

Advice leaflet – Internet and e-mail policies

Introduction

Electronic communications have revolutionised business communications, although the huge increase in use has taken some organisations by surprise. It is commonplace now for people at work to use e-mail as easily as using the telephone, and Internet access is often part of the setup of a workstation. Many people now routinely use e-mail and the Internet for personal communication and interest as well as in the workplace.

The government is committed to promoting workplace learning and development, and intends that everyone in the UK who wants it should have access to the Internet by 2005. Much of this access is in the workplace, and more organisations are going online every day.

Electronic communications offer unique benefits and challenges. There are technical aspects to any electronic system that an organisation may need to consider – this leaflet does not give detail of technical issues and organisations may wish to seek advice on these matters.

Why have a policy?

Clearly formulated policies can help ensure that decisions made within the organisation which affect workers:

- are well thought out, understood by all users, are consistent and fairly applied
- take full account of their effect on all areas of activity
- satisfy legal requirements
- contribute to a productive relationship between the employer, the workforce and their representatives.

Managers who know the objectives and policies of the organisation are more likely to act consistently and fairly. Workers can be more effective when uncertainties about the organisation's intentions and any inconsistencies in management decisions are removed. Involving workers and their representatives in the development, implementation and operation of policies is more likely to make them acceptable and successful.

It is important that organisations understand the potential for making the most of their IT systems. People need to know the opportunities that use of the Internet and e-mail offer.

Setting out rights, responsibilities and limitations on the use of organisational equipment will help the organisation prevent any unauthorised or careless use which might result in itself or its workforce creating a legal risk (see [Legal considerations](#) below). Such a policy should also make transparent any monitoring or interception that might be lawfully undertaken and the reasons for

such monitoring.

By having a written policy the organisation can:

- help protect itself against liability for the actions of its workers (vicarious liability)
- help educate system users about the legal risks that they might inadvertently take
- make clear to users who they should contact about any particular aspect of the policy
- notify users of any privacy expectations in their communications
- prevent damage to systems
- avoid or reduce unnecessary time being spent on non work related activities.

The organisation may wish to get individuals to 'sign off' that they have read and understood the policy perhaps by incorporating it in contracts or terms and conditions of employment. It should be part of the induction process for new workers. This will help prevent any claim that someone has not seen or understood the policy if a problem surfaces.

How should the policy be drawn up?

Consultation with trade union or other worker representatives if a union is not recognised in the organisation, as well as management and contractor representatives will help provide authority and legitimacy. Consultation will also demonstrate the commitment of the organisation and its senior management to producing a workable and sensible framework

The policy should generally cover everyone in the organisation unless there are good reasons for exceptions, for instance levels of access to organisational information.

Advantages of electronic communications

The advantages and benefits of electronic communications will depend on the aims of the organisation and the way the technology is introduced and operated, but common benefits might include:

- speed of communication probably the biggest benefit of e-mail, with the ability to contact a specified group of people at the same time if required. This should generally improve internal and external communications, although it does not follow that a reply will be received as quickly
- revolutionising the possibilities for flexible working, allowing easy contact for home-workers, for tele-workers and for video conferencing
- the opportunities the Internet offers for research, for contacting organisations or people in the same field of interest or trade, for

commercial transactions and the provision of a 'shop-window' for the organisation via a website.

Challenges of electronic communications

However, in introducing electronic communications the organisation should consider possible problems, which may include:

- e-mail is not the informal and transient form of communication that many people think it is, even 'deleting' or 'trashing' a message does not mean it is unrecoverable
- intensive use of e-mail, and unnecessarily wide broadcasting, can lead to 'information overload' and stress as workers try to keep up with the number of e-mails received
- the ease and speed of e-mail can lead to inadequate thought going into a message, and the possibility of the words or tone being misinterpreted by the recipient
- sites visited via the Internet are traceable
- there are a number of laws that cover electronic communications and employer monitoring of e-mails and Internet use by workers (see [Legal considerations](#) below).
- it is essential that any organisation using these technologies, or thinking of installing them, considers the impact they might have, the position of workers and the legal liabilities that may be incurred
- having a proper policy in place will help everyone understand the boundaries that may be imposed.


E-mail

As well as the many benefits of e-mail, it is essential that all workers in an organisation realise the following potential pitfalls:

- it is not an informal communication tool, but has the same authority as any other communication to and from the organisation
- external e-mails should have disclaimers attached
- it should be regarded as published information
- e-mails are not confidential, and can be read by anyone given sufficient levels of expertise
- binding contracts may be inadvertently created
- defamation of colleagues or other parties (deliberate or otherwise) may occur

- abrupt, inappropriate and unthinking use of language can lead to a bullying tone and possible offence to others even harassment for example, capitals are often interpreted as shouting
- consider whether a phone call may be a better way of discussing a complex or confidential matter.

The organisation may allow full personal use of the e-mail facility, or limited use, or prohibit any personal use (although the Human Rights Act 1998 suggests that employers should provide some private communication system for workers see [Legal considerations](#) below). If personal use is allowed staff should be made aware of the possibility of importing viruses into the system, and what action to take if, for instance, an e-mail has a suspect attachment, or they are sent a 'chain' letter. The organisation should have a nominated person, usually in computer support or personnel/human resources, who can advise on security issues. Small firms, who may outsource their computer support, will probably be able to include security issues within their maintenance contracts.

Breaches of the policy would then be dealt with as any other breach of the rules perhaps leading to disciplinary action as set out in the organisation's discipline and grievance procedures (see Acas [Advisory handbook - Discipline and grievances at work \(section 1 of 2\)](#), which includes the  [Code of Practice - Disciplinary and grievance procedures \[327kb\]](#) and gives examples of disciplinary and grievance policies).

Internet

The Internet is a valuable business tool for research and for comparing products, supply and prices. Some organisations allow reasonable personal use of the web, perhaps outside working hours, some allow no personal use at all. If personal use is granted, the organisation has to be aware of some of the issues that may arise, and a policy for use should be drawn up and communicated to everyone. Factors to consider include:

- connection costs can be high, with resulting high telephone bills
- viruses can be imported into the organisation's system
- inappropriate sites may be visited ('hard' or 'soft' pornographic, racist, sexist etc)
- people may spend too long on personal surfing during working time
- whilst there are no national or cultural boundary restrictions there are legal boundaries (see [Legal considerations](#) below).

Developing a policy

All organisations are different, and it is vital that all its policies are relevant to its needs. Whilst model policies are a useful basis from which to work, they must be tailored to the organisation, its business, and its workers.

A written policy, known to all the workforce, establishes the boundaries and uses that may be made of organisational equipment. Policy development may be achieved by use of a working party, with representatives of IT, personnel/human resources, worker representatives and any other directly interested parties such

as security advisers.

Most policies will seek to establish a balance between business and personal use, whilst encouraging staff to develop effective computer skills. In most organisations workers respond well to trust, and follow agreed policy guidelines in a responsible manner. The organisation may choose not to be too restrictive so as to prevent damage to existing employment relations.

Organisations should cross-reference any computer use policy with other relevant policies, for instance, the handling of confidential information, use and storage of personal data, consultation and communications at work, training, equal opportunities and harassment, and discipline and grievances at work.

Policy content

Some organisations will need to have a detailed policy, others maybe less so, but there will be features in common:

- how much personal use can be made, if any
- confidentiality issues, 'trade secrets', access to organisational information
- when to attach disclaimers to e-mails
- good housekeeping practices, including locking keyboards and password security
- use of language and appropriate etiquette (no capitalisation of text, correct forms of address and signing off)
- prohibition of inappropriate messages, for instance any that might cause offence or harassment on grounds of age, sex, race, disability, age, religion
- prohibition of deliberate accessing of offensive, obscene or indecent material from the Internet, such as pornography, racist or sexist material, violent images, incitement to criminal behaviour etc
- being aware of copyright and licensing restrictions that might apply to downloaded and forwarded material, whether Internet or e-mail, and including unauthorized software, games, magazine disc items etc. The importation of viruses is often through downloading files and programmes from external sources
- what monitoring, if any, will be carried out by the organisation
- what might happen if a breach of the policy occurs.

Guidelines and 'frequently asked questions' may also be used within the policy.

The main objective will normally be that any personal use does not interfere with individual work responsibilities and that workers understand that any personal use does not guarantee privacy of correspondence. This latter is particularly important if the organisation needs to have access to individual business-related

e-mails when that person is away from work. Private and confidential communications should generally be by phone or letter.

Management issues

Once a policy is in place it must be communicated to everyone. Communication methods may include:

- via e-mail, although that does not guarantee that the recipients will open it!
- a follow-up circular, or incorporation into a staff handbook (hardcopy or intranet) is sensible, and some organisations may wish to consider including any such policies into individual contracts
- a presentation to staff to explain the system and its use might be appropriate in smaller organisations, discrete departments or teams
- training in effective use should be available to all.

However communication of the policy is achieved it is vital that people understand the possibility of monitoring and lack of personal privacy this may entail (see [Legal considerations](#) below).

External recipients of e-mails should also know that monitoring is taking place or may take place. Ordinary written mail can give this information within the letter it is less obvious with e-mail, but a standard footnote, that can be added automatically to external e-mails, indicating that the organisation may monitor communications for business purposes could be considered. Such a footnote may also contain a disclaimer and statement that the communication is for the intended recipient only.

Any breaches of the agreed policy should be addressed through the organisation's disciplinary and grievance procedures. Managers must be trained to deal with breaches and other problems that might arise in e-mail and Internet use.

Responsibility for the policy

Generally speaking in larger organisations personnel/human resources staff are likely to be responsible for the overall operation of the policy, making amendments as necessary, and dealing with breaches. However, IT departments are more likely to be responsible for the security of the communications system and reporting possible breaches and problems. Some smaller organisations may contract out their IT work, including security responsibility.

Training is generally likely to be a management responsibility, with IT departments or contractors giving specific technical training as required. The policy should make clear who in the organisation is responsible for the implementation of training.

The field of electronic communications and the relevant legislation changes rapidly policies should be reviewed regularly and revised/reissued as necessary.

Monitoring of electronic communications

The decision whether to monitor systems and information should be part of the initial development of the policy. All organisations are likely to install anti-virus software to protect their systems, but there are many other forms of software available which can be used for automatic blocking and monitoring of flow and content of communications such as:

blocking access to certain Internet sites, particularly those that might contain offensive sexual, racist or violent images

- monitoring of e-mails, by content, size of attachments or graphic/animation files
- monitoring large scale circulation of e-mails which might make the system less effective and run less smoothly.

However, any monitoring of e-mail message content must be considered carefully, as it is intrusive and may be interpreted as a lack of trust in staff, and there must be in place proper procedures for monitoring and the maintenance of confidentiality by those carrying out any such monitoring. There are also serious legal considerations as given briefly in the Legal section below. Monitoring should be proportional to the legitimate business needs of the organisation.

Legal considerations

This section gives brief information of some of the laws that might be applicable to computer use in the workplace. Further legal advice should be sought if appropriate.

Some law covers the content of e-mail, or sites downloaded from the Internet; other legislation concerns privacy issues, monitoring of communications and surveillance at work. Some cover several aspects of employment relations.

Human Rights Act 1998

This provides for the concept of privacy giving a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act. *Halford v UK* 1997 suggests that employees have a reasonable expectation of privacy in the workplace, and employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring, for instance a staff telephone line or a system of sending private e-mails which will not be monitored.

Covert monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (see below). Employers should make sure workers know of any monitoring or recording of correspondence (which includes e-mails, use of Internet, telephone calls, faxes and so on).

Regulation of Investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of

communications.

There are two areas where monitoring is not unlawful. These are:

- where the employer reasonably believes that the sender and intended recipient have consented to the interception
- without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000. These include:
 - to ensure compliance with regulatory practices eg Financial Services Authority requirements
 - to ensure standards of service are maintained, eg in call centres
 - to prevent or detect crime
 - to protect the communications system this includes unauthorised use and potential viruses
 - to determine the relevance of the communication to the employer's business ie picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

Data Protection Act 1998

The Information Commissioner - responsible for enforcement of the Data Protection Act - has published a code of practice to help employers comply with the provisions of the data Protection Act. The Employment Practices Code clarifies the Act in relation to processing of individual data, and the basis for monitoring and retention of email communications.

Part 1 of the code covers recruitment and selection, Part 11 - deals with employment records, and Part 111 looks at monitoring at work, and Part IV deals with medical information. All are available from the Commissioner at www.dataprotection.gov.uk.

The code of practice *Monitoring at work: an employer's guide* states that any monitoring of emails should only be undertaken where:

- the advantage to the business outweighs the intrusion into the workers' affairs
- employers carry out an impact assessment of the risk they are trying to avert
- workers are told they are being monitored

- information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- the information discovered is kept secure
- employers are careful when monitoring personal communications such as emails which are clearly personal
- employers only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

Protection from Harassment Act 1997, Defamation Act 1996, Discrimination law (age, sex, race, disability, sexual orientation and religion or belief)

These laws all protect individuals from suffering abuse, harassment, defamation or discrimination at the hands of others. E-mail communications and the downloading of inappropriate images from the Internet may contain language or graphics that are insulting, demeaning or unlawful. Whilst the perpetrator of the message or download may be legally liable for damage caused, the employer may also have vicarious liability for the actions of their workers.

Contract law

It is just as possible to make a legally binding contract via e-mail as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer, or varying the terms of any existing contract.

Copyright law

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over software, which should not be downloaded without license.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

Computer Misuse Act 1990

This Act is mainly concerned with the problems of 'hacking' into computer systems.

Further information

Employee Privacy in the Workplace IDS Employment Law Supplement

Internet and e-mail policies IDS Study 682

Internet and e-mail use and abuse Clare Hogg CIPD London 2000

Managing e-mail and internet use Lynda Macdonald, Tolley's London 2001

Last printed version: May 2006

Last updated web version: September 2006