



ICT

Internet and E mail Access - an acceptable use policy statement for employees

At a recent 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' e mail system to send personal e mails whilst at work. As the credit card company had an effective e mail and internet policy in place they were able to defend the claim of unfair dismissal.

HMRC have also recently amended the legislation regarding use of computers and potential income tax benefits in kind. There are therefore several legal issues to consider.

E mail

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

Illegal material

Due to the lack of web policing, there are a large number of web sites which contain offensive, obscene and illegal (in the UK) material.

Viruses

Innocent looking web sites and e mails have been used to tempt internet users to download material which has been found to contain a virus.

To minimise potential problems, all employers should consider setting out a policy statement for all employees embracing internet and e mail access.

A suggested policy statement is shown below which you may find useful.

HMRC

An employer who allows an employee unrestricted private use of the employer's computer should report a benefit-in-kind on the employee's form P11D. This will result in an additional tax charge for the employee and extra employers' National Insurance (NI) contributions. The liabilities may not come to light until HMRC conduct a PAYE and NI compliance visit. However by properly managing the type of private use allowed, it is possible to remove this risk.

A suggested policy statement is shown below which you may find useful.

A Model Policy Statement

Policy and scope

The company (firm) (delete as appropriate) sees the internet and the use of e mail 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 firm's/company's internal information, our customers, our suppliers and our employees from malevolent, obscene and illegal material.

[Monitoring - Optional paragraph 1

With this in mind, the company (firm) reserves the right to monitor e mails 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 'e mail 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.]

[Monitoring - Optional paragraph 2

With this in mind, the company (firm) reserves the right to monitor e mail 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 copy of this statement, and signed by a director (partner) and employee.

All the company/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 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/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/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 e mail

All/The following users have access to the internet and e mail 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 e mails may not be sent/received unless in an emergency or with prior authority.

E mails and e mail attachments

E mails must conform to the same rules as issuing correspondence on the firm's/ company's headed paper.

E mails must be authorised by either a director (partner) (or manager).

E mails 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.

E mails must not contain offensive material.

E mails containing a virus must not knowingly be sent.

E mails coming from an unknown source must not be opened but disclosed to management (see Disclosure).

E mails sent externally, must contain the company's/(firm's) disclaimer (see sample below)

Browsing/Downloading material

Only material from bona fide business, commercial or governmental web sites 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

a 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/(firm's) laptop they must ensure that it does not knowingly contain illegal material.

b Using laptops/portables

Company/(firm's) laptops may be used for e mail/internet use without being connected to the corporate server. The software to allow such access and to control viruses, should be installed only by a member of the IT department.

Disclosure

Employees have a duty to report the following to management:

- suspect e mails/e mail attachments
- suspect web sites
- obscene/illegal material found on a PC
- persistent use of the internet for personal reasons
- persistent downloading of illegal/obscene/offensive material.

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 about the company/firm, our employees, clients and business contacts.

Continued >>>

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/firm's computer system or another organisation's or person's computer systems or data without authorisation or other hacking activities.

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 e mail and all attachments it may contain is 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]. If you are not the intended recipient, be advised that you have received this e mail in error and that any use, dissemination, printing, forwarding or copying of this e mail is strictly prohibited.

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

Companies Act 2006 Emails and web sites

Changes to Company law mean that as from 01/01/2007, every firm must now include their company registration number, place of registration and registered office address on corporate forms and documentation (this includes e mails and websites).

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

How We Can Help

We will be more than happy to provide you with assistance or any additional information required.

For information of users: 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.