Employee Internet Use Policy

Does Your Business Have One?

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Employee Internet Use Policy

Do you have employees who use your computers and telecommunications equipment to access the Internet? Do they send e-mails?

Personal use of telephones, mobiles, copiers, faxes etc pale into insignificance compared with the problems that can result from non-business, improper and unauthorised use of the Internet or e-mail. It's a strange fact that whilst few employees would ever consider sending their personal letters on their employer's letterhead, that's exactly what they do when they use business e-mail to send personal messages.

Here are several reasons why your business should have an Internet Use Policy:

- A strong policy protects both the employer and employees from misuse of the Internet, e-mail, and other electronic resources.
- It informs employees of the legal risks they may unknowingly take.
- It ensures that those who breach the policy do so from a conscious and independent choice and not through ignorance.
- In the event of legal action, the business is separate from the actions of individuals and has taken steps as a means of due diligence to have prevented their occurrence.
- It may reduce the time spent on non-work-related activities.
- An effective policy is continually evaluated in regards to its legal relevance, Internet relevance, and with the standards and expectations of all involved.

Employers should provide their employees with clear guidelines about which uses of the Internet are proper, and which uses are not. Employees should also be educated in the potential risks involved when sending e-mails or accessing the Internet. A clear policy that is enforced will help the employer reduce its risk of liability from improper Internet use.

Sending a few personal e-mails may not cost an employer much in lost productivity, but it raises several legal and moral issues:

- E-mails are not confidential and can be read by users with appropriate permission or expertise.
- The use of the "Reply All" key in place of the "Reply" key could result in an e-mail being sent to an inappropriate recipient list.
- Opening e-mail attachments from a dubious source may cause a virus to be downloaded to your system. New viruses are created daily, and even the most sophisticated virus checking software cannot guarantee to block all viruses.
- Opening e-mails from an unknown source may result in information about your system being uploaded to the e-mail sender. This information can then be used for sending "spam" mail.
- Downloading files from websites can import viruses.
- Information that identifies the "surfing" system can be registered when accessing a website. This could have legal implications if the site contains illegal matter.
- Though legislation on Internet use is still in its infancy, employers face a possible legal liability for the Internet use of their employees.
- Employee e-mails that offend or harass recipients could see employers facing legal action.
- E-mails have the same legal standing as other forms of communication to and from a company. Their inadvertent misuse could result in binding contracts being created.
- Employers might also be liable for any other unlawful use of company IT resources - for example, if employees infringe copyright law by downloading and disseminating publications.

Formulating and disseminating an Internet use policy and the implementation of appropriate disclaimers on all external e-mails will reduce your legal risks as an employer.

Should you have an Internet Use Policy?

The question is should businesses have an Internet Use Policy? This includes not only surfing the web but also sending and receiving e-mail, page and file downloads, viruses and anything else that is available online. An Internet Use Policy is about sending and receiving, who owns what, and what kind of monitoring should employees expect.

When setting an Internet use Policy, the most important points are that the Employer needs to:

- state what is and is not appropriate use of the Internet, e-mail, and other electronic resources;
- state what the consequences are of breaking the policy;
- protect itself, its employees, and its assets from misuse of electronic communication resources.

The Facts

In Summer 2005, Vault.com surveyed over 1,100 employees to determine how web surfing and e-mail use affects productivity and quality of life at work.

The survey[1] indicated that during work hours:

- 16% of respondents surf non-work related websites all the time;
- 37% of respondents surf non-work related websites a few times a day; and
- 34% of respondents surf non-work related websites a few times a week.

In the survey, only 9% of employees thought that they should never be able to access non-work related websites. 33% of employees said they should be allowed up to half an hour of personal Internet access and 11% of employees said they should be allowed more than an hour of personal Internet access.

Internet connectivity is almost ubiquitous among UK companies. The speed of access to the Internet at work combined with unsupervised time and little or no accountability adds up to hours of non work-related web surfing and millions of £s in lost productivity. An average of 30% to 40% of employee Internet activity is not business related[2]. Without an Internet use policy, your business is legally responsible for all such activity.

The survey also revealed that 29% of employees felt their employer should not have the right to monitor their Internet usage and 16% of employees took measures to avoid detection.

An Employer can be responsible for e-mails sent under its name.

The doctrine of vicarious liability applies equally to e-mails as it does to other forms of correspondence:

If the recipient reasonably believes the e-mail to be sent by someone representing the business, he/she is entitled to take the contents of that e-mail as representing the views of the company.

Drawing up Your Policy

The Vault.com survey already referred to, uncovered some further worrying aspects of employee Internet use:

- 87% of employees surf non-work-related websites while at work, and of this 87%, 53% engage in personal web surfing every day
- A majority of employees (56%) do not worry about their email or Internet use being monitored at work
- Only 35% of employees believe that surfing the Internet or sending non-work-related emails decreases productivity.

An Internet use policy need not be a lengthy document. It just needs to be clear and consistent about what your business does and does not accept. It should contain information on the disciplinary consequences of any policy breaches thus making it easier to take action against an employee who steps out of line.

Action Points[3]

- You could include the policy in employee induction manuals and ask your employees to sign off on the policy to indicate that they have read and understood it.
- You can also monitor the IT use of your employees with special software. However, take care - there are legal issues you need to be aware of. If employees are monitored without their knowledge, their privacy rights may be breached.

Internet Access Statistics 2008

According to estimates derived from the 2008 National Statistics Omnibus survey, in 2008 16.46 million UK households had Internet access. This represented 65% of households and an increase of 1.23 million households since 2007.

Great Britain has seen an average increase of over 1 million households per year connecting to the Internet since 2004, reaching a total of 16.05 million in 2008.

In 2008, 33.9 million adults (71% of the UK adult population) accessed the Internet in the three months prior to interview. This was an increase of 6.6% (2.1 million adults) from 2007. As in 2007, men were more likely to access the Internet than women (75% compared with 66% respectively). Adults aged 65 plus were still the least likely to use the Internet, with 70% stating they had never used it, down from 82 per cent in 2006.

In 2008, the proportion of adults who were recent Internet users who accessed the Internet every day or almost every day was 69% (23.5 million adults). The 16-24 age group used it most, with 77% using it every day or almost every day. For the first time the majority of adults aged 65 plus who used the Internet in the last three months, did so every day or almost every day (54%). Almost three quarters of men (73%) now use the Internet every day or almost every day, compared with two thirds of women (66%).

Of all UK households, 56% had broadband Internet access in 2008, an increase from 51% in 2007. Of the UK households with Internet access, 86% had a broadband connection in 2008.

For more information visit: www.statistics.gov.uk/pdfdir/iahi0808.pdf

Negative Aspects[3]

- Telling your employees that they are subject to monitoring may reduce the chances of a privacy breach, but it could also have a negative effect on their productivity. People tend to work differently when they are being monitored, as they often feel more self-conscious.
- Monitoring employees could also interfere with the relationship between employer and employee. It may reduce the employee's sense of being trusted and therefore valued.
- Another problem with monitoring is that someone needs to do it. Software might scan for obscene language, for example, and some software will block out porn or gambling websites. But no software program can adequately assess whether an e-mail is defamatory. Somebody would need to wade through a lot of material to monitor even a fraction of the electronic traffic that circulates in an office of any size.

Organisations will vary in the amount of personal IT use they tolerate. The policy will depend on the internal culture and how costly it is to have employees idle for some part of the day.

But while the contents of the Internet Use Policy may vary from business to business, it's clear that every organisation should have one.

Are you enforcing your Employee Internet Use Policy?

A recent survey of 300 business Internet users published on 27 February 2006 by network security provider SmoothWall indicates that employees are ignoring Employee Internet Use Policies, and that 38% of employees that are governed by a policy are unaware of its contents.

The survey found that while at work:
- 61% of respondents use personal e-mail
- 41% of respondents use instant messaging applications; and
- 23% of respondents use Skype.

The most popular sites visited by respondents were:
- News sites (85%);
- Shopping sites (40%); and
- Auction sites (37%).

The survey found that during working hours:
- More than 22% of respondents access non-work-related sites for more than an hour;
- More than a third of respondents access non-work-related sites for more than half an hour;
- 8% of respondents regularly download music or videos over the Internet; and
- 31% of respondents occasionally download music or videos over the Internet while at work.

Only 15% of those surveyed said they only accessed non-work-related sites during lunchtime and outside of core working hours. The downloading of music and videos should be of particular concern as not only does their downloading consume large amounts of bandwidth but may also breach copyright law.

Where an Employee Internet Use Policy is enforced:
- 19% of respondents said the policy is enforced by software control;
- 13% by management checks; and
- 28% by a combination of software and management controls.

40% of respondents said that an Employee Internet Use Policy was in place but was not enforced.

Source: Smoothwall

Don't forget contact lists

In the case of PennWell Publishing (UK) Ltd v Ornstein and others, a magazine editor and conference organiser had built up a list of around 1,650 contacts over his career. On joining PennWell he moved his contact list to their e-mail system and supplemented it with new contacts made during his employment there.

When he left PennWell to set up a similar business, the employee downloaded the list from PennWell's system and took it with him. PennWell asked the court to order him to return the list and not to make use of the contacts on the list.

PennWell had an e-mail policy which stated that the "employee may only use the e-mail system for business use" but there was no evidence that the employee had been told about the policy or that it was part of his contract.

PennWell lost because there was an implied contract that allowed the employee to take a copy of his personal information, even though the judge determined that as the list was on the employer's computer they "owned" the list.

Employers should ensure their e-mail policies make clear that address lists created and contained on the employer's computer system will belong to the employer and, in their entirety, may not be copied or removed.

"...while the contents of the Internet Use Policy may vary from business to business, it's clear that every organisation should have one."

Below, we have included a specimen Internet Use Policy – you can adapt it for your own organisation.

Specimen Internet Use Policy

(Definition: "Company" means [insert the name of your company or business]

This policy applies to all Company staff and to those others offered access to our resources.

(i) General Principles

(a) Use of the Internet by the Company's employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the Company and its business units. The Internet is to be used in a manner that is consistent with the Company's standards of business conduct and as part of the normal execution of an employee's job responsibility.
(b) Corporate e-mail accounts, Internet IDs and web pages should not be used for anything other than corporate-sanctioned communications.
(c) Use of Internet/intranet and e-mail may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
(d) The distribution of any information through the Internet, computer-based services, e-mail, and messaging systems is subject to the scrutiny of the Company.
(e) The Company reserves the right to determine the suitability of this information.
(f) If you produce, collect and/or process business-related information in the course of your work, the information remains the property of the Company. This includes such information stored on third-party websites such as webmail service providers and social networking sites.
(g) The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately.

(ii) Internet Usage: Internet

(a) No Company employee may visit Internet sites that contain obscene, hateful, pornographic or other objectionable or illegal materials.
(b) No Company employee may make or post indecent or defamatory remarks, proposals, or materials on the Internet including on blogs and social networking sites.
(c) No Company employee may use the Internet to perpetrate any form of fraud, hacking, or software, film or music piracy.
(d) Use of the Internet for non-business purposes is only permitted at the following times [insert times].

(iii) Internet Usage: E-mail

(a) Employees may not solicit e-mails that are unrelated to business activities or for personal gain.
(b) Employees may not send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
(c) Employees may not represent personal opinions as those of the Company.

(iv) Confidentiality

(a) Employees shall not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Company, or the Company itself except as may be necessary as "plug-ins" or otherwise as may be necessary for the proper discharge of duties under this agreement. In the case of a third party, the download must be covered or permitted under a commercial agreement or other such licence.
(b) Employees shall not reveal or publicise confidential or proprietary information which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/ network access codes, and business relationships.
(c) Users shall not send confidential e-mails without taking suitable precautions.

(v) Security

(a) Users shall not download any software or electronic files without implementing virus protection measures that have been approved by the Company.
(b) Users shall not intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
(c) Users shall not examine, change, or use another person's files, output, or user name for which they do not have explicit authorisation.

(vi) General

(a) Employees shall not perform any other inappropriate uses identified by the Director or line manager.
(b) Employees shall not waste time on non-Company business.

Protect your reputation and career

If you fail to follow this policy, you risk disciplinary action and termination of employment. The company also retains the right to report any illegal violations to the appropriate authorities.

Social networking sites

If your Internet Use policy does not cover acceptable use of social networking sites, consider introducing it.

State whether or not staff may use such sites during working hours and if so when (e.g. lunchtime). Perhaps make access only available from some centrally located computers.

Also, ensure that staff are aware that they may not post defamatory remarks about their colleagues, customers or the company on such sites.

13 Virgin staff were dismissed in November 2008 for making critical comments about both the company and its passengers on Facebook. Virgin were within their rights to dismiss these staff as they made it clear in a policy on social networking sites that bringing the company name into disrepute through this medium warranted dismissal.

Further Information

ACAS provide a guide to Internet and E-mail Policies, which can be found at:
www.acas.org.uk/index.aspx?articleid=808

Business Link also provide information on Internet and e-mail use and a sample Internet use template and E-mail use template at their "IT and e-commerce" section at
www.businesslink.gov.uk

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

References:

[1] Source: Vault Internet Use in the Workplace Survey, Summer 2005: http://www.vault.com/wps/portal/usa

[2] Source: IDC Research

[3] Report by RANONE:– www.ranone.com

Publication issued or updated on:
26 January 2012

Ref: 559