Policies to Protect all

The internet – get it right

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

The Internet is an essential tool for business. Email and the web offer a variety of ways to improve communications with staff, customers and suppliers.

However, allowing your employees unrestricted access to the Internet carries risks. If they accidentally or deliberately access illegal web content, eg anything related to paedophilia, your business could be open to prosecution. There is a security risk - your employees could download and install software infected by a virus. In addition, any abuse of your email facilities could cause internal and external problems. For example, sending bulk email could result in system overload and network congestion.

The first form of defence to create a "Internet and Email Usage Policy" that clearly states what is acceptable Internet and email usage, and what is not. If your policy is clearly stated and then breached, you will have a better chance of defending any action that may be taken against your business.

WHY YOU NEED INTERNET AND EMAIL POLICIES

There are two major reasons to introduce policies for Internet and email use within your business:

- To ensure that communications resources are not wasted and productivity doesn't suffer
- To help protect the business from potentially damaging material being sent or received via the Internet or email and any possible resulting legal action

In general, providing Internet access and email facilities to your staff has tremendous benefits. It can increase efficiency, aid communication and help employees increase their basic IT skills. Allowing staff to access the Internet and email facilities outside working hours can be seen as a perk of the job. However, controlling and policing such access may be difficult.

Trivial abuses of the system include transferring large file attachments, or wasting work time on Internet surfing, personal email or online chat.

More serious risks include:

- downloading files that contain viruses
- obtaining copyrighted material such as music or films transmitting valuable or sensitive business information without encryption
- distributing or relaying offensive or abusive material via email
- generating junk email, or spam, via mass mailings
- accepting files from people in online chat rooms which could bypass firewalls or email filters

More serious misconduct may result in disciplinary or even legal proceedings. This includes:

- accessing or downloading pornography or other offensive material
- libelling or defaming colleagues, or even external business contacts, via email
- using the Internet to commit fraud or other illegal acts

Introducing Internet and email usage policies should help you avoid these risks. It should also ensure that your business and staff get the best possible use out of your IT system.

Policies should state clearly what is and isn't permitted by staff using the Internet or email. You should ensure that your employees are aware of the policies and the consequences of breaching them.

CREATE AN INTERNET USAGE POLICY

You need to decide whether to allow your staff to access the Internet from work in their own time. Many businesses allow access as a goodwill gesture to improve employee relations. However, if you do grant permission, you should think about an Internet acceptable use policy (IAUP).

The IAUP should set out the terms and conditions for staff accessing the Internet from their workplace. It should contain:

- A definition of personal use - eg anything not directly related to work.
- Guidance on how much access time is acceptable and when access is allowed.
- A warning to abide by any copyright and licensing restrictions on Internet-sourced material.
- Instructions on what to do before downloading material - eg checking the size of the file and its source.
- Warnings on the danger of importing viruses through downloaded files and programs.
- What personal use is not permitted - eg accessing pornographic or indecent websites, or using chatrooms in which the use of offensive language is frequent.
- Any sanctions or disciplinary actions that may be taken if employees do not follow the policy guidelines.

Unless you explicitly state what is not acceptable, you will risk an unfair dismissal claim if you dismiss staff who access unsuitable material. You may also need to remind staff that access to the Internet is a privilege and not a right.

You must tell staff that their access may be monitored if you intend to do so. The IAUP could include warnings that:

- any websites visited are traceable back to specific individuals - even if deleted
- the frequency and length of time individuals spend viewing websites will be logged
- any transactions carried out using company resources shall be deemed "non-personal", including personal online banking

Next Month I will cover the contents of the Email Usage Policy

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