Policies to Protect all (cont..)

Contents of e-mail

John Gleeson
Director, iThink Technology
Email: info@ithink.ie

This is a follow on from last month's article regarding creating an Internet usage policy. Email has become an essential tool of modern business communications. It's fast and efficient, but can also potentially be a source of embarrassment or even litigation

Like any business communication, email should be treated as a professional and generally formal method of correspondence. Therefore it is important that you provide your staff with some guidance in the form of an email acceptable use policy (EAUP).

A clear policy can help your staff use email effectively and productively. It can also protect your business from possible legal action from employees, business contacts or customers if email is misused. Typically an EAUP should outline:

- what shouldn't be circulated on the company email system, including any offensive, indecent or obscene material, or anything likely to cause offence on grounds of sex, sexual orientation, race, disability, age, religion or belief
- what can be construed as inappropriate, discriminatory or libellous content
- rules for sending confidential business information via email - eg using encryption software to prevent unauthorised persons accessing it
- what you consider to be appropriate email etiquette, such as terms of address and sign-off, and the need to be formal and businesslike in all communications
- how attachments should be handled, such as checking for viruses - you may also want to set a maximum file size for attachments
- how much personal email use is acceptable
- how the laws governing data protection, e-commerce and email marketing affect your business
- guidance on saving, filing and photocopying emails for company records

Employees should also be informed that emails they send can be recovered even after deletion. You should also let them know what email monitoring may be carried out.

DEVELOPING PERSONAL INTERNET AND EMAIL USAGE POLICIES

You need to decide how much your staff will be allowed to use your network resources to access the Internet or use email. Totally forbidding personal Internet access and email can reduce goodwill, and damage your organisation as much as allowing staff to have a totally free rein. The ideal solution is a middle ground, where both the employee and the employer benefit.

The best way of developing your own Internet acceptable usage policy (IAUP) and email acceptable usage policy (EAUP) is to build a consensus based on sensible and reasonable compromises. Start by canvassing your staff and find out what they want. Create a simple questionnaire to determine what Internet access and personal email facilities your staff would like. Discuss the responses with your employees and try to agree mutually acceptable rules and regulations.

You could ask:

- "Do you have Internet access at home? If so is it broadband?" This may indicate whether staff are likely to use access provided by the business excessively.
- "What are you likely to use Internet access for?", eg leisure, hobbies, research, studying or shopping.
- "Typically how many personal emails do you send per week or month?"
- "Do you own a digital camera?" This could generate many large file attachments.
- "Do you own an mp3 player?" This highlights the need to avoid breaches of copyright.

Discussing your IAUP and EAUP with your staff may encourage their co-operation, and minimise resentment of monitoring or usage restriction. Be prepared to modify and amend your IAUP and EAUP when necessary.

MONITORING INTERNET AND EMAIL USAGE

Monitoring your staff's usage of the Internet or email should be handled carefully. Although it may be easily justified, you need to consider issues of personal privacy and confidentiality. The law allows you to monitor usage of the Internet and email by your staff only after notifying employees that you intend to do so. You should make employees aware of the type and scale of monitoring. Explain why there needs to be some form of monitoring, for example to:

- check and cater for resource utilisation
- protect the individual from exposure to offensive material
- maintain the integrity of the business

There are exceptions to this requirement - such as when monitoring is used for:

- prevention or detection of crime
- apprehension or prosecution of offenders
- collection or assessment of any tax or duty

You can use anti-virus software or filters that automatically block emails with high-risk attachments. You can also use software which automatically prevents people accessing inappropriate websites from your network. Be particularly careful when monitoring communications that are clearly personal. Avoid opening these emails or confine monitoring to the address or heading. And if you need to access an employee's email account while they're away, always let them know in advance. Remember to use your policies or employment contracts to inform employees about the extent of monitoring, or you will need to gain specific consent from them.

Should you require any further information or advice on any of the topics covered please do not hesitate to contact me at jgleeson@ithink.ie