



Internet and email policies

This factsheet gives introductory guidance. It provides basic information on acceptable use policies for using email the Internet, blogging and social networking at work.

Why have policies?

In many organisations, access to the Internet was initially limited to a few people in the IT or marketing groups. Today, with a PC on every desk, many employees find themselves with access to the Internet and email but with little understanding of either the potential problems or the real benefits which this can bring.

The purpose of implementing an acceptable use policy is to ensure that employees understand the way in which these technologies should be used in the workplace. This enables both employees and the organisation to gain the maximum value from email and the Internet, alerts them to the dangers that can arise to the organisation if the technology is misused (which may put the organisation at technical or commercial risk) and informs everyone of the consequences of misuse by employees (that is, disciplinary action). The content of such policies will, therefore, depend on the needs of the organisation and the expectations and requirements of its personnel. Before producing an acceptable use policy, an organisation must have developed an agreed strategy for using the Internet.

Data Protection Act 1998

A policy which outlines employers' responsibilities when monitoring employees' use of the Internet and email is also necessary to ensure organisations comply with the Data Protection Act 1998 (DPA). The Information Commissioner is responsible for overseeing compliance and has produced the employment practices code which includes guidance on an employer's rights to monitor staff.

The Code recommends that employers carry out an impact assessment to help them establish whether their Internet and email monitoring complies with the DPA. Such an assessment should identify:

The purpose of monitoring, the benefits it is likely to deliver, any likely adverse impact.

The assessment should also consider alternatives to monitoring or less intrusive ways it could be carried out.

Once the risk assessment has been completed it is important to draw up policies that spell out to staff the organisation's approach to monitoring in the workplace. Policies must state what is prohibited and any unauthorised access areas such as pornographic web sites, as well as highlight possible disciplinary consequences for breach of rules. The Code protects staff from covert monitoring except in exceptional circumstances, such as where there are grounds for suspecting criminal or equivalent malpractice.

Network security

The degree of network security which will be imposed should be determined as part of an organisation's electronic information strategy.

Technical security features such as firewalls, can be included, at a cost, on the local network. The introduction of viruses when downloading software or other files from the Internet poses a risk to the entire network. Anti-virus software provides an element of protection but downloading also needs to be strictly controlled through the Internet policy. These measures are generally managed by the IT department.

At individual user level, security is generally provided by using passwords. Your policy should state clearly any rules which you have for the format of passwords, changing passwords and for not disclosing them.

Browsing the web

The policy must state who will be allowed access to the Internet and whether this will be for business use only or for private use as well. A problem with browsing, even for business use, is that it can become unfocused and time-consuming. This wastes employees' time and, even where it is done in their own time, it ties up resources and may be costly in telephone charges (although the use of dial-up lines is now uncommon, especially in larger organisations). Occasionally, the IT department may undertake some monitoring to find out which websites are being accessed regularly and by whom. If monitoring is taking place, this should be stated in the policy together with the action which will be taken against anyone misusing the Internet.

Downloading information

Obtaining inappropriate text and images

Although it is possible for the system manager to bar access to certain sites, the Internet is growing so rapidly that it is impossible to prevent all inappropriate access automatically. Therefore, the policy has to state unequivocally that downloading offensive, obscene or indecent material is forbidden. In a CIPD survey, 70% of companies had taken disciplinary action as a result of employees viewing pornographic images.

Breaking copyright laws

Much of what appears on the web is, or claims to be, protected by copyright. The Copyright, Designs and Patents Act 1988 states that only the owner of the copyright is allowed to copy the information. Any copying without permission, including electronic copying, is prohibited. Many company libraries, for example, enforce rigorous policies on photocopying and a similar policy must be applied to copying from the Internet. The copyright laws apply not only to documents but also to software. The Federation Against Software Theft (FAST) is making rigorous efforts to counteract the use of illegally copied software.

Introduction of viruses

The greatest risk from viruses lies in downloaded programs and executable files. Spreading of viruses is also subject to prosecution under The Computer Misuse Act 1990. As a rule, all software for use in an organisation should be obtained from controlled legal sources by the system manager. Restrictions on the downloading of software should be clearly stated in the policy.

Obtaining incorrect or poor quality information

One of the main benefits of the Internet is the access which it gives to large amounts of information which is often more up-to-date than in traditional sources like libraries. Unfortunately, as the Internet is uncontrolled, some of this information is less accurate than it may appear. The policy must warn about the risks of obtaining and using such unregulated information.

Time wasting

As with browsing, downloading information from the Internet can be very time-consuming and wasteful of resources. The policy must make clear what is acceptable in terms of time spent downloading material.

Keeping a blog

Online diaries, known as blogs, have become increasingly popular as sources of information. The diaries are personal accounts, but there have been some recent cases where employees have been dismissed for discussing their organisation online. Therefore employers may need to specify in their Internet and email policy that blogging is unacceptable use.

Using email

Although email communication has the same speed and apparent informality as using the telephone, it also has the permanence of written communications and, as such, must be controlled to ensure that it meets the same standards as other published documents.

What are the advantages of using email?

It is a fast and inexpensive way of delivering messages and documents across long or short distances.

Information can be shared quickly and consistently between any number of people.

It removes the need to print and distribute information by conventional means.

What are the disadvantages of using email?

If it is used inappropriately, you and your colleagues may suffer from 'information overload syndrome' i.e. vital information being lost in many messages that are irrelevant.

It can stifle face-to-face communication or be used to abdicate the responsibility of communicating messages that should be done in person.

Access

The policy should state who is allowed access and how they can get it. In most organisations, it would be difficult to justify denying any particular groups access to this valuable communication tool.

Use

The policy should state whether email is to be used for business purposes only or is permitted for personal communication also. This largely depends on the organisation's culture and the controls which are already imposed. If (either implicitly or explicitly) the telephone may be used for personal communications, then it could be difficult to forbid a similar use of email, although there are clearly greater security implications in the widespread use of email.

Content

The policy should state that sending offensive email will not be tolerated. It is inappropriate, however, for the policy to list unsuitable material in detail since this may imply that anything not listed was acceptable. The sender of a message which causes offence must be subject to normal disciplinary procedures, but in this respect email is no different from any other interpersonal dispute (and has the advantage that, unlike purely verbal communications, it is possible to supply evidence to support a complaint).

Policies should take account of the DPA, which provides guidance on employers' rights when accessing staff email.

The Code allows organisations to check staff email accounts in their absence if they have been informed that this will happen.

However employees' privacy will be respected if they clearly mark that an email is personal, unless their employer has a valid and defined reason to examine the content.

Employees need to be made aware by the policy that the same laws apply to email as to any other written document and that therefore they should avoid making any inaccurate or defamatory statements.

For external email it is possible to include a disclaimer but the policy should still emphasise the need to act responsibly when writing email, and to seek advice before sending a message if there is any doubt about its contents.

Distribution

In spite of the benefits of email, there is a danger of loss of productivity associated with its excessive use. The policy should make clear the importance of only sending relevant emails and avoiding the automatic forwarding of all messages to long circulation lists which unnecessarily increases the traffic and the time spent dealing with irrelevant correspondence. The policy should also set out a procedure to cover wrong delivery. For example, it should state that a wrongly delivered message should be redirected to the correct person and that if the email message contains confidential information, use must not be made of that information and nor must it be disclosed.

Addresses

The Internet policy should make it clear who may or may not be given details of any particular email address.

Monitoring

Depending on an organisation's culture and the nature of its business, it may choose to monitor emails (either manually or automatically). If this is the case, the policy should state that email may be intercepted and read. Covert monitoring is only permitted in exceptional circumstances such as where there are grounds for suspecting criminal malpractice.

Housekeeping

Many organisations contain a section in their email policy on deleting or archiving information i.e. how people should store all the data they download. This must be based on the data protection principles that the information recorded is adequate, relevant, not excessive and not kept for longer than necessary. An assessment will help employers decide what their policy on deleting or archiving information should include. This will become increasingly essential due to the provisions of the Freedom of Information Act.

Internet policies

Internet policies need to address the following activities:

Looking for information on the Internet - 'browsing the web' or 'surfing' downloading information from the Internet communicating via email, both internally and externally working on the organisation's website.

These policies should form part of the standard organisation policies and procedures document or handbook. They should be introduced and explained during the employee induction programme. Where necessary, the policies should be reinforced during specialist training sessions.

The policies should give details of the penalties for breaching the rules for Internet use. Since the issues covered by the policies range from inconsiderate right through to illegal activities, the sanctions would similarly be expected to range from a verbal warning through to instant dismissal.

Internet policies contents checklist

access	who is entitled to access the web how to get access to the web who is entitled to use email how to get access to email
Passwords	rules for choosing a password rules for changing a password warning on disclosing passwords other organisations' websites
the web	prohibition on access to certain websites limitations on browsing the web for non-nusiness purposes your own organisation's website rules for adding information to your website guidelines for responding to website enquiries
downloading	prohibition on downloading offensive materials information on the implications of copyright laws guidance on the use of unchecked information
email	rules on disclosing email addresses limitations on private use of email the legal position regarding defamation and inappropriate advice restrictions on content of email rules for email distribution
monitoring	notifications that websites access may be monitored notification that email may be intercepted and read
disclaimers	wording to use in disclaimer documents which require disclaimers

Employers' liability

Employers are responsible for their employees' activities when using the Internet. For example, if software for use in an organisation is obtained illegally, the employer is liable even if it was obtained without his or her knowledge or permission. Similarly, information on a company's website or in its email can give rise to legal action against the company. Employers are responsible if employees send email messages which are defamatory or which breach confidentiality or contract. Any such messages will be disclosable for the purposes of legal action. In the case of *Western Provident Association v Norwich Union*³, it was shown that untrue and damaging statements about alleged financial problems at Western Provident were circulating on Norwich Union's internal email. This resulted in Norwich Union having to pay £450,000 in damages and costs.

In order to reduce liability, employers must be able to prove that they have a policy in place to prevent illegal actions and that appropriate steps are taken to enforce this policy.

Social networking

Social networks such as MySpace and Facebook are becoming increasingly popular as a means for people to stay in touch with friends and make new ones online. Research commissioned by content security specialist Clearswift in 2007 found more than a quarter of British office workers aged 18-29 were spending three or more hours a week at work on social networking sites. It is not just time lost which is of potential concern to employers, it is also the content which is posted. More than 40% of young workers surveyed by Clearswift had discussed work-related issues on social networking sites. An Argos employee was sacked in 2007 for gross misconduct following a disciplinary hearing after he posted a derogatory comment about his employer on Facebook.

However, corporate social networking can also be a useful way for employers to communicate and engage their employees. Some businesses are starting to use social networking forums to bring staff together from different locations disciplinary procedures the sanctions which will be imposed for breaching this policy or to introduce energy and 'buzz' into internal communications.

Employers should decide what approach they want to take to managing the use of social networks and ensure they are covered in their Internet and email policies. These should set out whether there are any limits on use, whether access to social networks is allowed at lunchtimes or whether there is a total ban. Policies should also state whether the use of such sites is monitored and the penalties for unauthorised access.

If access to social networking sites is allowed, the policy should make it very clear that defamatory statements about the organisation will be treated as a disciplinary offence and emphasise that confidential matters should not be discussed in such forums.

If employers set up corporate social networks, it should be made clear that there is a clear distinction between corporate social networking which is useful to the business and social networking for personal use.

Policies on corporate social networks should also cover issues about confidential information and defamation.

Contact the Business Crime Reduction Centre
on 0114 275 1283 or visit our website at www.bcrc-uk.org

Business Crime Reduction Centre, working with South Yorkshire Police to reduce crime against business

Business Crime Reduction Centre
4th Floor, Castle Market Buildings, Sheffield S1 2AH
Tel: 0114 275 1283 Email: info@bcrc-uk.org