



Email and Internet Usage Policies

July 2007

Email and Internet access are now vital employee tools in many businesses - but inappropriate usage can cause problems for your firm, or offence to other staff members.

Our E-Business Advisers discuss how you can gain the benefits and avoid the pitfalls of staff usage of these systems:

1. Why have an email and Internet usage policy?

Allowing your employees to use email and the Internet can give excellent productivity benefits - but it is not risk-free.

For example, your staff may not realise that it is possible to create a legally binding email contract, which can cause problems for your business.

They may browse inappropriate web sites with pornographic, racist or otherwise undesirable content. This can cause offence to other employees.

If you put a usage policy in place, clearly stating what is and is not acceptable, this gives you a better chance of defending any action taken against the business if the policy is breached.

It also means that you can discipline staff members who behave inappropriately in this regard. Without a usage policy, both of these options are severely restricted.

We have attached a typical Internet and email usage policy, which you may wish to adapt for your own firm.

2. Example email and Internet usage policies "Use of email policy"

The Company respects your rights regarding privacy and the following email use policy is to ensure that those rights are not compromised and that both yours and the Companies, interests are properly protected.

The Company will allow reasonable personal use of email, monitored through local management.

However, it must be recognised that the Company reserves the right, at its absolute discretion, to monitor and read all email and attachments sent to, or received from, the Internet. Therefore strict confidentiality of personal messages cannot be guaranteed.

Misuse of the company email system may lead to the Company Disciplinary Policy being implemented.

Email attachments

Under no circumstances must software be installed that has been received directly via email as an attachment.

This applies whether the sender is known to the user or not.

Any email that the user is unsure of must be reported to the IT Department immediately.

Internet browsing and email monitoring

The Company will allow reasonable personal use of the World Wide Web (www), monitored through local management.



Fact Sheet

Access to most unsuitable areas of the www has been automatically blocked, for example web sites of a pornographic, racist or otherwise inappropriate nature.

However, it must also be recognised that the Company reserves the right, at its absolute discretion, to monitor access to, and usage of, the www.

The Company has the capability to monitor all www use and can track which internet sites have been accessed, by whom, and when this has occurred.

Misuse of the www may lead to the Company Disciplinary Policy being implemented.

Internet downloads

The company does not recognise the Internet as a primary source and/or preferred method of software acquisition.

Consequently, there is no requirement for staff to download any software directly from the internet.

If a staff member thinks that they have a business application that can be sourced via the internet then the Software Acquisition Process will apply in the first instance.

The IT Manager will decide on the method of obtaining the software which may or may not involve an internet download. Installation will then be arranged on behalf of the user in accordance with these policies and procedures.

Virus/malicious code

Central systems are protected by Anti-Virus protection software. Individual client computers have the client virus detection software installed.

These systems run continually as background processes.

All data transferred to or from company computers is scanned for potential malicious code.

Additionally, all email sent to or received from the Internet is automatically scanned for inappropriate content and virus. All such messages can be monitored by the IT Department.

Suggested User Declaration

Name:

Position:

Department/Team:

Date of Employment: _____

I have read and understood the terms and conditions of the Company's Information Systems Policy.

I agree to abide by this policy during my period of my engagement, as either permanent or temporary staff, with the Company or its partners.

I further undertake to maintain my obligations regarding the security of Company information and data after I have ceased my employment with the Company or its partners.

Signed: _____

Date: _____

Email disclaimer

"This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are



Fact Sheet

addressed.

If you have received this e-mail in error please notify the originator of the message. This footer also confirms that this e-mail message has been scanned for the presence of computer viruses.

Any views expressed in this message are those of the individual sender, except where the sender specifies and with authority, states them to be the views of the originating Company.”

Scanning of this message and addition of this footer is performed by email filter software in conjunction with virus detection software.

3. Useful Links

<http://www.acas.org.uk/index.aspx?articleid=808>
Useful discussion of the concepts behind usage policies, staff engagement and your legal responsibilities.

www.businesslink.gov.uk -
National Business Link web site with many useful references covering issues regarding Internet and email usage.