

In order to protect the firm, its employees, customers and suppliers, all members of staff should be given a copy of the firm's policy regarding acceptable use of IT resources – particularly internet, email access, and data protection policies. This should form part of the contract of employment – to the extent that any breaches of the policy could result in disciplinary action, and in some cases dismissal.

Having an acceptable use policy not only helps protect the organisations exposure to rogue software, but can also help in disputes with employees.

Email

A number of companies have been sued for defamation after employees have electronically questioned the integrity of a competitor using email, and published these opinions externally.

In another example of a hearing at an industrial tribunal, an employee of a credit card company had his claim for unfair dismissal rejected. The reason for his dismissal was for using the firms' email system to send personal emails whilst at work. As the credit card company had an effective email and internet policy in place, they were able to defend the claim of unfair dismissal.

Illegal material

Due to the uncensored nature of the material on the internet, there are a large number of web sites which contain offensive, obscene and illegal (in the UK) material. Employees should not access such sites.

Viruses and phishing

Innocent looking web sites and emails have been used to tempt users to download material which has been found to contain a virus, or to disclose personal data they would not normally relay.

A Model Policy Statement

To minimise these kinds of potential problems, all employers should consider setting out a policy statement for all employees embracing internet and email access.

A suggested policy statement is shown below which you may find useful as a starting point.

Policy and scope

The company/firm (delete as appropriate) sees the internet and the use of email as an important business tool.

Staff are encouraged to enhance their productivity by using such tools – but only according to guidelines on their use as set out in this document.

The internet is largely unregulated and uncensored and we have a duty of care to protect the security of the company's/firm's internal information, our customers, our suppliers and our employees from malevolent, obscene and illegal material.

[Monitoring - Optional paragraphs 1

With this in mind, the company/firm reserves the right to monitor emails and internet sites visited, on an employee basis. However, this will only be performed where there is a suspicion of behaviour which breaches the company's 'email and internet access' policy.

Staff under surveillance will be informed, by management, that they are being monitored.

Covert monitoring will only be performed in exceptional circumstances and only when sanctioned by a senior officer(s) of the company/firm.]

[Monitoring - Optional paragraphs 2

With this in mind, the company/firm reserves the right to monitor email and internet traffic. However, individual users will not be identified in the monitoring process.]

It will be assumed that all staff understand and agree to the policies unless a director (partner) is notified otherwise. Any exceptions are to be appended to the employee's contract of employment and signed by a director (partner) and the employee.

All the company's/firm's resources, including computers, access to the internet and email are provided solely for business purposes.

The purpose of this policy is to ensure that you understand to what extent you may use the computer(s) owned by the company/firm for private use and the way in which access to the internet should be used within the company/firm, to comply with legal and business requirements.

This policy applies to all employees of the company/firm and failure to comply may lead to disciplinary action in line with the Disciplinary Procedure. In addition, if your conduct is unlawful or illegal you may be personally liable.

General principles

A computer and internet access is provided to you to support the company's/firm's activities.

Private use of computers and the internet is permitted, subject to the restrictions contained in this policy. Any private use is expected to be in the employee's own time and is not to interfere with the person's job responsibilities. Private use must not disrupt our IT systems or harm the company's/firm's reputation.

You should exercise caution in any use of the internet and should never rely on information received or downloaded without appropriate confirmation of the source.

Access to the internet and email

All/The following users have access to the internet and email from all/the following PCs.

Personal use

The internet may not be accessed for personal use during normal hours of employment. Occasional use for personal reasons is allowed outside working hours, however, the restrictions set out in 'Browsing/Downloading material' (below) must be adhered to.

Personal emails may not be sent/received unless in an emergency or with prior authority.

Emails and email attachments

- emails must conform to the same rules as issuing correspondence on the company's/firm's headed paper
- emails must not contain controversial statements/opinions about organisations or individuals. In particular, racial or sexual references, disparaging or potentially libellous/defamatory remarks or anything that might be construed as harassment should be avoided
- emails must not contain offensive material
- emails containing a virus must not knowingly be sent
- emails coming from an unknown source must not be opened but disclosed to management (see Disclosure)
- emails sent externally, must contain the company's/firm's disclaimer (see sample below)
- emails (sent and received) must be stored in the appropriate client files and use the same naming conventions which are used to store letters and other correspondence

Browsing/Downloading material

- only material from bona fide business, commercial or governmental websites should be browsed/downloaded
- no other material should be browsed/downloaded. This specifically includes games, screensavers, music/video and illegal, obscene or offensive material.

Laptops/portables and portable media devices

- Travelling with laptops/portables
Laptops are liable to be inspected by authorities particularly if travelling by air/sea/rail, both within and outside the UK. Where an employee has a company's/firm's laptop they must ensure that it does not knowingly contain illegal material.
Laptops containing corporate data should be encrypted, but see note below.
- Using laptops/portables on remote connections
Company's/firm's laptops may be used for email/internet use without being connected to the corporate server. Appropriate security software to allow such access and to control viruses, should be installed.
- Using portable media devices
Portable media devices include USB memory sticks, USB pens, CD's, DVD's etc.

Where these contain confidential corporate or personal data, the data contained on these devices should be encrypted, but see note below.

Note:

Advice should be sought if the laptop has solid-state drive as opposed to a conventional 'spinning' hard-disk drive, as solid-state drives have limited life-span. Whilst SSDs have no moving parts to fail mechanically, each block of a flash-based SSD can only be erased/written a limited number of times – currently up to approximately 1.25 million times – before it fails, and encryption will dramatically increase the number of writes.

Disclosure

Employees have a duty to report the following to management:

- suspect emails/email attachments/websites
- obscene/illegal material found on a PC
- persistent use of the internet for personal reasons
- persistent downloading of illegal/obscene/offensive material
- loss of corporate data or loss of machines/devices containing corporate data.

Disciplinary

A breach of any of the policies is a disciplinary matter.

Illegal activities will also be reported to the relevant authorities.

Inappropriate use

Computers are a valuable resource to our business but if used inappropriately may result in severe consequences to both you and the company/firm. The company/firm is particularly at risk when you have access to the internet. The nature of the internet makes it impossible to define all inappropriate use.

However you are expected to ensure that your use of computers and the internet meets the general requirements of professionalism.

Specifically, during any use of the computer or internet you must not:

- copy, upload, download or otherwise transmit commercial software or any copyrighted materials belonging to the company/firm or other third parties
- use any software that has not been explicitly approved for use by the company/firm
- copy or download any software or electronic files without using virus protection measures approved by the company/firm
- visit internet sites or download any files that contain indecent, obscene, pornographic, hateful or other objectionable materials
- make or post indecent, obscene, pornographic, hateful or otherwise objectionable remarks, proposals or materials on the internet
- reveal or publicise confidential or proprietary information (including personal data) about the company/firm, including its employees, clients and business contacts.

The following activities are expressly forbidden:

- the deliberate introduction of any form of computer virus
- seeking to gain access via the internet to restricted areas of the company's/firm's computer system or another organisation's or person's computer systems or data without authorisation or other hacking activities
- downloading corporate information onto portable media devices (such as USB pen or CD) unless management has expressly approved this activity
- uploading personal/private information (for example music, films or photographs) from portable media devices (such as USB pen or CD) onto a local or network drive, unless management has expressly approved this activity.

Monitoring

At any time and without notice, we maintain the right and ability to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the company/firm. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.

In order to ensure compliance with this policy, the company/firm may employ monitoring software to check on the use of the internet and block access to specific websites to ensure that there are no serious breaches of the policy. We specifically reserve the right for authorised personnel to access, retrieve, read and delete any information that is created by, received or sent as a result of using the internet, to assure compliance with all our policies. Such monitoring will be used for legitimate purposes only.

Sample Disclaimer

This email and all attachments it may contain are confidential and intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of [the company/firm]. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, printing, forwarding or copying of this email is strictly prohibited.

Please contact the sender if you have received this email in error.

Companies Act 2006 emails and websites

Changes to Company law mean that, every company must now include their company registration number, place of registration and registered office address on corporate forms and documentation (this includes emails and websites).

In particular, all external emails must include this information – whether as part of the corporate signature or as part of the corporate header/footer.

How abacus can help

We will be more than happy to provide you with assistance in formulating an acceptable use policy, or if any additional information is required.

This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.