to reflect new case law and the practical experience gained as the Data Protection Act 1998 is applied.

The Codes and guidance are not legally enforceable. However, any breach or disregarding of the principles supplied may be relied on by the Commissioner in any enforcement action. The main *Employment practices data protection code* is in four parts which have now all been published in a single document:

- Part 1: Recruitment and Selection
- Part 2: Employment Records
- Part 3: Monitoring at Work
- Part 4: Information about Workers Health.

The code takes account of *Durant v Financial Services Authority [2003] EWCA Civ 1746, CA* and amends the definitions of 'personal data' and 'relevant filing sytem' - see questions below on what data does the DPA apply to and manual personnel files.

The detailed guidance governs the four areas listed above and also for example:

- use of CCTV
- Telecommunications Directory Information and Fair Processing.

There is also useful special guidance for small businesses.

The eight data protection principles are given on the Information Commissioner's website. (See question below on the data principles).

- Go to Information Commissioner's website

- **What is data protection and what are the eight data protection principles?**

In essence data protection means that those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles.

Those about whom data are processed (data subjects) are also provided with a number of rights which they may use to access certain information about them, as well as control the way in which it is processed in some cases.

There are eight principles put in place by the Data Protection Act 1998 (DPA) to make sure that your information is handled properly.

The principles specify that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than is necessary
- processed in line with your rights
- secure
- not transferred to countries outside the EU without adequate protection.

It is against the law if a data controller, for example an employer, does not keep to these principles.

The eight data protection principles are given on the Information Commissioner's website.

- View guidance on Information Commissioner's website

It is worth emphasising that the above principles have given rise to many common misunderstandings. The Information Commissioner's Office (ICO) urges organisations not to hide behind the DPA unnecessarily. Organisations (including employers) are urged to think through whether they can respond to enquiries from individuals rather than using data protection as an excuse. A common sense approach is required with all data protection matters.Examples of absurdities resulting from a misunderstanding of the DPA includes the misapprehension that the DPA stops parents from taking photos in schools. In fact photographs taken purely for personal use are exempt from the DPA although the DPA may apply if photographs are taken for official use by schools and colleges and these images are stored with personal details such as names.

- **Does the Data Protection Act only apply to data processed in relation to employees?**

No, the Employment practices data protection code (see above question on interpreting the Data Protection Act 1998) refers to 'workers'. Examples of who would be classified as a worker are as follows:

- job/work applicants (successful and unsuccessful)
- former applicants (successful and unsuccessful)
- employees (current and former)
- agency workers (current and former)
- casual workers (current and former)
- contract workers (current and former)
- volunteers and those on work
- placements.

The Data Protection Act 1998 must be complied with when an employer provides information about the transfer of a business to which the Transfer of Undertakings (Protection of Employment) Regulations (TUPE) applies. TUPE requires that certain information is provided to the new employer before the transfer takes place including details of pay, hours, holiday entitlement and any details of disciplinary / grievance action relating to employees. Both parties must consider their data protection obligations early in the transfer process and only pass on accurate, current and secure information required by the new employer. In 2008 the Information Commissioner's Office issued new guidance on transfer of employee information in a TUPE transfer which is available on the ICO website.

- View guidance

- **What data does the Data Protection Act apply to? Are videos, CCTV and emails covered?**

The Data Protection Act 1998 (DPA) can apply to computerised and manual records, photographs, CCTV footage, mainframes, laptops, organisers, palm pilots, audio and video systems, telephone logging/surveillance systems, microfiche and microfilm.

The definition of data falling within the DPA is complex. It includes information:

- which is personal data ('personal data') relating to a living individual, and
- includes any expression of opinion about the individual and/or
- includes an indication of the intentions of the data controller or any other person in respect of the individual.

The individual must be identified from the data (or from the data and other information which is in the possession of the data controller).

The data must also be:

- processed by means of equipment operating in response to instructions given for that purpose, or
- recorded with the intention that it should be so processed, or
- recorded as part of a relevant filing system, or
- form part of an accessible record.

The Durant case

There has been confusion and litigation over what types of information and filing systems fall within the definition of data but in the case of *Durant v Financial Services Authority [2003] EWCA Civ 1746, CA* the Court of Appeal gave some guidance – please also see question below on manual filing systems below.

Essentially the Financial Services Agency (FSA) refused part of an applicant's request for access to data which included a file containing a few documents.These documents mentioned Mr Durant's complaint together with other complaints in a file which was divided alphabetically according to complainants' names.

The key points from the case were:

- That the DPA only applies to **manual** systems if they provide similar sophistication of access to that provided by a computer system in finding a file, or any particular information it contains. A system that requires an employee to search through files fell outside the definition.
- The mere mention of a name in data does not make it personal data. The data had to be about the employee, there was no need to disclose data if the employee was not the focus of the data or if it was not biographical.

Post Durant case developments

Following *Durant, t*he EC Article 29 Data Protection Working Party adopted an opinion on the concept of personal data by a European data protection advisory committee which gave 'personal data' an even wider interpretation to enable employees to see more information.The Opinion was adopted in June 2007 and the Information Commissioner revised its previous guidelines.

Although employees now appear entitled to see more information, every document merely mentioning an individual's name does not have to be disclosed. The following is a summary of the key points which govern the decision of what 'data' is 'personal' for the purposes of the DPA following the revised guidance. Employers should look at each subject access request individually. Personal data will include that which is obviously about an individual or clearly linked to them. In other cases it may be necessary to consider if the data:

- has biographical significance*
- can be used to inform or influence a decision about an individual

- focuses or concentrates on an individual as its central theme rather than some other person, object or transaction
- is linked to an individual so that it provides information about that person
- affects a person's privacy, whether in his personal or family life, business or professional capacity
- is capable of having a potential impact on an individual.

*For example data will be included even if it merely records an individual's whereabouts at a particular time or involvement in a matter or an event. An attendee in the minutes of a meeting does have biographical significance because the minutes record the individual's whereabouts at a particular time. (Although the disclosure may only be limited to the list of attendees, depending on the content of the meeting.).

The following are other examples of personal data:

- information about the medical history of an individual,
- an individual's salary details,
- information concerning an individual's tax liabilities,
- information comprising an individual's bank statements,
- information about individuals' spending preferences,
- information, for example about a house or a car, could be personal data because that information is directly linked to an individual, and
- marketing lists containing a name together with contact details such as address, telephone number and e-mail .

As referred to above, the Information Commissioner published revised guidance on 'personal data' in August 2007. This can be found with other guidance on the DPA, including the use of CCTV systems, on the Information Commissioners's website.

- View guidance on personal data
- View guidance on cctv systems

- **After the Durant case are manual personnel and other manual files likely to be covered by the Data Protection Act?**

Although *Durant v Financial Services Authority [2003] EWCA Civ 1746 CA* did not deal with personnel records, it seems that the case suggests that much of the information held in personnel files is likely to be sufficiently biographical and contained in a sufficiently accessible filing system for it to fall within the definition of personal data. It would be unwise for employers to disregard the Data Protection Act 1998 (DPA) without specific advice from solicitors.

After the *Durant* case and the subsequent guidance issued by the Information Commissioner, manual personnel files (and other manual files) which:

- use individuals' names or unique identifiers as the file names, or
- which are sub-divided or indexed to allow retrieval of personal data without a manual search (such as, sickness, absence, contact details etc.)

are likely to be held in a 'relevant filing system' for the purposes of the DPA.

The DPA applies to both information held on computer and manual information provided the manual data is organised into a ''relevant filing system'. A 'relevant filing system' is defined in section 1(1) of the DPA as 'any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured either by reference to the individual or to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible'.

Employees and ex-employees (and sometimes their legal representatives) may attempt to use the DPA to obtain information which they are not entitled to if the law is applied strictly. Of course, an organisation which wishes to be open, may voluntarily disclose information held in a manual form as long as the confidentiality of other employees is not compromised.

In *Durant* the Court of Appeal took the view that the Act was only intended to cover manual files of sufficient sophistication to provide similar accessibility as a computerised filing system.

The following key points can be drawn from guidance issued by the Information Commissioner after the case.

A relevant filing system:

- is not any manual filing system which requires a person to search through files to find information qualifying as personal data,
- is limited to a system which is structured or referenced in such a way as to indicate at the outset of the search whether specific information capable of amounting to personal data is held within the system and, if so, in which file or files it is held, and
- must have a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located.

Additional points include the following:

- the protection given by the legislation is for the privacy of personal data, not documents as such,
- it is only to the extent that manual filing systems are broadly equivalent to computerised systems in ready accessibility to personal data that they are within the system of data protection,
- files must be indexed or structured in such a way as to allow the retrieval of information about a specific individual for example a file which is subdivided in alphabetical order of individuals' names is likely to fall within the provisions of the Act,
- where manual files fall within the definition of relevant filing system, the content must either be so sub-divided as to allow the searcher to go straight to the correct category and retrieve the information requested without a manual search, or must be indexed to enable directly finding the relevant page, and
- a filing system containing files about individuals, or topics about individuals, where the content of each file is structured purely in chronological order will not be a relevant filing system as the files are not appropriately structured/indexed/divided or referenced to allow the retrieval of personal data without leafing through the file.

In August 2007 the Information Commissioner published a technical guidance note consisting of frequently asked questions on relevant filing systems. Further guidance is expected to follow.

- View guidance note

- **If an individual entitled to request to view their personnel file from an employer, what is the procedure?**

As indicated in the question above on manual files, an employee will probably be entitled to make a written request for certain information from an employer (and other data controllers) including a personnel file, depending upon the content of the information and the way the information is held.

If the request is made the appropriate fee must be paid to the data controller for dealing with access requests - the current maximum is £10.00 .
The individual is entitled to:

- be told whether personal data about them is being processed
- a description of the data concerned
- the purposes for which it is being processed
- the recipients or classes of recipients to whom it is or may be disclosed
- have communicated in an intelligible form the personal data concerned and any information available to the data controller as to the source of the data.

These provisions mean in effect that an employee may request access to data held on them either in a computer or in paper form. As personal data includes any expression of opinion about an individual, if the employer has any adverse comments, for example, in relation to performance, the employee will have a right to see them. Employers must not make any special alterations to data so as to make it more acceptable to the data subject.

Data controllers do not need to comply with a request that is similar or identical to a request made by the same individual previously, unless a reasonable interval has passed since the previous request was made.

A data controller must respond to an access request promptly (which is taken to mean as quickly as it reasonably can). They must respond within 40 days of receipt of the request, or within 40 days of receipt of:

- the information required to satisfy themselves as to the identity of the person making the request so that they can find the information that person wants
- the appropriate fee.

There are shorter time limits for credit files and school pupil records.

- **If an employer contracts out payroll services what are the obligations as regards the supply of data to this third party?**

Under the definitions supplied in the Data Protection Act 1998, this contractor is a third party data processor. In order for this contractor to perform the contract, it will be necessary to supply them with certain items of personal data for employees, such and name, address, national insurance number and salary details. Such data must be fairly and lawfully processed in accordance with the data protection principles. It would be advisable to take measures (for example including a specific term in the contract with the payroll service) to ensure that the data supplied will only be processed for the specific purpose of the contract. Enquiries should also be made with the contractor to ensure adequate measures will be taken regarding the storage and security of the data supplied.

Of course there should also be a detailed communications and data protection policy which fully explains to employees both how they should process any personal data and the information if any which is held about them.

- **What is the definition of 'sensitive personal data' and what additional measures must an employer take when processing this type of data?**

Sensitive personal data is personal data relating to the data subject's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life

- actual or alleged criminal offences, criminal proceedings and convictions. (For further information on criminal convictions and their disclosure, see question below on criminal conviction information).

The Data Protection Act 1998 (DPA) gives additional protection to sensitive personal data over and above that given to other personal data.

To lawfully process sensitive personal data, at least one of the conditions contained in Schedule 3 of the DPA must be met. The main ones are:

- The explicit consent of the data subject has been freely given.
- The processing is necessary to comply with any obligation or legal duty imposed on the data controller.
- The processing is necessary to to protect the vital interests of the data subject or another person (for example life threatening issues such as disclosure of a data subject's medical history to a hospital casualty department treating the data subject after a road accident).
- The processing is necessary for, or in connection with, legal proceedings (including prospective legal proceedings).
- The processing is necessary for the exercising of legal rights or obtaining legal advice.
- The information contained in the personal data has been made public by the data subject for equal opportunities monitoring.
- The processing is necessary as it is deemed to be in the public interest.

(Further guidance on various aspects of sensitive personal data can be found from Common Services Agency v Scottish Information Commissioner (Scotland) [2008] UKHL 47; [2008] WLR (D) 231).

- **Do employers need to seek explicit consent from employees before processing data relating to the reasons for sickness absence ?**

Data relating to the medical condition of an employee amounts to sensitive personal data for the purposes of the Data Protection Act 1998 and care needs therefore to be taken with the processing of such data. Guidance on obtaining and handling information about workers' health was been published by the Information Commissioner's Office in December 2004.

The Employment practices data protection code: Part 4: information about workers health addresses the collation and use of information about a worker's physical or mental health. It does not impose new legal obligations.

The Code covers sickness and injury records, occupational health schemes, information from medical examination and testing, drug and alcohol testing and genetic testing. As this information is sensitive data employers should only collect health information where it is necessary for health and safety reasons, or to prevent discrimination, or to satisfy other legal obligations or if each worker has freely given his or her explicit consent.

The Information Commissioner recommends that absence and sickness records be kept separately.

- View code

- **Is there any guidance on the length of time personnel records or individual items of data should be retained?**

The fifth data protection principle provides that 'personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'. Neither the Data Protection Act 1998 (DPA) nor the *Employment practices data protection code: Part 2: employment records* sets a specific time

period that is appropriate for the retention of workers' records. It is therefore the responsibility of the employer to decide on retention periods.

- View the code

The termination of an employment relationship does not mean that all records should be deleted; there may be a real business need to retain some of them. For example, it may be necessary to retain some information with which to enable references to be provided in the future or in respect of the employee's pension arrangements or to be able to defend future claims. Employers should also be aware that the DPA does not override any statutory requirement to retain records, for example in relation to income tax or certain aspects of health and safety.

For more detailed information on recommended retention periods see our factsheet on Retention of personnel and other related records.

- View the factsheet

- **How do the requirements of the Data Protection Act 1998 apply to the provision of references?**

The basic position is that the provision of a reference will generally involve the disclosure of personal data under the Data Protection Act 1998 (DPA). Accordingly in most circumstances, and in particular where a reference is likely to have a serious impact on future job prospects, a employee may be able to obtain access to that reference through the DPA.

However the position is complicated by the fact that the DPA applies differently to a reference which is in the possession of the ex-employer who has given the reference, and to references which are under the control of the new employer who has received it. For further details see the question on data protection in our References FAQ.

- Go to References FAQ

- **What can an employee do if they believe that an employer has breached their rights under the Data Protection Act?**

An aggrieved employee can appeal to the Information Commissioner for an assessment as to whether processing of personal data is being carried out in accordance with the principles contained in the Data Protection Act 1998 (DPA).

The Commissioner has the power to serve an **information notice** requesting certain information from the employer.

If the finding is that a breach of the data protection principles has occurred, the Commissioner may serve an **enforcement notice** on the employer. An enforcement notice can require an employer to take remedial steps and take certain actions, for example require them to cease to process data, or if the data is inaccurate to remedy this, or even erase certain items of data.

An employer can **appeal** against an enforcement notice to a tribunal If the appeal is on a point of law then an appeal may be made to the High Court (or Scottish and Irish equivalent). An employer wishing to appeal against an enforcement notice should do so within 28 days of the date on which the notice was served unless exceptional circumstances apply.

The Commissioner also has the power to obtain a **warrant** to enter and inspect premises where it is believed that any of the data protection principles have been or are being contravened. Warrants may be issued by a

Circuit Judge on being satisfied that there are reasonable grounds for suspecting that an offence has been or is being committed.

Where there is a serious contravention of the data protection principles.The Information Commissioner also has the power to serve a **monetary penalty** notice for breaches of the data protection principles. This notice will require the data controller to pay a penalty by the deadline set out in the notice. Before serving such a notice, the Information Commissioner must first serve a notice of intent which will allow for written representations before the penalty notice is served. To serve a monetary penalty notice, the Information Commissioner has to be satisfied that the contravention was deliberate or that the data controller knew (or ought to have known) of the risk, and that the contravention would be likely to cause substantial damage or distress. Future regulations will set a maximum penalty.

The employee may also seek compensation under the DPA, for example, in the case of an inaccurate reference as a consequence of which a conditional offer of employment is withdrawn in addition to any discrimination claim which may arise. Employees may also serve a written notice under the DPA and ultimately apply to the High Court or County Court for an order to force the employer to reconsider their decisions or for the rectification, blocking, erasing or destruction of personal data in certain cases.

Under the Criminal Justice and Immigration Act 2008 there are tougher penalties for breaches of the data protection obligations. Obtaining, disclosing or procuring the disclosure of personal information without the consent of the organisation which holds the information is a criminal offence and the Secretary of State has the power to increase the penalty to a maximum of two years' imprisonment.

- **Can an employer video employees, monitor and or intercept or monitor telephone calls, emails or use of the Internet?**

This question is extremely hard to answer and legal advice should be taken in each set of circumstances. Monitoring by videoing and or tapping of incoming and outgoing telephone calls, faxes and e-mails on a public telephone system is illegal except as permitted by any regulations or other legislation.

Need for policies

All employers must have a detailed communications, internet and data protection policy in place covering monitoring, use of email and intranet, and data protection. If they do an employer may be able to:

- monitor and or intercept a communication where the employee has given consent in advance, for example in the contract of employment, and
- in certain very limited circumstances monitor and/or intercept a communication where the employee has not given consent.

The cases *Halford v UK* and *Copland v UK* demonstrate the need for all employers to have a detailed communications, internet and data protection policy and or to inform employees of possible monitoring or interception of commications (see under heading Examples of monitoring below).

Relevant legislation

Even if the employer has a policy, it's actions must be authorised under the following legislation: the Data Protection Act 1998, Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA), the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/2905) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

The Human Rights Act 1998 (HRA) incorporates into UK law the principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 of the Convention provides that every

person has the right to respect for privacy and family life, home and correspondence.

Courts and tribunals in the UK are bound to take the provisions of the HRA into consideration when interpreting employment legislation under which an employee is making a claim.

Guidance on monitoring

The *Employment practices data protection code: Part 3: monitoring at work* contains detailed guidance on monitoring of communications. If an employer intends to monitor their workers, they should:

- be clear about the purpose of such monitoring
- conduct an assessment of the impact
- justify the benefits of monitoring communications
- communicate the policy on monitoring to workers to rebut any expectation of privacy of communications in the work environment.
- View Code

Under RIPA employers retain the right to carry out monitoring without the employee's specific consent first being obtained for:

- recording evidence of business transactions
- ensuring compliance with regulatory or self-regulatory guidelines
- maintaining the effective operation of the employer's systems (eg preventing viruses)
- monitoring standards of training and service
- preventing or detecting criminal activity
- preventing the unauthorised use of the computer/telephone system, for example, ensuring the employee does not breach the company's email or telephone policies.

Nonetheless, RIPA provides that it will be necessary for employers to take reasonable steps to inform employees that their communications might be intercepted.

The Home Office has published *A code of practice on covert surveillance* and Acas has published an advisory leaflet on internet and email policies.

- View Home Office code
- View Acas leaflet

Examples of monitoring

The following cases relate to events before the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) Regulations 2000 were fully in force. However they remain useful to emphasise the importance for employers of having a policy dealing with the supervision of telephone, e-mail and internet use.

In *Halford v UK [1997] IRLR 471, ECHR* Alison Halford took her case to the European Court of Human Rights. The question before the ECHR was whether surveillance in the form of monitoring personal telephone calls made by an employee from her employer's premises were covered by the notion of 'private life' and 'correspondence' and therefore constituted a breach of article 8(1). The ECHR decided that the surveillance, in all the circumstances, was a breach of the employee's human rights. A factor in the ECHR's decision was that the telephone on which the employee's calls were monitored and recorded was provided specifically for personal use and therefore it was held that the employee had a 'reasonable expectation of privacy'.

In the case of *Copland v The United Kingdom (unreported, 62617/00 3 April 2007, ECHR* the deputy principal of a Welsh college arranged for an employee's telephone, e-mail and internet usage to be monitored - there was no policy in force at the college dealing with the such matters. The ECHR eventually held that the monitoring was a breach of her right to respect for private life under Article 8. The Court indicated that monitoring might be permissible but only in pursuit of a 'legitimate aim'.

However, if the procedures referred to above, had been followed the HRA issue may not have arisen.

- **What should an employer do to manage employees' use of social networking sites such as Facebook?**

The use of social networking sites such as Facebook,Twitter, MySpace, Bebo, Friendster or information from YouTube has become a problem for many employers. The TUC referred to the UK's Facebook users 'as 3.5 million HR accidents waiting to happen'. In order to prevent or minimise these 'accidents', what should an employer do? The short answer is that employers must have an Internet and communications policy which specifies the web use that is, and is not, acceptable. Further guidance and examples are set out under separate headings below.

Positive and negative aspects

The positive aspects of social networking sites involve creating and developing work-related relationships. The sites can be a fast effective method helping employees to keep in touch with clients. However it is important to create the right balance with policies including guidance on what behaviour is acceptable and what is not. Personal access to the internet including networking sites can also boost staff morale and assist in the work life balance.

Negative aspects include risks of the following:

- employees time-wasting and lost productivity,
- employers using information gained on such sites to make discriminatory decisions about vetting new employees or their promotion etc,
- employees breaching the employer's confidentiality,
- damaging the company's reputation by making defamatory statements about the employer, fellow employees or clients,
- employees making known to the other millions of users what working for the organisation is really like in their opinion.

Legal issues

Many potential legal issues surround the use of social networking sites. For example:

Breach of contract

There is an implied term of mutual trust and confidence between employer and employee in all employment contracts. A very negative and damaging posting or communication about the employer may entitle the employer to state that this term has been broken and warrant the employee's dismissal after appropriate investigation and action in accordance with the Acas code on disciplinary and grievance procedures and the organisation's disciplinary procedure.

Data protection

As far as data protection is concerned merely looking at someone's information on a site is not a breach of data protection law. Although the Information Commissioner's Office has investigated certain networking sites and voiced concerns about the the fact that it is difficult to take off all personal information from some of the sites.

Defamation

If defamatory material is posted on a social networking site a claim idefamation claims may arise against the employee.

Discrimination

Difficulties arise if information from networking sites is used to make discriminatory decisions, for example to refuse a job on grounds of race, sexuality, religion or age. Employers must not make a decision on such a basis otherwise they are exposed to expensive discrimination claims. Also only a minority of candidates will have profiles on social networking sites and using information from this source can give an unfair advantage or disadvantage to certain candidates possible discriminating against younger people who use the sites more.

Other discrimination claims may arise if employees post discriminatory material about other employees which could amount to bullying or harassment. Employers may be vicariously liable for such acts unless they took such steps as were reasonably practicable to prevent the postings.

Health and safety

In 2007 a UK based employer saw internet video clips of employees performing stunts wearing its uniform. An employer who discovers information like this should follow the company's disciplinary procedure to investigate the possibility of a breach of health and safety legislation on the part of the employee. If an employer is ware of this and fails to investigate there may be liability for personal injuries in the law of negligence.

Practical issues

Realistically, employers are going to continue to look at networking sites as part of the recuitment process and there is no restriction on them doing so. However, this is no substitute for a properly conducted interview and selection process which is focussed on relevant information concerning the candidates' abilities to do the job. Much information on networking sites will not have any relevance for the position in question.

Similarly, an isolated comment about a bad day at work should be seen in context, as a highly interventionist approach to employees' personal lives can damage relations with the workforce.

Employers should bear in mind the following:

- Consider whether there is a real need to check social networking sites as part of the recruitment process of vetting job applicants and if they do ignore any information which may lead to a discriminatory decision.
- Check staff handbooks and contracts of employment to ensure that employees are aware of the Internet and communications policy and that social networking sites are clearly covered by the policy.
- Specify in the policy and contracts of employment what internet and communications use will constitute gross misconduct sufficiently serious to justify summary dismissal.
- Check that the organisation's disciplinary policy co-ordinates with the policy on abuse of the internet.
- Specify clearly in the Internet and communications policy that private and business communications could be intercepted and warn employees in advance of the monitoring which will take place and why. Employers must ensure that such monitoring is reasonable and in accordance with data protection and human rights obligations.
- Depending on the nature of the business employers must decide whether to allow unlimited access, restricted access or a complete ban.

Restrictions on use

Many employers have adopted a complete ban on social networking sites at work because of the time wasting concerns. However if employers previously allowed staff use of their work computers and telephones for reasonable personal use this may include social networking sites. Employers who trust their staff may wish to allow responsible personal use of the internet during break times as long as this does not interfere with work or damage the employer's reputation. As use of social networking sites increases and in times of economic difficulty it is likely that more organisations will choose to block or limit social networking sites whilst at work.

Employers therefore have a number of options with respect to networking sites when creating or updating their Internet and communications policy. There can be:

- unlimited access to social networking sites (this may suit employers where the marketing and business generation aspects of these sites are crucial), or
- restricted access for work purposes only, or
- restricted personal use for example during lunch hour and after work, or
- completely block from using certain sites from the organisation's computer network.

A number of large employers are adopting a complete ban on accessing networking sites from their work computers.

Examples

There are numerous examples of issues concerning the use of social networking sites by employees including:

- Directory enquiries group 118 118 discovered workers were making comments about callers they had dealt with. The company investigated the workers who were involved and disciplinary proceedings followed.
- Virgin Atlantic dismissed 13 cabin crew after disciplinary proceedings concerning messages on Facebook referring to passengers as 'chavs' and making jokes about them.
- an employee was dismissed after less than a month in her job following her comments on a networking site on how boring her job was.
- A prison officer was dismissed for gross misconduct after befriending former and current inmates on Facebook.

See also question below on the potential liabilities and risks for an employer if employees misuse the email system and the Internet.

- **What are the potential liabilities and risks for an employer if employees misuse the email system and the Internet?**

All employers must have a detailed communications, internet and data protection policy in place covering monitoring, use of email and the internet and data protection. If they do not the areas of risk and liability for an employer if employees misuse the email systems and the Internet include:

Defamation

An example of such a claim was seen in the case of *Western Provident Association v Norwich Union,The Times, 8 July 1997*. The defendant had to pay approximately £450,000 in an out-of-court settlement to one of its competitors as a result of a rumour that the competitor was in financial trouble which was spread by its employees through its internal email system.

Breach of confidentiality or trade secrets

This is made considerably more likely with the simplicity and the global nature of email and the Internet when coupled with a lack of awareness of the risks that incorrect usage presents.

Intellectual property rights

An employee who downloads unlicensed software can easily infringe intellectual property rights. Employees are typically not sufficiently aware of the legal issues involved to seek permission from the author before downloading material and using it for business purposes.

Breach of contract

Emails are capable of forming contractual documents. Contracts can easily be formed by careless emails and non-compliance with the terms of any such contracts will of course render a business liable for a breach of

contract claim. Emails tend not to be subject to the same safeguard procedures as paper documents which are often checked before the company signs them off.

Discrimination

Many forms of discrimination claim can occur via emails, including harassment.

Where an employee carries out an act of harassment or discrimination in the course of their employment, the employer is vicariously liable for that act even when the act is unauthorised.

Once an issue of email harassment has been raised and the harasser identified, immediate action should be taken to stop the harassment and instigate the disciplinary procedure while supporting the harassed employee. In order to handle this safely, it is essential an employer has a clear policy and guidelines in place.

The case of *Walker v Charles Russell* demonstrates the dangers of email comments and the liability they can attract. A black secretary in a city law firm resigned and a solicitor colleague sent an email asking for her replacement to be a busty blonde. She sued the company for race discrimination and the case was settled out-of-court for an undisclosed amount.

See also the question above on how employers should manage employees' use of social networking sites such as Facebook.

- **What is the Freedom of Information Act and to whom does it apply?**

The Freedom of Information Act 2000 (FOI Act) gives the general right of access to all types of 'recorded' information held by public authorities (and those providing services for them). It also sets out exemptions from that right and places a number of obligations on public authorities. Under the FOI Act any person making a request to a public authority for information will be entitled to be informed whether that information is held and to have that information communicated to them.

The Information Commissioner promotes good practice, public authority compliance with the FOI Act, disseminates information and gives advice about the FOI Act. Only some of the data protection principles will apply to personal data held by public authorities.

Public authorites have two main responsibilities under the FOI Act:

- to produce a 'publication scheme', and
- to deal with individual requests for information.

The FIOI Act applies to all public authorities including bodies such as the NHS, schools, the Police and other organisations such as the Post Office, although the duty to adopt a publication scheme comes into force at different times for different authorities.

From 1 January 2005 individuals have been entitled to make requests for specific information and public authorities have a duty to handle the request in line with the provisions of the Act.

Many authorities will have formal complaints procedures which should be set out in their publication schemes, and the Information Commissioner would be unlikely to consider a complaint from an applicant who had not first attempted to resolve the matter in this way.

More information is available from the Information Commissioner and Department for Constitutional Affairs.

- Go to Information Commissioner's website
- Go to DCA website

- **Are there any future developments expected in the area of of data protection?**

Data protection has been a permanently and rapidly evolving area for some time. In late 2007 there were several very high profile breaches concerning the protection of personal data including for example the disappearance of:

- two computer discs containing the entire child benefit data base of 25 million people when HMRC reportedly posted them to the National Audit Office using normal post,
- the hard drive of a computer containing the personal details of three million UK driving test applicants, and
- assorted patient information by nine NHS trusts.

As a result the House of Commons Justice Select Committee published a report on the protection of private data in January 2008.
This report is likely to lead to further legislation and developments. These potential developments are summarised under the following headings:

Notification

At present if any data is lost then the Data Protection Act 1998 (DPA) does not require companies to notify either the Information Commissioner or those affected by the loss of data. It is now likely that further legislation will be introduced which will at the very least require:

- a compulsory reporting system to be followed if data is lost, and
- rules on notification letters to specify the breach and the steps that should be taken to deal with the breach.

Data and Government

An important conference to consider progress with freedom of information and data protection legislation and the democratic process will take place on 13 May 2009. This is intended to look at underlying policy issues and challenges for the future. The need for any future changes may be highlighted during this conference.

General spot checks and enforcement powers

The Information Commissioner has no power to conduct unannounced spot checks and inspections on organisations that process people's personal information without the consent of the organisation to be inspected.The Prime Minister has already indicated that the Information Commissioner's office will be able to spot-check Government departments. However legislation appears likely to extend full audit and inspection powers to all public and private organisations which process people's personal information. To enable the Information Commissioner to take appropriate action where necessary increased funding will also be required.

The report is available on the Committee's website.

- Read report

For details of developments since this update see our Recent developments section.

- Go to Recent developments section