

THE EMPLOYMENT PRACTICES DATA PROTECTION CODE

Part 3: MONITORING AT WORK: SUPPLEMENTARY GUIDANCE.



A. ABOUT THIS GUIDANCE

This guidance does not in itself form part of the Information Commissioner's 'Employment Practices Data Protection Code'. It is intended to complement the main Code by giving supplementary information about the issues covered in it. This guidance includes notes and examples as well as a set of frequently asked questions and useful contact details. We hope it will be of use to those seeking a more in-depth understanding of the issues covered in the Code itself.



B. NOTES AND EXAMPLES.

This section of the Supplementary Guidance is designed to be read alongside the relevant good practice recommendations of the Code itself. These notes and examples are intended to give readers a better understanding of some of the practical issues that may arise when implementing the Information Commissioner's good practice recommendations.

3.1. Managing Data Protection.

- 3.1.1.** In a small business the responsibility might simply be with the owner of the business. Where there is a management structure, responsibility should be allocated to a senior manager in the personnel or human resources function or someone in a comparable position. Those with overall responsibility must be in a position to feed their knowledge into other areas of the business where information about workers is processed, and to ensure that the organisation has a co-ordinated approach to data protection compliance.

Ideally data protection should be seen as an integral part of employment procedures rather than as a stand-alone requirement. For example, in the company's IT security procedure there should be a section on monitoring which should be based on the relevant benchmarks in this Code. Procedures are only of value if they are current and adhered to. Review and upgrade procedures as necessary and put a mechanism in place to ensure that they are being followed on the ground. This might involve some form of audit or self-certification by managers.

- 3.1.2.** It is important to remember that data protection compliance is a multi-disciplinary matter. For example, a company's IT staff may be primarily responsible for keeping computerised personal information secure, whilst a human resources department may be responsible for ensuring that the information requested on a job application form is not excessive, irrelevant or inadequate. All workers, including line managers, have a part to play in securing compliance, for example by ensuring that waste paper bearing personal information is properly disposed of.

An employer is liable to pay compensation for damage suffered by an individual as a result of a breach of data protection law arising from the actions of a line manager unless it is clear that the line manager has been acting outside his or her authority. Employers can help protect themselves against claims by training line managers and having clear procedures in place.

- 3.1.3.** It may be helpful to assess personal information held on workers using the same categories as are used in the various parts of this Code, i.e. personal information processed in connection with recruitment and selection, employment records, monitoring at work and medical information. Consider who in your organisation will be collecting, using, storing and destroying such information. Only when you have ascertained this will you be able to check that your organisation is complying with the Act.
- 3.1.4.** When making your assessment of personal information consider if all the information collected on workers is necessary for the employment relationship. For example, information concerning workers' lives outside work is unlikely to be necessary. However, it might be legitimate to request information about workers' other jobs where there is a justifiable need, for example, in connection with Working Time Regulations, or to request information about their children in connection with an application for parental leave.
- The collection and use of sensitive data must satisfy a sensitive data condition.
- 3.1.5.** Workers should be broadly aware of the legal duties that the Act places on employers and their own role as workers in meeting them. In particular, workers should be aware of how data protection compliance impinges in practical terms on the way they perform their work. It is also crucial to make workers aware of the possible consequences of their actions in this area, e.g. disciplinary action or personal criminal liability. It is useful to incorporate such information in the general induction process for new workers and to regularly remind existing workers of their obligations
- 3.1.6.** Failing to notify when required to do so or failing to keep a notification up to date is a criminal offence. The person responsible for data protection should ensure that entries concerning workers' data on the Register of data controllers are complete, accurate and up-to-date. This may be a duty that he or she personally undertakes or it may be delegated.

3.2. The general approach to monitoring.

- 3.2.1.** There are risks that the Act will be breached if line managers institute monitoring of their workers without authority and without taking into account the provisions of this Code. Business practices should be designed to ensure that monitoring does not take place without careful consideration of the requirements of the Act and this Code.
- 3.2.3.** If monitoring is to be justified on the basis that it is necessary to enforce the organisation's rules and standards, these rules and standards must be known and understood by workers. In some cases the standards may be obvious, for example that it is unacceptable to engage in criminal activity in the workplace, but in others they may not. The easiest way of doing this is likely to be to set out rules and standards, for example in relation to acceptable uses of e-mail systems and internet access, in a policy that is made known to and accessible by all workers affected. Either in this policy or separately, the employer should go on to set out the circumstances in which monitoring may take place, the nature of the monitoring, how information obtained through monitoring will be used, and the safeguards that are in place for the workers who are subject to the monitoring.
- 3.2.4.** Workers who are subject to monitoring should be aware when it is being carried out, and why it is being carried out. Simply telling them that, for example, their e-mails may be monitored may not be sufficient. They should be left with a clear understanding of when information about them is likely to be obtained, why it is being obtained, how it will be used and who, if anyone, it will be disclosed to. The necessary information can be provided, for example, through signage in areas subject to monitoring or through details given in a staff handbook. Workers should be kept aware of existing monitoring, perhaps by reminding them periodically. Where significant changes to monitoring arrangements are introduced they should be told about these.

- 3.2.6.** Monitoring may involve others having access to personal information about workers. In some cases the information may be of a private nature, for example if monitoring extends to the content of e-mail messages. As far as possible such information should be excluded from monitoring. Where this is not possible and monitoring is nevertheless justified the numbers of those who have access to the information must be kept to a minimum. They must be subject to rules to ensure the information is kept securely, not misused or improperly disclosed. They should also be trained to understand the data protection principles that arise when carrying out monitoring. Monitoring may well be more intrusive if those who have access to private information are close colleagues or the manager of a worker. Therefore employers should take care to identify the most appropriate person/people to undertake monitoring, for example for larger businesses this might be those with security or personnel responsibilities.
- 3.2.7.** Personal information obtained for a particular purpose should not be used in a way that is incompatible with that purpose. If monitoring is justified on the basis of addressing a specific risk faced by the employer, the use of information to address a lesser risk, that on its own would not justify monitoring, should be avoided. It is in any case likely to be unfair to workers to tell them that the monitoring is undertaken for a particular purpose and then use the information for another purpose that they have not been told about unless it is clearly in the worker's interest to do this or the information reveals activity that no employer could reasonably be expected to ignore. The type of activities that an employer could not reasonably be expected to ignore might include criminal activity at work, gross misconduct or breaches of health and safety rules that jeopardise other workers.
- 3.2.8.** Equipment or systems malfunction can cause information collected through monitoring to be misleading or inaccurate. Information can also be misinterpreted or even deliberately falsified.
- 3.2.9.** Many businesses buy monitoring systems 'off the shelf'. In such cases the business should make sure the system facilitates data protection

compliance. In other cases appropriate system requirements should be specified. Particular care should be taken with suppliers from outside the EU who may not be used to working within the confines of data protection law. The legal responsibility for compliance rests clearly with users rather than suppliers of systems. Users cannot simply blame the system. The Information Commissioner does though recognise that it may take some time to bring existing systems up to the desired standards. He will take this into account should the possibility of enforcement action arise as a result of a breach of the Act.

If personal information is kept or collected by an employer for its purposes the information must be made available to the worker if an access request is made, unless an exemption applies. (See Employment Practices Code, Part 2, section 9, 'Workers access to information about themselves' for more information about this.) With e-mail or video monitoring this may be onerous, particularly if the system used does not store information in a way that makes any personal information readily retrievable. This is a factor employers should take into account in their impact assessment.

- 3.2.10** Sometimes a customer for a supplier's products or services may seek to impose a condition requiring the supplier to monitor its workers. For example a contractor working in a defence establishment may be required to undertake periodic security checks on those workers employed on the relevant contract. If this monitoring involves processing personal information about the workers it will not be justified simply because it is a condition of business. Such a condition cannot override the employer's obligation to comply with the Act. Monitoring of workers by the supplier or contractor must be based on the outcome of its own assessment. This does not stop the supplier or contractor being guided by any assessment the customer for its products or services might have undertaken for itself.

3.3. Monitoring electronic communications

3.3.1. It is a fundamental requirement of data protection law that workers are aware of the monitoring. One way to achieve this is for the employer to establish, document and communicate a policy on the use of electronic communications systems. However workers will base their expectations of privacy not only on the employer's stated policy but also on its practice. For example, if the employer's policy imposes a ban on personal telephone calls but in practice the employer 'turns a blind eye' to a limited number of personal calls, the employer will not be able to depend on there being a complete ban as its justification for carrying out monitoring. The capabilities of electronic systems should be used to remind workers of their responsibilities. These can be set so that workers cannot proceed to access the internet or e-mail services without acknowledging the acceptance of certain conditions.

3.3.2. Except in limited circumstances that are unlikely to apply to the monitoring of communications by employers, interception, without the consent of sender and recipient, is against the law unless it is authorised by the Lawful Business Practice Regulations. This is the case for both public and private sector businesses. An interception occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. It therefore includes access to e-mails before they have been opened by the intended recipient, but does not include access to stored records of e-mails that have been received and opened. Bear in mind that in many cases, for example customer enquiries, the intended recipient of a communication will be the business itself rather than a specific individual. Monitoring of such incoming communications by the business will not involve an interception. There are though likely to be incoming communications, including but not limited to private ones, where the intended recipient is a specific individual. Monitoring that extends to the content of these before they have been opened by the intended recipient is likely to involve an interception.

See Part E of this document, on the Lawful Business Practice Regulations, for more information about this.

Where practicable limit monitoring to that necessary to ensure the security of the system, e.g. protection from intrusion and from malicious code such as viruses or Trojans, or detection of the misuse of passwords.

Take account, particularly in any impact assessment, of the ability of automated monitoring to reduce the extent to which extraneous information is made available to any person other than the parties to a communication. For example, monitoring to protect the security of a system can generally be automated. Monitoring to detect references to matters of particular sensitivity, for example the name of a company involved in a merger negotiation, might also be automated. Automated monitoring systems are becoming increasingly sophisticated and their capabilities should be exploited to assist data protection compliance, for example through the ability to target monitoring at suspicious patterns of activity.

- 3.3.4** Do not introduce monitoring or the recording of the content of calls in all cases. If recording is necessary to provide evidence of business transactions, e.g. in telephone banking, and it is undertaken only for this reason it will not be 'monitoring' within the scope of this part of the Code. Recording should though be limited to those calls involving, or likely to involve, transactions. Take into account, particularly in any impact assessment, the possibility that acceptable benefits might be achieved by the use of an itemised call record. If the itemised call record alone is insufficient, assess whether it can be used to help ensure that monitoring is strictly limited and targeted. For example, there might be evidence that commercial secrets are being passed to a competitor. By examining itemised call records it might be possible to narrow down those under suspicion and target monitoring accordingly.

See 'How Intrusive is Your Monitoring' on page 27 of this document for more information about this.

- 3.3.5.** Although this Code of Practice is primarily concerned with information about workers rather than external callers, employers should bear in mind that monitoring workers will often involve collecting information about those people who make calls to or receive calls from the organisation as well as about workers themselves. Where monitoring goes beyond simply listening-in in real time on calls without recording them and so involves the processing of personal data, these people should also be told that monitoring is taking place and why. Unless it is self-evident that monitoring is taking place and why, provide this information, where reasonably practicable, through the use of recorded messages on telephone systems. Don't forget that those who might be making personal calls to workers are less likely to expect that their calls may be monitored, or to understand why, than, for example, customers who might expect some recording to take place. If there is no better way of providing information, instruct workers to inform callers that their calls may be recorded and to explain why this is the case.

3.3.6. Where employers pay for mobile phones which workers may use for personal calls or for land lines in their homes, they may receive itemised bills directly or via their workers. Employers should bear in mind that workers' expectations of privacy are likely to be significantly greater at home or outside the workplace than in the workplace. This distinction should be reflected in making an impact assessment. If bills are received directly, workers should be made aware of the extent of information about personal use received by the employer. In either case, information about personal calls should not be used for monitoring. It may be used for billing or in exceptional circumstances, where there is evidence of work related criminal activity, accessed as part of a specific investigation.

3.3.7. In an impact assessment of e-mail monitoring you should consider the following;

- Can analysis of e-mail traffic rather than monitoring the content of messages be used? If the traffic record alone is not sufficient, can the traffic record be used to narrow the scope of content monitoring, for example to restrict any examination of the content of messages to those that are being sent to a rival organisation?
- Is it feasible to use an automated monitoring and detection process that for example detects malicious code such as viruses or Trojans, or limits the size of attachments that can be received?
- Is there a risk that monitoring the content of messages will breach a duty of confidence owed to workers or customers?
- Are there secure lines of communication, for example for the transmission of sensitive information from the worker to an occupational health advisor or for trade union communications that will not be subject to monitoring? Some systems can be set up so that messages to and from particular individuals or sections of the organisation are not subject to monitoring or are monitored differently to others.
- Is there a system that allows workers to mark personal communications as such?
- What would be the implications of making adjustments to the system, for example to provide facilities that allow messages to be sent that do not bear the employer's 'official' heading? The provision of such facilities should reduce the risk of employers' liabilities in respect of personal e-mails sent using the employer's equipment.

- Can any monitoring be confined to external rather than internal e-mail messages? In some cases monitoring of internal messages might be more intrusive for workers whereas the benefits of monitoring might come mainly from external messages.
- Can e-mails that are marked personal, or which there are other grounds to believe are personal, be excluded from monitoring or treated differently? Apart from automated monitoring which rejects or returns unacceptable messages for security reasons messages that are personal should only be opened in exceptional circumstances, for example where a worker is suspected of using e-mail to harass other employees.
- Is there a ban on personal use of the e-mail system or a restriction on the types of messages that can be sent? Such a ban or restriction does not in itself justify the employer knowingly opening messages that are clearly personal. However an employer designing monitoring is entitled to work on the assumption that messages in the system are either all likely to be business ones or, if personal, are only likely to be of a particular type. If personal use is prohibited it may be possible to detect personal messages from the header or address information and take action against the sender or recipient without opening them.
- Are workers provided with a separate e-mail account or an encryption capability? Are they allowed access to web-based mail services for personal use?
- Are systems for recording information about e-mail use reliable? Employers should bear in mind that e-mails and associated records can be misleading or even falsified, and if cited in court could be challenged.

In an impact assessment of internet access monitoring you should consider the following;

- Can monitoring that prevents rather than detects misuse be used, for example by blocking access to inappropriate sites or material by using web-filtering software? Consider the capabilities of the latest technology, for example, products are available that, it is claimed, can undertake complex analysis of images and thereby prevent the display of sexually explicit material without disrupting normal business activity.

- Is it possible to prevent misuse of systems by recording the time spent accessing the internet rather by monitoring the sites visited or the contents viewed?
- Is it possible to limit the use of the information collected? For example, if the issue is that a worker has been spending too much time on the internet for purposes that are not work-related, is it necessary for the worker's manager to be told exactly what sites have been visited?
- Can private internet access be separated from business access, perhaps by having a different log-on for private use and then limiting the collection of information on private use to the length and time of the session?
- Can monitoring be done on an aggregated basis, for example examining logs of which sites have been accessed from which departments and only focussing on specific workers if it is apparent there is a problem?

See 'How Intrusive is Your Monitoring' on page 27 of this document for more information about this.

3.3.8 Accessing the contents of a worker's personal e-mails or other correspondence will be particularly intrusive. This should be avoided wherever possible. It is particularly important if the worker has a genuine expectation of privacy. This might be confined to e-mails where the words 'private' or 'personal' have been included in the message header if workers have been clearly instructed to mark personal e-mails in this way. If the content of personal e-mails is to be accessed, the employer must have a pressing business need to do so, e.g. grounds to suspect the worker of work-related criminal activity. This must be sufficient to justify the degree of intrusion involved and there must be no reasonable, less intrusive alternative. It is recommended that the impact assessment approach is used to determine whether this is the case. An employer is, of course, entitled to take into account anything workers may have been told about the likelihood and extent of monitoring in its assessment.

- 3.3.9** Monitoring external e-mails will mean processing information about those people who send e-mails to or receive e-mails from the organisation, as well as about workers. Unless it is self-evident, these people are also entitled to be told, where practicable, that monitoring is taking place and why. This may not be easy to achieve. Employers would not, for example, be expected to inform external senders of e-mails that messages will be virus checked even though this may involve processing their personal information. However, if information about external contacts is to be used in ways they would not expect, then they should be told. If e-mail responses are solicited, for example, when job applicants are asked to send in their applications by e-mail, it should be possible to provide any necessary information beforehand, for example in the job advertisement. If e-mails are unsolicited, the information could be provided in any response.
- 3.3.10** The purpose for doing this should be to ensure the business responds properly to its customers and other contacts during a worker's period of absence. Workers should be aware that communications addressed to them will be opened in their absence. Employers may wish to encourage the use of a marking system to help protect personal communications when the intended recipient is absent. Only in exceptional circumstances should e-mails that are clearly personal be opened, for example if the worker is suspected of using the employer's communication system to engage in criminal activity
- 3.3.11** There are a variety of ways in which workers can be told about the retention of information about their e-mail or internet usage. This might be done by giving them an information pack addressing this when they are given access to the office's internet or e-mail systems, or by displaying on-line information on their computer. It is important to ensure that workers are aware of retention periods and, in particular, that they are not misled into believing that information will be either deleted or retained when this is not the case.
- 3.3.12** Websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising or mis-keying. Workers should have the opportunity of explaining or challenging any information before action is taken against them.

3.4. Video & audio monitoring

- 3.4.1.** Continuous video or audio monitoring is particularly intrusive for workers. The two combined are even more intrusive. The circumstances in which continuous monitoring of individual workers is justified are likely to be rare, for example work in particularly hazardous environments such as refineries or nuclear power-stations, or where security is a particular issue, for example in the premises of a precious stone dealer. This is different from the security monitoring of public or semi-public areas where workers may pass from time to time, e.g. corridors or car-parks. Depending on how and why it is set up, such monitoring may not fall within the scope of this part of the Code. It is in any case much more likely to be justified, particularly if one of its purposes is to protect workers or their property.

In an impact assessment of video and/or audio monitoring you should consider the following;

- Can video and audio monitoring be targeted at areas of particular risk, for example where there is a risk to safety or security?
- Can monitoring be confined to areas where workers' expectations of privacy will in any case be low, for example areas to which the public have access?
- Can video and audio capability be treated separately?
- Will the employer be in a position to meet its obligations to provide subject access to and, to the extent that it might be necessary, remove information identifying third parties from audio and video recordings?

Employers carrying out monitoring should make it clear to workers that monitoring is taking place and where and why it is being carried out. This could be done by ensuring that in areas subject to monitoring, a prominent sign is displayed that identifies the organisation responsible for the monitoring and why it is being undertaken, and says who to contact regarding the monitoring. Simply telling workers that from time to time they may be subject to video or audio monitoring is not sufficient. A good rule of thumb for fairness is for the employer to consider whether workers, at the point at which they are subject to monitoring, would be aware that it is taking place. Although in limited circumstances the Data Protection Act allows for covert monitoring, for example where telling workers about the monitoring would be likely to prejudice the detection of crime, workers should normally be told clearly when monitoring is taking place.

- 3.4.3.** Not only workers but also others who might be caught by monitoring should be informed that it is taking place and why it is taking place. Any notification given should identify the organisation responsible for the monitoring, its purposes, and should say who to contact regarding the monitoring.

3.5. Covert monitoring.

- 3.5.1.** Where the carrying out of monitoring results in the collection or other processing of personal information, those who are subject to it should be made aware that it is being carried out and why it is being carried out. The more intrusive the monitoring the more precise the information given to workers needs to be. Where video or audio monitoring takes place workers should have specific information such as the location of cameras or microphones. Where communications are monitored the information may be less specific but workers should know when to expect that information about them will be collected. In any other case the monitoring is likely to be covert.

Covert monitoring is monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place. Employers should ask themselves if the workers about whom they are collecting information would be likely to know the collection is taking place. If the answer is 'no', the monitoring will be covert. Covert monitoring may take place inside or outside the workplace. The covert watching of a worker by another person is not in itself subject to the Data Protection Act, but once it results in a record being kept about the worker, the Act will apply.

Covert monitoring will only be justified in a particular case if openness would be likely to prejudice the prevention or detection of crime or equivalent malpractice or the apprehension or prosecution of offenders. There may be cases where one of the other exemptions in the Act could apply, but these are unlikely to arise in the employment context. It is therefore essential that the employer makes a considered and realistic assessment of whether such prejudice is likely. A reliable test of whether covert monitoring is justified is to consider whether the activity being monitored is of sufficient seriousness that it would be reasonable for the police to be involved. This does not mean, though, that the employer need necessarily involve the police. However, the implications of covert monitoring are such that senior management authorisation ought to be a prerequisite.

- 3.5.3** It is hard to see circumstances where an employer would be justified in installing secret video cameras or other covert monitoring devices in areas where workers would have a genuine and reasonable expectation of privacy. This would include toilets. It is also likely to include closed offices allocated to individual workers for their exclusive use, although the extent to which particular parts of the workplace can genuinely be regarded as private will vary from employer to employer. Whilst in exceptional circumstances covert monitoring in private areas might be

justified, for example where there is evidence of drug-dealing on the premises, any such monitoring should take place with the intention of involving the police.

- 3.5.4** An employer does not avoid its obligations by engaging a private investigator or other agent to collect personal information about workers on its behalf. If an employer engages a private investigator to collect information covertly on workers the private investigator will be a 'data processor'. The employer retains responsibility for data protection compliance. This can be discharged through the contract the employer must have with the private investigator and under which data protection obligations must be placed on the investigator.
- 3.5.5** Limit the number of staff involved in covert monitoring and identify clearly who has authorisation to be involved. Clear rules should be set down limiting the disclosure of and access to personal information obtained. Information about workers who are not the target of the investigation should be deleted as soon as practicable. The type of activities that an employer could not reasonably be expected to ignore might include criminal activity, gross misconduct or practices that jeopardise the safety of others.

3.6. In-vehicle monitoring

3.6.1. In an impact assessment of monitoring of vehicles used by workers you should consider the following;

- Can the monitoring be conducted without yielding information that relates to the private use of vehicles? Information about the location of the vehicle will be the most intrusive.
- Is private use of vehicles supplied by, or on behalf of, the employer, allowed? Where private use of vehicles is allowed, monitoring their movement when used privately, without the freely given consent of the user, will rarely be justified. (Note: this means that if the vehicle is used for both private and business use there ought to be a 'privacy button' or other arrangement that enables the monitoring to be disabled. However where an employer is under a legal obligation to monitor the use of vehicles, even if used privately, for example by fitting a tacograph to a lorry, then the legal obligation will take precedence.)
- Is monitoring of workers' own vehicles to take place? Monitoring of such vehicles will only be justified where the vehicle is being used for business purposes, the worker has freely consented to the installation and use of any monitoring device, and the information collected by the employer is strictly necessary for its business purposes, for example to reimburse the worker for the cost of business use.

The approach of making an impact assessment should be applied to monitoring even if vehicles are provided by, or on behalf of, the employer, exclusively for business and related use, e.g. home to work journeys.

3.6.2 It is important to lay down clear rules as to what private use is or is not allowed of vehicles supplied by, or on behalf of, the employer and the conditions that attach to both private and business use. Workers should be told clearly of any monitoring that takes place and how any information obtained will be used. It should be possible for the user to disable any monitoring of the vehicle's movements when it is being used privately although there may be a facility to override this in exceptional circumstances, e.g. theft.

Ensure workers given access to vehicles are aware of the policy.

3.7. Monitoring through information from third parties.

- 3.7.1.** An impact assessment should be based on the presumption that workers are entitled to keep their private lives private and that employers should not intrude into this unless they face a real risk to which the intrusion is a proportionate response. As part of the assessment, consider whether there is evidence that the monitoring is justified. For example, a worker's financial circumstances should not be monitored unless there are firm grounds on which to conclude that a worker in financial difficulties in the job in question actually poses a significant risk to the employer. One area where this might be the case is in some parts of the financial services industry where there are particular opportunities for fraud.
- 3.7.2.** Workers can be told about the sources that will be used to carry out checks on them in a variety of ways. General information can be put in a staff handbook, displayed on a notice board or delivered on-line to workers with access to computer systems. However, where a specific check is to be carried out, the worker should be directly informed of this unless to do so would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- 3.7.3.** Section 55 of the Act makes it a criminal offence to obtain personal information without the authority of the data controller. Credit reference agencies hold a range of information about individuals. Some can only be used for credit decisions. An employer using a facility for employee monitoring that is provided to assist it in making credit decisions about customers is likely to be obtaining information without the authority of the agency.

Bear in mind that information held by credit reference agencies is based on public records which are not compiled with worker monitoring in mind. They can be incorrect or misleading.

Do not monitor workers through information you have as a result of a different relationship with them, e.g. as a customer or client, unless it is based on a condition of employment and the intrusion caused by the monitoring is justified by the risk faced. This is only likely to be so in special cases, for example a bank must not routinely monitor the bank accounts of all workers. If monitoring can be justified it must be targeted at particular individuals and particular information that poses a risk. For example monitoring to detect serious indebtedness by bank workers with a particular opportunity for fraud might be justified on the basis that preventative action can then be taken. This would not however justify

examining the details of payments made by these workers unless criminal activity was suspected.

- 3.7.5.** As with any worker records, steps should be taken to ensure the reliability of staff that have access to monitoring information. This is especially important where private or confidential information is likely to come into their hands. This is not simply a matter of carrying out background checks; it also involves instruction or training and ensuring that workers understand their responsibilities in respect of such information. Consider placing confidentiality clauses in the contracts of employment of relevant staff.
- 3.7.6.** Once information has been obtained through monitoring and any necessary evaluation of this made, do not retain the information unless there is an overriding reason for doing so. Usually it will be sufficient to record that the evaluation has been carried out and its result. As a general rule, unless there is a legal or regulatory obligation to do so, the information should not be retained for more than 6 months. There might however be some exceptions, for example where the information has ongoing relevance to the placement of the worker, such as might be the case with an employment agency that routinely places its workers in a variety of short-term assignments with its clients.



C. CONDITIONS FOR PROCESSING SENSITIVE DATA: WHEN CAN SENSITIVE PERSONAL INFORMATION BE PROCESSED?

The Act sets out a series of conditions, at least one of which has to be met before an employer can collect, store, use, disclose or otherwise process sensitive personal information. The conditions which are most likely to be relevant to monitoring at work are:-

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

Note: This condition can have quite wide application in the context of monitoring at work. Employers' rights and obligations may be conferred or imposed by statute or common law, which in this context means decisions in relevant legal cases. For example, they will include obligations;

- to ensure the health, safety and welfare at work of workers
- to ensure a safe system of work
- to ensure a safe working environment
- not to discriminate on the grounds of race, sex or disability
- to protect customers' property or funds in the employer's possession
- not to dismiss workers when it is unfair to do so

Thus an employer may be able to collect and use sensitive data in the course of monitoring workers if the monitoring is necessary to enable it to meet its legal obligations, for example to ensure the safety of workers, or to prevent unlawful discrimination. The collection and use of sensitive personal information must however be 'necessary' for exercising or performing a right or obligation that is conferred or imposed by law. This condition would, for example, be satisfied if there is evidence that a worker is using the employer's e-mail system to subject another worker to racial harassment, and there is no reasonable alternative to monitoring the worker's e-mail if the employer is to ensure it meets its obligations not to discriminate on the grounds of race.

- The processing –

a) is of information in categories relating to racial or ethnic origin, religious or other beliefs of a similar nature, or physical or mental health or condition,

b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment,

c) contains safeguards for the data subject.

Note: This condition may have some relevance to monitoring that is designed to prevent discrimination on the grounds of racial origin, religion or disability. Processing must be “necessary”, emphasising that monitoring should only be used where discrimination cannot reasonably be addressed by other means.

- The processing is necessary

- for the exercise of any functions conferred on any person by or under an enactment or

- for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Note: This condition will be relevant for a public sector body that has specific legal duties placed on it in relation to the conduct or probity of its workers. It will also be relevant when a public sector body concludes that in order to discharge its wider statutory functions it is necessary for it to monitor workers and in doing so to process sensitive personal information.

- The processing is in the substantial public interest, is necessary for the prevention or detection of any unlawful act and must necessarily be carried out without the explicit consent of the data subject being sought, so as not to prejudice those purposes.

Note: This condition will cover situations where monitoring is necessary to detect criminal activity in the workplace and where seeking the consent of the workers involved would amount to a tip off. ‘Unlawful acts’ include not only criminal matters but also acts that breach other statutory or common law obligations.

- The processing is in the substantial public interest, is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or other service and is carried out without the consent of the data subject because the processing
 - is necessary in a case where consent cannot be given by the data subject
 - is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or
 - must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

Note: This condition will be relevant to the monitoring of calls to confidential counselling, advice or support lines such as those run by some charities, for example The Samaritans. It will cover the position of the caller but not of the worker taking the call.

- The data subject has given explicit consent to the processing

Note:

Employers seeking to rely on this condition must bear in mind that:-

- *the consent must be explicit.* This means the worker must have been told clearly what personal data are involved and the use that will be made of them. The worker must have given a positive indication of agreement e.g. a signature;
- *the consent must be freely given.* This means the worker must have a real choice whether or not to consent and there must be no significant detriment that arises from not consenting.

The extent to which consent can be relied upon in the context of employment is limited because of the need for any consent to be freely given. For example if the direct consequence of not consenting is dismissal, being passed over for promotion or the denial of a significant benefit that would be given to a consenting worker, consent is unlikely to be freely given.



D. HOW INTRUSIVE IS YOUR MONITORING?

The tables below give guidance on the degree of intrusiveness involved in monitoring the content of various types of communication that are likely to take place in a typical workplace. The tables are intended to illustrate that the more personal the nature of the communication, the higher the threshold for monitoring it. The table on the following page should help employers to carry out the impact assessment referred to throughout this section of the Code.

Pure business communications	
These are the types of communications that only deal with business matters. Typically they would include letters sent out on a business' headed paper or electronic equivalents. The communication contains no information of a particularly personal or intimate nature.	
Example	Guidance on monitoring
<p>1: An e-mail from a company accountant to a supplier querying why an invoice has been submitted for goods that have not been supplied.</p> <p>2: Work contact details monitored these submitted by a health and safety officer to a website so that information about fire safety equipment can be returned.</p>	<p>Disclosure of its contents would be unlikely to cause damage or distress to any worker. To the extent to which it is not obvious, it is sufficient that workers are aware in that general terms that the work they do is likely to be or checked. It is difficult to envisage how communications could be considered to be a disproportionate infringement of privacy.</p>

Business communications including personal information	
These are communications taking place in the workplace that are clearly for genuine business reasons but contain information that is of a personal nature. Many 'personnel' type communications will fall into this category and in many instances the worker identified in this type of communication would object to the information being made widely available in the workplace.	
Example	Guidance on monitoring
<p>1: An e-mail from a worker to a line manager requesting leave of absence from work because of a serious sickness in the family.</p> <p>2: A report submitted by e-mail for a disciplinary hearing relating to a workers alleged misconduct.</p>	<p>A worker must not be misled into thinking that a communication is private if this is not the case. Whether monitoring these communications is a proportionate response will depend very much on the circumstances of of the case. Those carrying out any monitoring should be clear on procedures and fully trained. They have responsibilities to ensure that information obtained through monitoring is kept secure, only used for the purpose for which it was obtained and is deleted once the purpose for carrying out the monitoring is complete</p>

Personal communications	
This Code makes it clear that there is no obligation under the Act for employers to provide communications equipment for workers' own personal use. However, many employers choose to do this. Although employers may provide such facilities, they will need to manage any risks to the business arising from such usage. For example, a worker might use internet access facilities to download pornography in the workplace. It follows, therefore, that even where personal use of communications systems is allowed, there may be exceptional circumstances where monitoring is necessary. There will in any case be a need to check for malicious code to ensure security of the system.	
Example	Guidance on monitoring
<p>1: A worker visiting a patient support group website to seek advice on a condition not related to his or her employment.</p> <p>2: An e-mail between two workers complaining to each other about how they are treated by their employer.</p>	<p>These are circumstances in which workers might reasonably expect that their communications will be private, unless workers have been told clearly that monitoring will take place. Even if workers are told this, it will be intrusive and must be kept to the minimum necessary to address risks. A ban on personal communication does not in itself justify monitoring of the content of such communication. Such a ban and the existence of alternative facilities for personal communications are relevant factors but the monitoring must still be a proportionate response to the problem it seeks to address.</p>



E. THE LAWFUL BUSINESS PRACTICE REGULATIONS

This section provides guidance to employers who wish to monitor electronic communications (e.g. telephone calls, fax transmissions, e-mails, internet access) on how they can meet the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations.). The RIPA and LBP Regulations cover a complex series of situations, of which monitoring in the workplace is only one. This guidance is designed to assist businesses, including public authorities, when they act as employers, but not in other situations. It is intended to cover all the main points but is necessarily simplified. It is not a complete statement of the law but employers following it are unlikely to find themselves on the wrong side of the law.

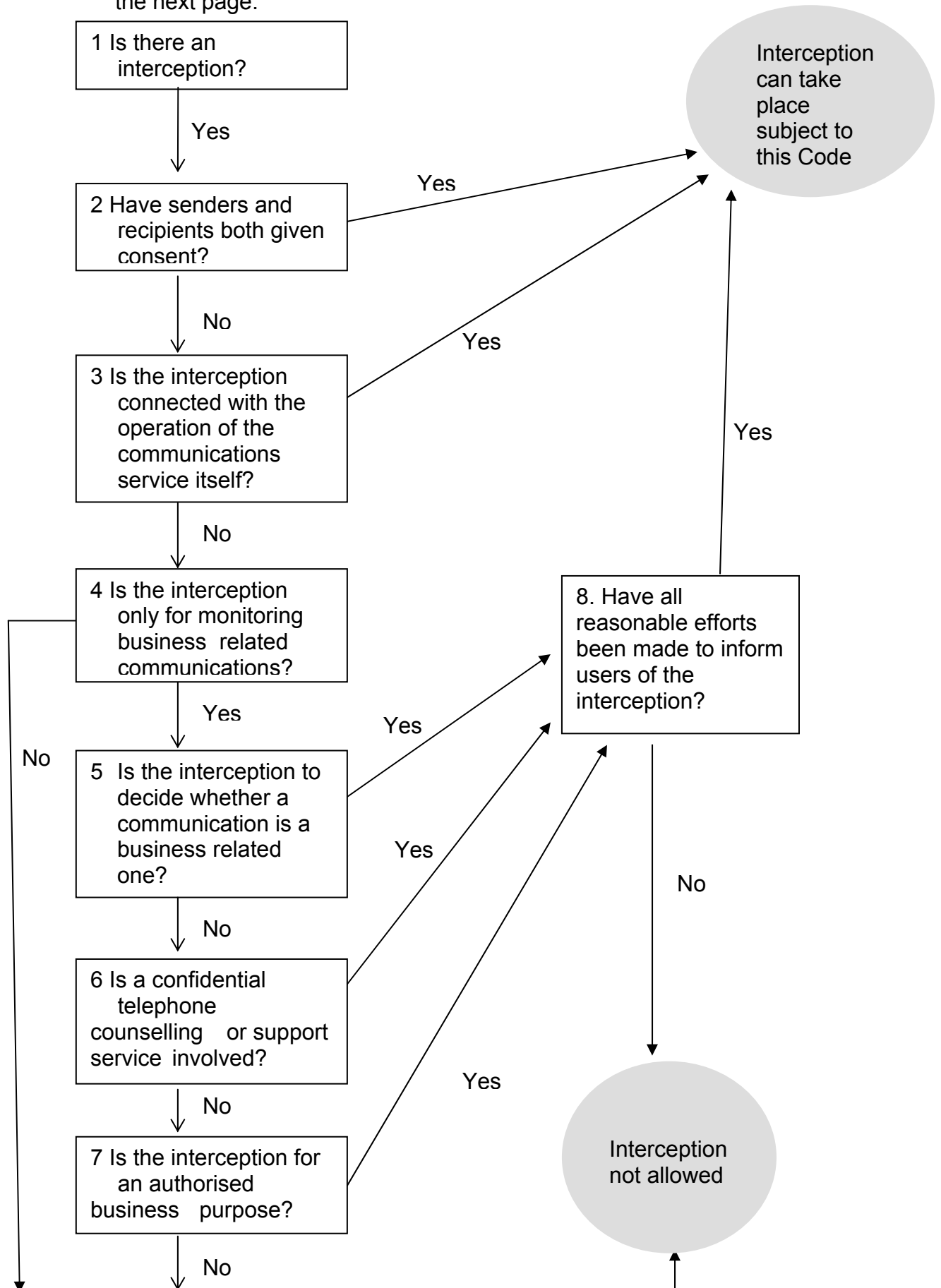
Under RIPA it is against the law for a business to intercept an electronic communication on its, or anyone else's, system. There are some exceptions. Most of the exceptions contained in RIPA itself are unlikely to apply to the monitoring of communications by employers, for example where an interception is authorised under a warrant. The RIPA exceptions that may be relevant are:

- where the interception takes place with consent
- where the interception is connected with the operation of the communications service itself

In addition to the exceptions in RIPA itself, the Lawful Business Practice Regulations set out further exceptions where, in connection with the carrying on of a business, an interception will not contravene RIPA. These exceptions will be particularly relevant to employers. They set out the circumstances in which a business is authorised to carry out an interception for the purpose of running its business. The regulations are designed to meet the legitimate needs of businesses to manage their information systems, making use of the capabilities of modern communications technology, but in a way that is consistent with high standards of privacy. It must be remembered though that they are not exemptions from the Data Protection Act.

An interception of communications that does not come within the exceptions in the LBP Regulations or in RIPA itself is against the law. It is irrelevant whether or not the monitoring associated with the interception would satisfy the other provisions of this Code. On the other hand, if the interception does come within the exceptions, the monitoring cannot proceed regardless. The collection, storage, and use of personal information that is involved in the monitoring must still satisfy Data Protection requirements.

This diagram may assist employers in checking whether the requirements of RIPA and the LBP Regulations are met. Explanatory notes follow on the next page.



EXPLANATORY NOTES

1. Is there an interception?

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 intended recipient. Depending on the nature of the communication the intended recipient may be simply a business or a specific individual. Examples where interception may take place include a supervisor listening in to calls, a business opening e-mails stored on a server before they have been opened by the intended recipient, and an automated system that opens e-mails and/or their attachments to check them for viruses. Examples that do not involve interception include a business accessing a stored collection of e-mails that have been received and opened or deleted by the intended recipient, and a business accessing a stored collection of sent e-mails.

2. Have senders and recipients both given consent?

Interception is allowed if the business has reasonable grounds for believing that both the sender and recipient have consented to the interception. Interception is also allowed in certain other circumstances without the consent of the sender or recipient. However, if a business is to rely on consent in order to legitimise an interception, there must be some action from which consent can be inferred, for example, the caller saying "yes" when asked or proceeding with a telephone call after hearing a message saying that calls are recorded. Consent must be freely given. Businesses might choose to rely on consent to cover the interception of telephone calls or internal e-mails but it is hard to see how consent can readily be obtained from external senders of e-mail.

3. Is the interception connected with the operation of the communications system itself?

Interception without consent is allowed if:

- it is undertaken by or on behalf of a business that provides a telecommunications service, and
- it takes place for purposes connected with the provision or operation of that service.

Providing a telecommunications service means providing access to and facilities for making use of an electronic communications system. Employers will often be providers of a telecommunications service in respect of their own networks. They might rely on this provision where,

for example, incoming e-mails are intercepted by the IT department in order to divert them so as not to block up an e-mail gateway.

4. Is the interception only for monitoring business-related communications?

Interception without consent is not allowed by a business unless the interception is solely for monitoring (or recording) communications which:-

- involve the business entering into transactions, or
- relate in another way to the business, or
- take place in some other way in the course of carrying on the business.

These categories cover most business communications but they do not include personal communications by workers unless they relate to the business. Interception will not be allowed if it is carried out wholly or partly to gain access to the contents of personal communications sent to or by workers that do not relate to the business. This does not prevent interception which is carried out only to gain access to the contents of business communications but which may incidentally and unavoidably involve some access to other communications on the system.

5. Is the interception to decide whether a communication is a business related one?

Interception without consent is allowed if it is to monitor, but not record, communications to check whether they:-

- involve the business entering into transactions
- relate in another way to the business

For example, an employer may open e-mails in an absent worker's in-box if this is necessary to see whether there are business communications that need to be dealt with in the worker's absence. However, the employer should not open e-mails that in their unopened state appear not to relate to the business, e.g. e-mails that are marked 'personal' in the header, unless there are convincing grounds on which to believe they are in fact business related.

6. Is a confidential telephone counselling or support service involved?

Interception without consent is allowed if it is to monitor, but not record, communications to a confidential, free, telephone counselling or support service operated in such a way that users can remain anonymous. This is to enable help-line workers to receive appropriate supervision and support.

7. Is the interception for an authorised business purpose?

Interception without consent is allowed if it is part of monitoring (or recording) business communications for one of the following purposes:-

- To establish the existence of facts (e.g. to collect evidence of transactions such as those involved in telephone banking or to keep records of other communications where the specific facts are important, such as being able to prove that a customer has been given certain advice)
- To check that the business is complying with regulatory or self-regulatory procedures (e.g. to check that workers selling financial services are giving customers the “health warnings” required under financial services regulation)
- To check the standards that workers are achieving (e.g., to check the quality of e-mail responses sent by workers to customer enquiries)
- To show the standards workers ought to achieve (e.g. for staff training)
- To prevent or detect crime (e.g. to check that workers or others are not involved in defrauding the business)
- To investigate or detect unauthorised use of the telecommunications system (e.g., to ensure that workers do not breach the employer’s rules on use of the system for business purposes, for example by sending confidential information by e-mail without using encryption if this is not allowed. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised)
- To ensure the security of the system and its effective operation (e.g., to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

8. Have all reasonable efforts been made to inform users of the interception?

The requirement of the LBP Regulations is to make reasonable efforts to inform users of the system that an interception may take place. Workers, including temporary or contract staff, will be users of the system but outside callers or senders of e-mail will not be. Where, as will usually be the case, interception involves the collection, storage or use of personal information, the requirements of the Data Protection Act to provide information to those whose data are processed will come into play. Information required under both the LBP Regulations and the Data Protection Act overlaps and can of course be provided at the same time.



F. FREQUENTLY ASKED QUESTIONS

1. We own the equipment workers use for communications and they've been told we are going to monitor them. Isn't that enough?

You may well own the equipment, but the rules of data protection still apply to personal information processed on it. Telling workers about the monitoring is important, but telling them about it in general terms is unlikely to be sufficient. Workers should be told about the specific circumstances in which messages they send or receive may be seen by others. Even if workers have been told about monitoring, the other rules of data protection still apply. This means, for example, that the information obtained through monitoring mustn't be irrelevant or excessive. The benefits monitoring brings should be sufficient to justify carrying it out. The Code recommends the use of an impact assessment to check whether monitoring is justified.

2. But what if we completely ban private e-mail use and internet access?

A ban can be an important factor but is not necessarily an over-riding one. A ban on private use doesn't in itself allow the employer to access messages that are clearly private. The intrusion involved in accessing such messages must still be justified by the benefits gained. It might, for example, be possible to identify an e-mail as private from its header and take action against its sender or recipient for breach of the rule without reading the message's content. In any case there might well be genuine business messages, for example ones sent by a worker to his or her occupational health advisor that a worker has legitimate grounds for wishing to keep private.

3. Is it right that we can never open private e-mails in the course of monitoring?

There is no absolute ban on an employer accessing the content of private e-mails, but any such access ought to be carefully considered. Much depends on the reasons for access, any rules the employer might have for private use of the system, what workers have been told about monitoring and what steps are taken to keep the intrusion to a minimum. There is, for example, likely to be little to prevent an employer who suspects a worker of engaging in criminal activity in the workplace and who reasonably believes that this may involve the sending or receipt of e-mails from accessing the contents of his or her messages. The opening of e-mails that are clearly private should not be undertaken lightly though.

It is unlikely that opening private messages merely on the off chance that evidence of wrong-doing will be found will be justified if this involves revealing their contents to an individual other than the sender or intended recipient.

4. The Lawful Business Practice Regulations allow a wide range of monitoring. Don't they override the Data Protection Act?

No. When carrying out monitoring both pieces of legislation must be complied with, one doesn't override the other. The Lawful Business Practice Regulations deal with the interception of electronic communications. Not all monitoring involves interception. Even where it does, the Regulations work in tandem with the Data Protection Act. An interception, if it is not done with the consent of the parties to the communication, must satisfy one of the conditions in the Lawful Business Practice Regulations. In so far as it then involves the recording and use of personal information it must also comply with the Data Protection Act. Although the conditions in the Lawful Business Practice Regulations allow for interception of business related communications in a range of circumstances, monitoring that involves interception and is targeted on the contents of personal communications that are not business related is not permitted.

5. How does the Act affect virus checking?

The Act does not prevent employers monitoring their systems to check for viruses or other forms of malicious code. In fact the Act requires those handling personal information to use technical means to safeguard their systems. Virus checking should though be conducted in the least intrusive way possible consistent with achieving good security. It is preferable, for example, from a privacy viewpoint, for suspect messages to be rejected or quarantined for collection by the intended recipient rather be opened and read by a systems administrator.

6. Does the Code really require us to provide our workers with separate e-mail accounts for private messages?

No, this is a misunderstanding. The Code says that if an employer chooses to provide a separate facility for private messages this will be an important factor in deciding what monitoring of the business related account is justified. If a separate account is provided for private messages this will help limit any intrusion that results from monitoring the business account.

7. We have to prevent sexual and racial harassment of workers. Are we justified in checking e-mail and internet access to do so?

Employers have legal obligations on them that require them to take active steps to prevent racial or sexual harassment in the workplace.

Nevertheless it is hard to see a justification for randomly or routinely accessing the content of e-mail messages, particularly private ones, sent to or from workers or checking which websites they have visited in the course of private internet use on the off-chance that evidence of harassment will be found. Where there are grounds to suspect that a particular worker or workers are using e-mail to harass others or are downloading inappropriate material from the internet then targeting monitoring at those workers' e-mail or internet use may well be justified.

8. We undertake work as a contractor for a bank and they insist we monitor our workers' creditworthiness. If they require us to do this does this mean we can do it regardless of what the Data Protection Act says?

No. As you are monitoring the creditworthiness of your workers you must be satisfied that the intrusion they face is justified by the benefits the monitoring brings to you and the bank. You are obviously entitled to take the bank's circumstances into account in assessing what monitoring is justified, but the assessment should be yours. You are also entitled to take into account the extent to which workers genuinely have a free choice whether or not to subject themselves to the monitoring, i.e. are they able to choose not to work on the bank's contract without suffering any detriment? Incidentally, you must not use a facility provided to you by a credit reference agency for checking your customers to check your workers without the agency's knowledge and agreement.

9. Is it acceptable for us to install hidden video cameras? We told all workers some months ago that we might do this.

Video cameras are particularly intrusive. The notice you have given to workers will not be sufficient unless it is the case that providing more specific information would be likely to prejudice the prevention or detection of crime or equivalent malpractice, for example because the camera has been set up to monitor a worker you suspect of theft. Because video cameras are intrusive workers should generally be aware of exactly where they are located and what they are being used to detect.

10. We collect a lot of information about workers through monitoring e-mails and internet access. What do we have to do when one of them makes a subject access request?

If a worker makes a subject access request he or she is entitled to access to all the information of which he or she is the subject. This will include internet access logs and e-mail records. Remember though that a worker will not be the subject of a message simply because he or she is its sender or recipient. Clearly the more information that is amassed about workers through monitoring, the more onerous employers may find it to respond to subject access requests. Systems that are designed with subject access in mind are though likely to reduce the burden considerably.



G. USEFUL ADDRESSES

1. Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545745 (for information and other parts of the Code)
or 01625 545740 (for notification)

Fax: 01625 524 510

E-mail: mail@dataprotection.gov.uk
(for information and requests for other parts of the Code)
or mail@notification.demon.co.uk

Websites: www.informationcommissioner.gov.uk
(for information and to download other parts of the Code)
or www.dpr.gov.uk (for notification and to view the register)

2. Advisory, Conciliation and Arbitration Service (ACAS)

Brandon House
180 Borough High Street
London
SE1 1LW

Telephone: 020 7396 5100

Website: www.acas.org.uk/contact_us.html (contact details of offices throughout the UK)

3. British Standards Institute (BS7799)

BSI-DISC
389 Chiswick High Road
London
W4 4AL

Telephone: 020 8995 7799

Fax: 020 8996 6411

E-mail: info@bsi-global.com

Website: www.bsi.org.uk

4. Chartered Institute of Personnel and Development

CIPD House
Camp Road
London
SW19 4UX

Telephone: 020 8971 9000

Fax: 020 8263 3333

Website: www.cipd.co.uk

5. Commission for Racial Equality

Elliot House
10-12 Allington Street
London
SW1E 5EH

Telephone: 020 7828 7022

Fax: 020 7630 7605

E-mail: info@cre.gov.uk

Website: www.cre.gov.uk

6. Department of Trade and Industry

Communication and Information Industries Directorate
151 Buckingham Palace Road
London
SW1W 9SS

Telephone: 0207 215 5000

Website: www.dti.gov.uk/cii

7. Confederation of British Industry

Centre Point
103 New Oxford Street
London
WC1A 1DU

Telephone: 0207 395 8247

Website: www.cbi.org.uk

8. Disability Rights Commission

DRC Helpline
Freepost MID 02164
Stratford-upon-Avon
CV37 9BR

Telephone: 08457 622 633

Fax: 08457 778 878

Textphone: 08457 622 644

E-mail: ddahelp@stra.sitel.co.uk

Website: www.drc-gb.org

9. Equal Opportunities Commission

Customer Contact Point

Arndale House

Arndale Centre

Manchester

M4 3EQ

Telephone: 0161 833 9244

Fax: 0161 838 8312

E-mail: info@eoc.org.uk

Website: www.eoc.org.uk

10. Office of the E-envoy

Stockley House

130 Wilton Road

London

SW1V 1LQ

Telephone: 020 727 63208

Fax: 020 727 63292

E-mail: dannison@cabinet-office.x.gsi.gov.uk

Website: www.e-envoy.gov.uk

11. Trades Union Congress

Congress House, Great Russell Street

London

WC1B 3LS

Telephone: 020 7636 4030

Fax: 020 7636 0632

Website: www.tuc.org.uk