

An Internet policy for your employees

The Internet is a powerful tool for improving your business' efficiency. But it can also be a great way for employees to waste time, damage the security of your IT system and give you legal headaches.

If you do not already have an Internet policy, you should actively consider putting one in place. A well-thought-out policy can help you enjoy the benefits of the Internet while reducing the pitfalls. It encourages employees to use the Internet effectively, states what you consider to be acceptable use, and sets up procedures to minimise security and legal risks.

This briefing outlines:

- The main elements you need to include in your Internet policy.
- How to implement and enforce this policy.

1 Access rules

1.1 Give employees proper **training** before they use the Internet. This should cover:

- How to use your Internet software.
- Your Internet policy, and how it works.
- Efficient use of the Internet.

1.2 Make sure employees follow your **access procedures**.

- Configure software to maximise security. Do not allow employees to change settings or use other software.
- Depending on the nature of your connection, employees may need to disconnect once they have finished using the Internet. You can set your Internet connection to close down after a specified time if it is not

being used.

- Only give employees remote access (eg using a laptop) to your network or Internet connection when it is absolutely necessary.

2 Using the Internet

2.1 Encourage the use of appropriate services.

- Promote the use of internal and external email for business communications, when appropriate.
- Get employees to access websites for business purposes.

2.2 Control misuse of the Internet.

- Limit personal use (see **3.1**).
- Restrict the sites that employees can visit

Directors' Briefing

a book in four pages

More than 160 briefings are now available.

If you need further information or help, ask the distributor of this briefing about the services available to you.

(see 3.2).

- Control downloads (see 4).
- Control or ban online purchasing (see 5).
- Control or prohibit other uses of the Internet, such as postings on social networking sites, chatrooms or forums (see 6).

2.3 If you have a company **intranet**, you may want to set up extra internal services that work with your Internet software.

For example:

- Make important documents available via browser software.
For example, production schedules, sales targets, standard letters and forms and company policies.
- Set up a bulletin board to improve internal communication without creating excessive levels of email.
- Install diary software that allows employees to schedule meetings and book rooms.

3 Web browsing

3.1 Make it clear in your policy that the web should be mainly or solely used for **business** purposes.

- Some companies ban personal use altogether.
- Some companies allow limited personal use, as long as it does not affect employees' work.
This may improve employees' Internet skills and overall efficiency. But it may be difficult to define 'limited use', and this could make your Internet policy harder to enforce.
- Some companies restrict personal use to set times (eg during lunch breaks).
- Some companies have a more flexible attitude to Internet use outside normal working hours.
But the same cost, security and legal issues apply.

3.2 Restrict the sites that employees visit.

- Social networking sites are a common time-waster. Some companies ban their use altogether.
Other sites can also be offensive and legally problematic (for example, pornographic sites or sites that promote racism).
- Sites that take up a lot of bandwidth can slow down Internet access for other employees. For example, sites that feature videos or music.

- Remove the links to popular websites often available as a default feature on browser software.
Such sites can be major timewasters. For example, online shopping, computer games, sports results and gambling.
- Sites that require you to register can cause problems.
This may leave you open to receiving junk email (spam) or other unsolicited marketing materials.

4 Downloads

Downloading files from the Internet involves certain risks, which your policy should aim to minimise.

4.1 Reduce **security** problems. Downloaded files may contain viruses.

- Install virus-checking software and update it regularly.
- Get your IT manager to configure browser software to disable potentially harmful applications.

4.2 Ban employees from downloading **inappropriate files**, and from installing software (see box).

- All software should be installed by an authorised employee.

4.3 Make sure employees understand **copyright** and other intellectual property issues.

- Any information published on the Internet will normally be protected by copyright.
- The use of software downloaded from the Internet is covered by copyright laws. Remind employees that unauthorised copying is a criminal offence.

4.4 Set limits on the size of **downloaded files**.

- If employees need to download large files, make them do it when the Internet connection is not otherwise needed.
- Avoid downloading large files between 2pm and 4pm, when the Internet is often busy and slow.
- Make sure employees know that printing out large web files can be slow and clog up the printer.

5 Online purchasing

5.1 Make all employees aware of the potential **contractual** liability arising from online ordering and purchasing.

- Tell employees they should only enter contracts on the company's behalf if they have permission to do so. Even then, they must read the terms and conditions carefully to avoid entering into a contract with harsh terms.

5.2 Only allow online purchasing from approved **suppliers**.

Personal downloads

The Internet can be a tempting environment for many employees, who often see little wrong in downloading material for their personal use during working hours.

The most popular types of downloaded files are generally music, video clips, pornographic images or films and free or demo software.

Make sure your policy states the kinds of file you consider to be unacceptable. Failing to control or ban such downloads could lead to a number of problems.

A Time spent online will go up.

Such files are often large, and can take a long time to download (see **4.4**).

- Your phone bill will increase if you only have a dial-up connection.
- Employee productivity is likely to be affected.

B The performance of your systems and software may suffer.

- Downloaded files can take up a lot of disk space, slowing your system down.
- Other users may find Internet connection speeds are noticeably slower when large downloads are being made.

C The security of your system may be threatened (see **4.1**).

D There are legal issues.

- You may be liable for files downloaded on your system. For example, images, text or even music protected by someone else's copyright.

- You may want to encourage online ordering for regular orders from existing suppliers to make ordering quicker and more convenient.

5.3 Allow online purchasing only by **authorised employees**.

- Purchases should be made by employees authorised to make purchases by traditional methods (eg telephone).

5.4 Make sure **payments** are handled securely.

- Check that any sites you use for online purchasing include secure technology. You can often tell if a site is secure when the web address starts with https://, or when your browser displays a padlock symbol. Some sites are members of recognised security schemes, such as VeriSign.

6 Other uses

6.1 Take particular care with **networking sites** and similar services.

Their informal nature may encourage employees to make defamatory comments for which you may be liable.

- Employees should not use these services to comment on your company or competitors or disclose any business information without the express written authority of a director.
- Set up an authorisation procedure for joining new services.
- Apply the same policy you use for email.
- Make sure employees know any communications they send will carry their (company) email address.
- Clearly define what you consider to be acceptable and unacceptable behaviour.

6.2 Generally, you should prohibit the use of online **chat** services and networking sites.

- Many companies now ban the use of networking sites and chat rooms altogether.
- You may wish to make exceptions in specific circumstances. For example, if the network administrator needs to join a technical chat room.
- Clearly define what you consider to be acceptable and unacceptable usage.

7 Your own website

Use your policy to help make sure your website runs smoothly.

7.1 Nominate an **individual** to be responsible for your website.

- Set out how other employees and any contractors will be involved.

7.2 Put appropriate **technical** standards and controls in place. For example:

- Control how the site is updated. Only allow authorised employees to update the site.
- Set limits on the size of files you put on your website. Excessively large files will slow down access to your site.

7.3 Do not infringe other people's **intellectual property** rights.

7.4 Make sure **all employees** understand their responsibility for the website.

- Let employees know if they are responsible for keeping any material up to date. Make this a performance review issue.
- Encourage all employees to be aware of what information is carried on the site and what services are offered.

(and email). If you wish to use monitoring software, you must tell employees that you intend to do so in both your Internet policy and your employment contracts.

- Virus-checking and other security software must be considered.

Ask IT experts what automated solutions could work for you.

8.4 Enforce the policy.

- Make an individual responsible for enforcing the policy. Typically, the network administrator will be responsible for routine enforcement (eg monitoring traffic). But a director should take overall responsibility.
- Apply the policy consistently and fairly to everyone, including yourself. Clarify any exceptions.
- Make sure you have an appropriate disciplinary procedure in place to deal with breaches of the policy.

The policy will only provide legal protection if it is properly implemented and enforced.

8 Implementing policy

8.1 Consult employees on what should be included in the policy.

8.2 Make the policy **available** to everyone.

- Ask employees to sign a copy to confirm they have read it.
- Refer to the policy in your employment contracts.

8.3 Put in place any **software** that will help regulate Internet use without obstructing legitimate access.

- Filtering software automatically prevents access to inappropriate sites. But this may fail to block all inappropriate sites and could inadvertently prevent access to useful sites. You can also use such software to allow access to specified sites only at certain times (eg outside normal working hours).
- Monitoring software produces a log of the sites each user visits, and any downloads made. But unless you actively check the log, monitoring software will only provide evidence after problems have occurred. There are legal restrictions on how you may monitor employees' use of the Internet

© BHP Information Solutions Ltd 2009. ISSN 1369-1996. All rights reserved. No part of this publication may be reproduced or transmitted without the written permission of the publisher. This publication is for general guidance only. The publisher, expert contributors and distributor disclaim all liability for any errors or omissions. Consult your local business support organisation or your professional adviser for help and advice.