

INTERNET AND E MAIL ACCESS - AN ACCEPTABLE USE POLICY STATEMENT FOR EMPLOYEES

At a recent industrial tribunal, an IT manager had her claim for unfair dismissal rejected. Her crime? Accessing the internet for personal use whilst at work.

There are 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.

A MODEL POLICY STATEMENT

The company (firm) (delete as appropriate) sees the internet and the use of e mail as an increasingly 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.]

[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.

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 (see below re. restrictions on the type of material viewed or downloaded).

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)

Downloading material

Only material from bona fide business, commercial or governmental web sites should be downloaded.

No other material should be downloaded - particularly screensavers, games and illegal/obscene 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. Installing software to allow such access should be cleared with a member of the IT department.

Disclosure

Users 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 material.

Disciplinary

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

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.

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.