CONTENTS

1. Introduction 1

2. The Regulation of Investigatory Powers Act 2000 1
   2.1 What is interception? 2
   2.2 What is “lawful authority”? 2

3. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 3
   3.1 Permitted interceptions 3
   3.2 Scope of the permitted interceptions 3

4. The Data Protection Act 1998 6
   4.1 General obligations under the Data Protection Act 1998 6
   4.2 Fair and lawful processing 7
   4.3 Disclosure and transfer of personal data outside the EEA 7
   4.4 Subject Access Requests 8
   4.5 Sanctions under the DPA 1998 8
   4.6 The Information Commissioner’s Employment Practices Code 9
   4.7 Impact assessment under the Code 11
   4.8 Good Practice Recommendations under the Code 12

5. Company policies 14
   5.1 Obligations under the Lawful Business Regulations and the DPA 1998 14
   5.2 Using company policies to limit liability 14
   5.3 Banners 17

APPENDIX 18
1. INTRODUCTION

Few businesses today could operate efficiently without electronic communication systems. Use of mobile telephones, voicemail, e-mail, personal digital assistants and the internet have revolutionised the way companies operate, improving efficiency and communications on a global scale. However electronic communications have also exposed businesses to a number of risks particularly in relation to employee use of these systems.

Employers have long been aware of the risks connected with employee access to company stationery, fax or telephone which could be used to enter into commitments on behalf of the company without requisite authority or for conducting fraudulent transactions for which the company could be held liable. However, these problems are compounded when the method of communication is by electronic means, particularly by e-mail, which allows for immediate and widespread dissemination of communications. The advent of sophisticated technology has also meant the increased use of company systems by employees for personal reasons, which again causes concern for employers in respect of any liability for inappropriate use. Finally, modern IT systems are more vulnerable than ever to security breaches in the form of viruses, unauthorised access to systems or theft of company hardware (including laptops or personal digital assistants) containing confidential information.

Companies consider IT systems to form part of their assets and as such assume that they have complete control over them. In general terms there are two ways in which control can be asserted:

- by intrusive means, through the interception and monitoring of employee communications and internet use; and

- by persuasive means, through the introduction of clearly defined standards for employee communications disseminated through policies and training schemes.

However any control of employee communications in the UK must be exercised within the parameters of European human rights legislation. Modern IT systems which integrate internet, e-mail and telephone systems are capable of capturing and recording an enormous amount of data. Invariably this will raise privacy issues where employee use of electronic systems will result in the processing by employers of personal data contained in e-mails and voicemails and, where recorded, in telephone calls. The European Convention on Human Rights affords individuals a right to privacy under Article 8. The requirements set out in the Article have in part contributed to the creation of the Data Protection Act 1998 (DPA 1998) which regulates the processing of personal data and the Regulation of Investigatory Powers Act 2000 (RIPA 2000) which regulates the interception of any communication (whether personal or not) in the course of its transmission.
2. THE REGULATION OF INVESTIGATORY POWERS ACT 2000

RIPA 2000 prohibits controllers of systems (which would include employers) from intercepting communications in the course of their transmission without lawful authority. If an employer intercepts unlawfully, the sender or recipient of the communication may be able to obtain an injunction or sue for damages.

2.1 What is interception?

According to RIPA 2000, an “interception” takes place if the contents of a communication are made available during the course of its transmission to someone other than the sender or the intended recipient. The main types of intrusive controls that a company will want to employ, such as the use of automated software programs to block incoming e-mails, the opening of e-mails stored on a server or in an individual’s inbox before they have been read by the intended recipient and the listening in to, or recording of, telephone conversations, will amount to the “interception of a communication in the course of its transmission”. Recording incoming or outgoing e-mail communications will also amount to interception.

Certain commentators have suggested that accessing e-mails in an individual’s inbox that have already been opened would also constitute an “interception during the course of transmission”. This is because the time during which a communication is being transmitted under RIPA 2000 includes:

“any time when the system by means of which the communication is being or has been transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it”.

Although the phrase “collect it or otherwise have access to it” could conceivably be broad enough to cover the continued storage of an opened e-mail message on the recipient’s system (for example, in an inbox or on a server) the more likely interpretation is that the terms “collect” and “have access to it” refer to different ways in which e-mails may be accessed within an organisation (i.e. whether individuals download them from a central server or whether they appear directly in an individual’s inbox). This interpretation is also favoured by the Information Commissioner (the officer responsible for the enforcement of the DPA 1998) who has stated in guidance that once a communication has been read by a recipient it is no longer being transmitted and assures that the same regime applies to the interception of communications whether delivered by post or by a telecommunications service.

2.2 What is “lawful authority”?

RIPA 2000 authorises interception of communications in cases where the business has reasonable grounds to believe that both the sender and the intended recipient have consented to the interception. Securing such consents in the context of e-mail correspondence or telephone communications is problematic and in most cases businesses would prefer not to have to do so. It is therefore more likely that employers wishing to intercept business communications will seek to rely on the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations) which allow employers to intercept communications for a number of strictly defined purposes.
3. THE TELECOMMUNICATIONS (LAWFUL BUSINESS PRACTICE) (INTERCEPTION OF COMMUNICATIONS) REGULATIONS 2000

The Lawful Business Regulations allow employers to intercept and record communications in certain prescribed circumstances without obtaining the consent of the parties to the communication.

3.1 Permitted interceptions

The Lawful Business Regulations allow employers to intercept and record communications in the course of their transmission for the following purposes:

(i) to establish the existence of facts;

(ii) to ascertain compliance with regulatory or self-regulatory practices or procedures which are applicable to the employer in carrying on of his business or applicable to another person where that person is supervised by the employer in respect of those practices or procedures;

(iii) to ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties;

(iv) in the interest of national security;

(v) for the purpose of preventing or detecting crime;

(vi) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunications system; and

(vii) in order to secure the effective operation of the system or where it is necessary as an inherent part of the effective operation of the system.

In addition, the Lawful Business Regulations allow businesses to intercept (but not to record) communications:

(viii) for the purpose of determining whether they are communications relevant to the employer’s business; and

(ix) made to anonymous confidential voice-telephony counselling services.

3.2 Scope of the permitted interceptions

At first glance, the Lawful Business Regulations appear to give employers the ability to intercept communications for a wide variety of purposes. For example, the use of automated software programs to block incoming e-mails could be permitted for the purpose of investigating or detecting the unauthorised use of the telecommunications system (see (vi) above), whereas the reading of an unopened e-mail may be justified where this is done to establish the existence of certain facts (see (i) above) or to determine whether there are communications relevant to the employer’s business (see (viii) above).
However, there are a number of further limitations which employers must consider before relying on the permitted purposes listed in the Lawful Business Regulations. These are as follows:

**Interception of communications which are relevant to the employer’s business**

To be lawful, the interception must be effected solely for the purpose of monitoring or (where appropriate) keeping a record of communications which are relevant to the employer's business. This restriction clearly implies that employers may not intercept for the purpose of recording or monitoring communications which are personal. This may be problematic in circumstances where an employer uses automated software programs to intercept e-mail for the purpose of protecting its system because such software may be incapable of distinguishing between personal and business communications. In these circumstances an employer must ensure that the purpose for using such software is solely to prevent the corruption of business communications and not to monitor or keep a record of any personal communication. Where any interception by an employer results in personal communications being intercepted it is important that the restrictions imposed by the DPA 1998 are also observed. This is discussed further in section 4 below.

**Informing users of the system**

Before any interception takes place, the employer must have made reasonable efforts to inform every person using the system that communications transmitted by this method may be intercepted. A user of the system would include all employees but not third parties who correspond with them. There is no prescribed manner in which employees must be informed although this requirement is generally satisfied by circulating a written policy to all employees (see section 5 below).

**Business use of the telecommunications system**

In order for any interception to be lawful, the telecommunications system in question must be provided at least partly for use in connection with that business.

**Interaction with the Privacy and Electronic Communications Directive 2002/58/EC**

The Lawful Business Regulations implement requirements originally set out in the Telecoms Data Protection Directive 97/66/EC and now incorporated in the Privacy and Electronic Communications Directive 2002/58/EC (the Directive) which assures the confidentiality of communications by means of a public communications network and publicly available electronic communications services. The Directive prohibits listening, tapping, storage or other kinds of interception or surveillance of communications by others than users, without the consent of the users concerned. However it does allow Member States to authorise the recording of communications in the course of lawful business practice for:

"the purpose of providing evidence of a commercial transaction or of any other business communication".


In addition the Directive allows for Member States to restrict the requirement for the purpose of safeguarding “national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or unauthorized use of the telecommunications systems”.

The text of the Directive is particularly relevant in relation to interceptions carried out under the Regulations for the purpose of:

(i) establishing the existence of facts; or

(ii) to ascertain the compliance with regulatory or self regulatory practices; or

(iii) to ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties

as they will only be permitted to the extent that this is authorised by the Directive. Although it does appear that (i) above does fall within the scope of the Directive this is less clear in the case of (ii) or (iii) above. Although there has not been any challenge to the validity of the scope of the Regulations to date, employers who are relying on interception solely for the reasons set out in (ii) and (iii) above would do well to check whether or not they can justify this interception under any of the other permitted interceptions listed above.
4. THE DATA PROTECTION ACT 1998

Even where an employer is satisfied that the interception of a communication is lawful under the Lawful Business Regulations, it is likely that additional issues will be raised by the DPA 1998.

This is because:

(i) all communications will contain some data which identifies a living individual (and will therefore be “personal data” under the DPA 1998); and

(ii) the actions of intercepting, monitoring or recording will amount to “processing” under the DPA 1998.

In general terms, the DPA 1998 will apply to all types of intrusive controls that a company may apply to employee use of its electronic communications, including controls which do not necessarily amount to interception under the Lawful Business Regulations. For example, the consulting of records which indicate what telephone numbers an employee has called or which internet sites have been visited does not qualify as an interception (and so will not be restricted by RIPA 2000); however it will still amount to processing under the DPA 1998.

4.1 General obligations under the Data Protection Act 1998

The DPA 1998 prohibits the processing of personal data by data controllers (a term which would include employers) established in the UK unless certain details relating to the data controller and any proposed processing have been notified to the Information Commissioner. This will involve the filling in of a standard form available from the Information Commissioner’s website and the payment of an annual fee of £35. Failure to notify is a criminal offence.

In addition, all processing of personal data by employers must be in accordance with the eight data protection principles set out in the DPA 1998. In summary these require that:

(i) all processing is done fairly and lawfully;

(ii) all processing is for specified and lawful purposes;

(iii) personal data are adequate, relevant and not excessive in relation to the purpose for which they are processed;

(iv) personal data are accurate and, where necessary, kept up to date;

(v) personal data are not kept for longer than necessary;

(vi) the rights of the data subjects are observed;

(vii) appropriate security measures are adopted; and

(viii) personal data are not transferred outside the EEA unless that country ensures an adequate level of protection.
Breath of a data protection principle is not an offence but may result in an enforcement notice or an information notice being issued by the Information Commissioner. The issuing of a notice is likely to cause embarrassment to an employer and have an impact on its employee relations. Failure to comply with such notices is a criminal offence.

4.2 Fair and lawful processing

Although all eight principles will apply to monitoring activities, the first principle (fair and lawful processing) is particularly relevant. In order for any monitoring or intercepting of employee communications to be fair and lawful a number of conditions must be met:

1. All data subjects (this will include both employees and other parties to, or referred to within, employee communications) must be made aware of the extent and purpose of any monitoring; and

2. Employers must either ensure that they:
   (i) seek the consent of the data subjects to such monitoring; or
   (ii) can justify the monitoring on the grounds that it is in their legitimate interest to do so and that such activity does not amount to unwarranted prejudice to the rights and freedoms and legitimate interests of the data subject; and
   (iii) where monitoring involves the processing of sensitive personal data, the explicit consent of employees must be obtained.

The Information Commissioner has made it clear that in order for consent to be valid under the DPA 1998 it must be freely given, and that this may be an issue in respect of employees. Employers should therefore ensure that they can justify any monitoring of employee communications on the grounds that it is in their legitimate interest to do so. Moreover, monitoring of sensitive personal data should be avoided wherever possible.

4.3 Disclosure and transfer of personal data outside the EEA

The eighth data protection principle restricts the transfer of personal data to countries outside the EEA which do not have equivalent levels of protection of data. This principle will be relevant in circumstances where monitoring is carried out in one jurisdiction (i.e. the UK) and information gathered is then disclosed to persons in other jurisdictions (e.g. to managers of a parent company situated in the US). Disclosures of these types are problematic under the DPA 1998 and can only be done where the data subject has given their consent (having understood the implications of their data being transferred to a less secure jurisdiction) or where the UK employer enters into an agreement with the US-based persons to ensure that the personal data will be kept secure in accordance with the DPA 1998 principles. To assist companies exporting personal data to entities established in countries which do not have equivalent levels of data protection the European Commission have devised a set of model contracts which have been approved by the Information
Commissioner and which set out a series of standard clauses which provide for transfers of data to be made securely. By following these model clauses a company can avoid breaching the data export provisions of the Act. For more information on the model contracts and other issues surrounding data export please refer to our client publication “An Introduction to the Data Protection Act 1998”.

4.4 Subject Access Requests

Section 7 of the DPA 1998 gives every data subject the right of access to his or her personal data. Under this provision a data subject who makes a request in writing to a data controller and pays a fee of £10 is entitled to receive copies of all personal data held on that individual by the data controller within 40 days of the request. These rights of access are very wide and employers should be aware that except in cases where disclosure would prejudice a criminal investigation the results of any monitoring exercise carried out on an individual are likely to fall within the scope of a request, even if an internal disciplinary matter is contemplated. Companies that monitor individuals should therefore be aware that even in circumstances where they may be justified in covertly monitoring an individual, any information gathered during that process may need to be disclosed in a subsequent access request made by that individual.

4.5 Sanctions under the DPA 1998

Under the DPA 1998 the Information Commissioner is charged with a statutory duty to promote the data protection principles and is empowered to take enforcement action when they are breached. Where an employer has failed to observe the principles because, for example, it has failed to properly inform employees of any proposed monitoring, the Information Commissioner may issue an enforcement notice which would require the employer to cease any such processing and to ensure compliance with the relevant principle within a specified time frame. Failure to comply with such a notice is a criminal offence.

There are a number of criminal offences under the DPA 1998. Employers should be particularly aware of the offences under s55 relating to disclosing or selling personal data knowingly or recklessly without the consent of the data controller. The breadth of this offence was recently illustrated in the case of R v Rooney [2006] All ER (D) 158 (Jul). In that case the defendant was a civilian employed by the police in personnel. The defendant’s sister had a relationship with a police officer which ended. One year later the defendant heard that the police officer had moved in with another officer to an address in Turnstall. Using the police database to which she had access for work-related purposes, the defendant looked up the new couple’s address. She then informed her sister that the couple were living in Turnstall but did not disclose the precise address. The defendant was convicted of two counts of unlawfully obtaining personal data and of one count of unlawfully disclosing personal data. The defendant appealed against the latter conviction on the basis that the information disclosed did not amount to personal data but the Court of Appeal upheld the conviction. The reference to the police officers’ residence in Turnstall was sufficient to constitute information contained in personal data. This result demonstrates the width of the offence of unlawful disclosure: the offence is complete even if the information
disclosed in itself would lack the detail sufficient to render it “personal data” for other purposes. The reason for this appears to be the derivation of that information from personal data which has been unlawfully obtained. Employers should ensure that their employees are aware that legitimate access to personal data during the course of their work does not entitle them to access that data for other purposes or pass on any of the information contained therein.

If an employee can show that its employer has unreasonably refused to supply personal data in response to a data subject request, he may seek a court order compelling the employer to do so. This might also lead to enforcement action by the Information Commissioner. However persistent or vexatious requests will not be assisted by the Information Commissioner or the court, which is obliged to take into account the frequency of requests and other relevant circumstances when considering whether to grant an order under s7(9) DPA 1998.

Employees may also have redress against employers under the s 13 DPA 1998 where they suffer damage or damage and distress as a result of any unauthorised processing and where the employer is unable to prove that he had taken reasonable care. However in Johnson v Medical Defence Union Limited (No.2) [2006] EWHC 321 Mr Justice Rimmer made it clear that there was nothing in the 1998 Act giving a data subject the right to compensation for a general loss of reputation. Such a claim would need to be made under the law of defamation.

4.6 The Information Commissioner’s Employment Practices Code

Observance of the DPA 1998 in the context of employee relationships is complex. To assist employers with their obligations under the DPA 1998 the Information Commissioner has issued the Employment Practices Code. Part Three of this Code covers the issues relating to employers who monitor the activities of their workers. The other parts of the Code which are not discussed here relate to recruitment (Part One), employee records (Part Two) and medical records (Part Four).

The Code contains a set of guidelines intended to apply to employers of all sizes. The Code is based on the Information Commissioner’s interpretation of the DPA 1998 and states what employers must do in order to comply with the Act. The Code itself is neither a statute nor a regulation but failure to comply with the Code will be taken into account by the Information Commissioner when determining whether to issue an enforcement notice for breach of the DPA 1998. The Information Commissioner has also issued a set of supplementary guidance which provides further insight into the issues covered in the Code itself.

The Code is concerned with the collection of information about employees with a view to checking their performance or conduct. It covers all types of monitoring including the use of CCTV, in-vehicle monitoring and covert monitoring as well as the monitoring of electronic communications.

The Code is primarily concerned with “systematic monitoring”. This involves the monitoring of all workers as a matter of routine, perhaps by using automated software to scan all e-mail messages.
Examples of activities addressed in the Code which relate to electronic communications are as follows:

(i) randomly opening an individual’s e-mail or listening to their voicemail while searching for evidence of malpractice;

(ii) the use of automated checking software to collect information about workers (e.g. to see exactly what they are sending and receiving). As discussed above, this would also amount to interception under RIPA 2000 (see sections 2 and 3 above);

(iii) examining a log of websites visited in order to check that individual workers are not downloading pornography;

(iv) storing recordings of telephone calls made to or from a call centre either to listen to as part of employee training or to simply to have on record to refer to in the event of a customer complaint; and

(v) systematically checking logs of telephone numbers called to detect the use of premium rate services.

Although the Code makes it clear that the DPA 1998 still applies to “occasional monitoring”, that is where an employer introduces monitoring as a short term measure in response to a particular problem, this type of activity is less likely to be covered by the Code. Examples of “occasional monitoring” would include keeping a watch on e-mails sent by a worker suspected of racial harassment or installing a hidden camera when workers are suspected of drug dealing on the employer’s premises. Furthermore the Code does not apply to occasional access to business records which have not been collected primarily with a view to keeping a watch on employees’ performance or conduct. Examples of these types of activities include:

> looking back through customer records in the event of a complaint to check that the customer was given the correct advice;

> checking a collection of e-mails sent by a particular worker which is stored as a record of transactions. This is permitted to ensure the security of the system or to investigate an allegation of malpractice; or

> trawling back through a log of telephone calls made which is kept for billing purposes. This is allowed where it is undertaken to establish whether a worker suspected of disclosing trade secrets has been in contact with a competitor.

The effect of this is that the Code does not really provide guidance in relation to one-off access to business records. Businesses that wish to access such records may wish to consult Part Two of the Code which relates to employment records and provides guidance relating to grievance and disciplinary investigations. In general terms, however, the act of looking through business records
which includes personal data will still amount to “processing” under the DPA 1998 even though it is not addressed in the Code. Employers must therefore ensure that such processing is done fairly and lawfully and that the rules on data export are observed (see section 4 above).

4.7 Impact assessment under the Code

Neither the Code nor the DPA 1998 prevent monitoring. However the Code requires that any adverse impact that monitoring might have on employee privacy is justified by the benefits to the employer and others. To assess whether monitoring can be justified, the Code suggests that employers carry out an “impact assessment” in order to establish the following:

(i) What is the purpose behind the monitoring arrangement and what are the benefits it is likely to deliver?

(ii) What is the likely adverse impact of the monitoring arrangement? For example, what intrusion will there be into the private lives of workers and others? Will there be interference with their private e-mails? Will workers know about the monitoring and be in a position to act in order to limit the intrusion? Will the monitoring result in confidential or otherwise sensitive information being seen by those who do not have a business need to know?

(iii) What alternatives are there to monitoring or are there different ways in which it might be carried out? (For example, employers should consider whether automated software programs are more appropriate means of monitoring as opposed to human intervention or whether a spot check on an individual is preferable to blanket monitoring.)

(iv) What obligations arise from the monitoring? (For example, have employees and third parties been notified of the monitoring? Have all the data protection principles been observed?).

(v) Is the monitoring justified? (The assessment should consider factors such as the benefits expected, the adverse impact and alternatives, whether any intrusion is really necessary and any consultation with trade union or other employee groups.)

Impact assessments must be carried out in respect of each type of monitoring (e.g. e-mail, internet, telephone and voicemail).

The Code maintains that making an impact assessment need not be a complicated or onerous process. However, it does recommend that where appropriate the steps carried out are documented in some way. This may be helpful in circumstances where the employer has to justify monitoring as a result of a complaint by an employee.
4.8 Good Practice Recommendations under the Code

The Code sets out a number of “good practice recommendations” under six separate headings. Those which are of specific relevance to the monitoring of electronic communications are set out in the Appendix.

It is important to note that, unlike the Lawful Business Regulations which apply only to interception activities, these recommendations will apply to all intrusive monitoring controls. The following are important issues to consider:

General considerations

Before implementing any monitoring activity the relevant line managers should ensure that they are complying with internal procedures and that they are acting with authority. In most cases line managers will need to be briefed on the relevant aspects of RIPA 2000 and the DPA 1998 before commencing a monitoring exercise to avoid compliance issues. Where the monitoring is intended to enforce the organisation’s rules and standards it is important that these rules and standards are properly communicated to employees as well as details of the nature and extent of any monitoring (see “Informing employees” below). In all cases businesses should ensure that those who have access to personal data obtained through monitoring are kept to a minimum and that information collected for monitoring purposes is not used for other purposes unless it is clearly in the individual’s interest to do so or if the information collected reveals activity that no employer could reasonably be expected to ignore.

Informing employees

As with the Lawful Business Regulations, all employees must be informed of any monitoring of their communications. The obligations under the DPA 1998 are likely to be more onerous than under the Lawful Business Regulations. For example, the Code makes it clear that simply informing workers that their e-mails may be monitored may not be sufficient. Employees should be left with a clear understanding of when information about them is likely to be obtained, why it is being obtained and how it will be used and who it will be disclosed to. As discussed in section 5 below, the best way of complying with this requirement would be to document the company’s monitoring policy and to distribute it to all employees.

Informing third parties

The extent to which third parties (i.e. individuals who e-mail or call employees) need to be informed of any monitoring is unclear. The supplementary guidance to the Code states that the key issue is to try and identify whether or not any monitoring may be self-evident. For example, the use of automated software for the purpose of virus-checking incoming e-mails would not need to be disclosed to any external sender of e-mails even though this might involve processing their personal data. However, if information about external contacts is to be used in a way which is not expected, then they should be informed. The recording of telephone calls and the interception of communications which are clearly personal would in most circumstances not be
expected by third parties and in cases where this takes place third parties would need to be given advance notice. In the case of telephone calls, this may be done by way of recorded message or by instructing employees to inform their callers that communications are being recorded. It is less clear how e-mail correspondents would be informed although the Code suggests that in the case of unsolicited e-mails sent to employees, information relating to any monitoring (other than that carried out by automated means for the purpose of virus-checking) may be provided in any response.

**Monitoring telephone calls**

The Code distinguishes between listening in of calls (e.g. in call centres) and actual recording of calls. Although listening in of calls would amount to an interception and therefore subject to the Lawful Business Regulations, the Code only applies to the recording of calls.

Blanket recording of the content of telephone calls should be avoided. Employers should consider whether any need for monitoring calls may be met in the first instance by referring to itemised call records. Where calls are recorded both employees and any external callers should be informed unless it is self-evident that recording is taking place.

In relation to mobile phones, the Code makes it clear that employees may have a greater expectation of privacy where mobiles, for which the employer pays, are used outside the workplace (either at home or on business). In these cases they should be aware of the nature of and reasons for any monitoring.

Where employers think that it is necessary to check the voicemail accounts of workers who are absent from the office, employers must make sure that employees are aware that this will happen.

**Monitoring e-mail**

When considering what type of monitoring should be applied to e-mail, employers should consider which controls are less likely to have an adverse impact. In particular the use of automated software is preferable to human intervention. As indicated above, employees (and where relevant external senders of e-mails) must be informed of the extent of any monitoring. Wherever possible, employers should ensure that e-mail monitoring is confined to addresses or headings unless it is essential for a valid and defined reason to examine content. Employers should also avoid opening e-mails which clearly show that they are private or personal. Where employee e-mail accounts need to be checked in the absence of workers, employers must make sure that employees are aware that this may happen.

**Monitoring internet use**

Where internet access is monitored, employers should consider using controls which prevent rather than detect misuse of the internet, such as automated blocking software. Again, employees must be informed of such monitoring.
5. COMPANY POLICIES

5.1 Obligations under the Lawful Business Regulations and the DPA 1998

As discussed above, both the Lawful Business Regulations and the DPA 1998 require employers to inform employees about the different monitoring activities that they undertake. Neither the Act nor the Regulations prescribe how employees should be informed; however the Code recommends that where employers wish to monitor electronic communications they should establish a policy on their use and communicate it to employees. The recommendations on what such a policy should include are set out in the Appendix.

The supplementary guidance to the Code makes it clear that even where an employer has set out a clear policy regarding its monitoring activities an employee’s expectation of privacy will invariably also be based on how that policy is enforced in practice. For example, if an employer bans personal telephone calls but then repeatedly turns a blind eye to a limited number of personal calls, the employee may justifiably have an expectation of privacy in relation to those calls. The employer would therefore not be able to use the ban as the basis of its impact assessment justifying a blanket recording of all calls on the grounds that there should not be any personal calls being made. Employers should therefore set standards and policies which are based on actual practice and enforce them.

The process of drafting such a policy will invariably amount to an “impact assessment” of all the proposed monitoring and will assist a company in ensuring that their policies fall within the recommendations of the Code.

5.2 Using company policies to limit liability

Apart from ensuring that employers fulfil their legal obligations to inform employees, there are a number of other advantages to introducing a policy on electronic communications. In particular, the policy can be used to set out the standards that the company would expect employees to observe when using company systems. By setting standards, the employer is effectively attempting to reduce the possibility of their systems being used in a manner which would lead to liability for the company. This form of persuasive control together with the use of banners (discussed in section 5.3 below) can often be as effective in reducing liability for a company as the use of intrusive controls, such as interception of communications.

Issues such as defamation, inadvertent commitments, discrimination and confidentiality will all be of concern to employers.

Defamation

If employees make defamatory statements in e-mails, employers may be held vicariously liable for that defamation if the statement is made in the course of their employment. This can be the case even where the employer has not authorised the statement. An example might be where a sales representative makes defamatory comments about a rival firm.
To avoid charges of defamation, employers should specifically state in their company policies that employees are to treat e-mail as a mode of formal correspondence, akin to a letter as opposed to a telephone conversation. This principle applies as much to ‘internal’ e-mails as to those addressed to recipients outside the company. Liability for defamation can arise even where an employee’s libel is published only to his colleagues. Employees should also be made aware that in the case of a claim being brought against the company all e-mails may need to be disclosed and that even apparently deleted e-mails may be traced and recovered.

**Inadvertent commitments**

Given the informal nature of e-mail, one of the major concerns is that employees enter into commitments without proper authority or make representations to another firm of which the employer is unaware.

This problem is not unique to e-mail: it could equally apply to conversations over the telephone. However, e-mail will leave a trail, being stored on the systems of both the employer and the other party. As such, a party seeking to rely on e-mail discussions as evidence of misrepresentation or contractual terms will not face such severe evidential problems as one seeking to rely on oral conversations to the same end. In this respect, employees must be made to recognise that e-mail is to be regarded as a formal means of communication and should be treated accordingly.

**Discrimination**

Where the content of employees’ e-mails may give rise to a claim for sexual harassment or discrimination, the employer may well be held liable. Section 41 of the Sex Discrimination Act 1975 provides that in the context of such a claim, anything done by an employee in the course of his employment will be treated as done by his employer, irrespective of whether it is done with the employer’s knowledge or approval. There are parallel provisions in the Race Relations Act 1976.

Such vicarious liability can be avoided only if the employer can show that it took all practicable steps to prevent employees from committing such acts in the course of their employment. Issuing clear guidelines as to unacceptable e-mail content together with a warning that breaches of those guidelines will be sanctioned as a serious disciplinary offence, will not necessarily be conclusive but may assist in avoiding liability.

**Confidentiality and privilege**

In the absence of sabotage by third parties, there are two ways in which confidentiality might be breached by e-mail, namely:

(a) deliberate or inadvertent disclosures by employees; and

(b) failure by the company and/or employees to impose effective obligations of confidence on the recipients of e-mails containing sensitive information.
As regards (a), there is little that can be done to prevent deliberate breaches of confidence by employees, save for including in the e-mail policy a section on the importance of protecting confidential information and pointing to the serious disciplinary consequences that will follow from breaching this guideline. Inadvertent disclosures may be minimised in the same way and requiring employees to include a confidentiality disclaimer before sending messages may reinforce the impact of the relevant policy statement (see section 5.3 below).

The problem noted at (b) arises because a company’s correspondents will be required to treat information received from the company as confidential only if placed under a contractual or equitable obligation to do so. The use of a confidentiality banner may be helpful in this regard as it will inform the recipient of the e-mail of the confidential nature of that communication. However, in order to rely on such a banner it is important that it is brought to the attention of the recipient and this is best achieved by placing the disclaimer at the top of the e-mail. In this way the recipient is put on notice of the confidential nature of the e-mail’s contents before he reads it (see section 5.3 below).

A related issue concerns legally privileged e-mail correspondence. Normally legal privilege attaches to all confidential legal advice given to clients by their counsel, which will mean that in civil proceedings the client will not be obliged to disclose that advice to the other side. The sending of advice by e-mail will not itself amount to a waiver of privilege and it is not necessary for a banner to specifically state that a communication is privileged for it to be so. However, it is important to note that privilege will be lost if the privileged document is disclosed other than under express and strict conditions of confidentiality. It is therefore important to consider whether unencrypted e-mail is the most appropriate means for delivering legally privileged advice bearing in mind that the excessive distribution of an e-mail, even wholly within a company, may lead to waiver of privilege.

Security and other issues

The standards that an employer will want to introduce will vary from organisation to organisation. However, in addition to the issues discussed above, employers may consider that their company policies require that all employees:

> refrain from disseminating material unless the copyright in the material belongs to the company;

> do not send or solicit large files by e-mail;

> do not send or solicit junk or spam e-mail;

> do not use company e-mail addresses for personal use; and

> do not send e-mails or make telephone calls from another employee’s work station.
5.3 Banners

All e-mails sent by employees to recipients ought to have a banner ‘disclaimer’ attached. The purpose of such a banner is to limit the company’s liability for the content of the e-mail.

Banners are generally short and in standard form. This can raise issues where they are used to limit liability on a wide range of issues. In addition, banners are frequently applied automatically even in circumstances where they are inappropriate. For example, frequent use of a banner stating that a communication is legally privileged or confidential when it clearly is not may lead to problems where the employer wishes to rely on such disclaimers in situations where the communication is in fact confidential. Employers should therefore carefully consider what risks are most relevant to their businesses and then adopt the most suitable banner. Banners should be reviewed regularly.

Companies which allow employees to use e-mail for personal use should consider developing alternative banners. This is because the employer is more likely to want to limit liability for all personal content and as such will require a much more strongly worded disclaimer. This will allow the company banner to focus on the primary concerns (for example confidentiality). The appropriate disclaimer should be included at the top of the e-mail, so that the recipient can be presumed to have read the statement before reading the body of the communication. The e-mail system should be configured such that it is not possible for an external e-mail to be sent without the relevant banner attached. If there are alternative banners for business and personal use, the option to attach one of them (but not both or neither) should be given automatically once the sender has elected to send the e-mail but before it is sent.

This memorandum is not intended to contain definitive legal advice which should be sought as appropriate in relation to any particular transaction. If further information or advice is required, please contact your usual adviser at Slaughter and May.

© Slaughter and May, 2006
APPENDIX

Good Practice Recommendations under the Code

The following are extracts from part three of the Information Commissioner’s Employment Practices Code, which is available at www.ico.gov.uk

3.1 The general approach to monitoring

3.1.1 Identify who within the organisation can authorise the monitoring of workers and ensure they are aware of employer’s responsibility under the Data Protection Act 1998.

3.1.2 Before monitoring, identify clearly the purpose(s) behind the monitoring and the specific benefits it is likely to bring. Determine – preferably using an impact assessment – whether the likely benefits justify any adverse impact.

3.1.3 If monitoring is to be used to enforce the organisation’s rules and standards make sure that the rules and standards are clearly set out in a policy which also refers to the nature and extent of any associated monitoring. Ensure workers are aware of the policy.

3.1.4 Tell workers what monitoring is taking place and why, and keep them aware of this, unless covert monitoring is justified.

3.1.5 If sensitive data are collected in the course of monitoring, ensure that sensitive data condition is satisfied.

3.1.6 Keep to a minimum those who have access to personal information obtained through monitoring. Subject them to confidentiality and security requirements and ensure that they are properly trained where the nature of the information requires this.

3.1.7 Do not use personal information collected through monitoring for purposes other than those for which the monitoring was introduced unless: (a) it is clearly in the individual’s interest to do so; or (b) it reveals activity that no employer could reasonably be expected to ignore.

3.1.8 If information gathered from monitoring might have an adverse impact on workers, present them with the information and allow them to make representations before taking action.

3.1.9 Ensure that the right of access of workers to information about them which is kept for, or obtained through, monitoring is not compromised. Monitoring systems must be capable of meeting this and other data protection requirements.

3.1.10 Do not monitor workers just because a customer for your products or services imposes a condition requiring you to do so, unless you can satisfy yourself that the condition is justified.
3.2 Monitoring electronic communications

3.2.1 If you wish to monitor electronic communications, establish a policy on their use and communicate it to workers – see “Policy for use of electronic communications” below.

3.2.2 Ensure that where monitoring involves the interception of a communication it is not outlawed by the Regulation of Investigatory Powers Act 2000.

3.2.3 Consider – preferably using an impact assessment code – whether any monitoring of electronic communications can be limited to that necessary to ensure the security of the system and where self-assessment can be automated.

3.2.4 If telephone calls or voicemails are, or are likely to be, monitored, consider – preferably using impact assessment – whether the benefits justify the adverse impact. If so, inform workers about the nature and extent of such monitoring.

3.2.5 Ensure that those making calls to, or receiving calls from, workers are aware of any monitoring and the purpose(s) behind it, unless it is obvious.

3.2.6 Ensure that workers are aware of the extent to which you receive information about the use of telephone lines in their homes, or mobile phones provided for their personal use, for which your business pays partly or fully. Do not make use of information about private calls from monitoring, unless they reveal activity that no employer could reasonably be expected to ignore.

3.2.7 If e-mails and/or internet access are, or are likely to be, monitored, consider – preferably using an impact assessment – whether the benefits justify the adverse impact. If so, inform workers about the nature of the extent of all e-mail and internet access monitoring.

3.2.8 Wherever possible avoid opening e-mails, especially ones that clearly show they are private and personal.

3.2.9 Where practical, and unless this is obvious, ensure that those sending e-mails to workers, as well as workers themselves, are aware of any monitoring and the purpose behind it.

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

3.2.11 Inform workers of the extent to which information about their internet access and e-mails is retained in the system and for how long.
Policy for use of electronic communications

Employers should consider integrating the following data protection features into a policy for the use of electronic communications:

> Set out clearly to workers the circumstances in which they may or may not use the employer’s telephone systems (including mobile phones), the e-mail system and internet access for private communications.

> Make clear the type and extent of private use that is allowed, for example restrictions on overseas phone calls or limits on the size and/or type of e-mail attachments that they can send or receive.

> In the case of internet access, specify clearly any restrictions on material that can be viewed or copied. A simple ban on ‘offensive material’ is unlikely to be sufficiently clear for people to know what is and is not allowed. Employers may wish to consider giving examples of the sort of material that is considered offensive, for example material containing racist terminology or nudity.

> Advise workers about the general need to exercise care about any relevant rules, and about what personal information they are allowed to include in particular types of communication.

> Make clear what alternative can be used, e.g. the confidentiality of communications with the company doctor can only be ensured if they are sent by internal post, rather than by e-mail, and are suitably marked.

> Lay down clear rules for private use of the employer’s communication equipment when used from home or away from the work place, e.g. the use of facilities that enable external dialling into company networks.

> Explain the purposes for which any monitoring is conducted, the extent of the monitoring and the means used.

> Outline how the policy is enforced and penalties which exist for a breach of policy.
CONTACT ADDRESSES

London
One Bunhill Row
London EC1Y 8YY
United Kingdom
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Paris
130 rue du Faubourg Saint-Honoré
75008 Paris
France
T +33 (0)1 44 05 60 00
F +33 (0)1 44 05 60 60

Brussels
Square de Meeûs 40
1000 Brussels
Belgium
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
47th Floor
Jardine House
One Connaught Place
Central
Hong Kong
T +852 2521 0551
F +852 2845 2125

www.slaughterandmay.com