

Creating an Email and Internet Usage Policy

Company and IT directors are currently bombarded with confusing legislation, litigation and liability regarding content sent or downloaded by staff, including defamatory, racist or pornographic material and whether or not they should be monitoring.

Litigation is on the increase - companies on the receiving end have included Norwich Union, the Chevron Corporation and Dow Chemical. Loss or theft of data is also a real threat - Gartner Group has valued the loss of business information through email, some of it accidental (due to the informal nature of email and the Internet) at over \$24 billion a year. And this is aside from the threat posed by viruses attached to files. Recent cases such as Love Bug, which TrueSecure estimates cost organisations more than \$700 million, and the Trojan attack on Microsoft, have highlighted problems associated with infection and data loss from email borne viruses.

For organisations to protect themselves and their employees from these business and network integrity threats associated with email and Internet use, we recommend that organisations should establish an Email and Internet usage policy. This needs to clearly define what is acceptable and unacceptable business and personal use. They should also educate their employees on the policy and enforce it using a content security solution.

In spite of the recent European Human Rights Act which highlights the issues surrounding email monitoring in the workplace, a recent survey on UK companies shows that as many as two thirds do not have an Internet or Email policy in place or do not enforce it. Using software to monitor the policy and having mechanisms for enforcing shows commitment to protecting company and employee alike.

So what should be addressed in an Email and Internet Usage Policy?

1. Monitoring and Enforcing: an indication of the measures in place to show determination to enforce; the penalties for/consequences of breaching the policy; why the policy exists

(protection of staff, company reputation and IT security).

2. Responsibility: name the individuals responsible for training and indicate where to go for answers to queries regarding the policy; employees should be fully aware at all times of what constitutes the policy and know the consequences should it be abused.

3. Liability: details of legal liability should the policy be breached (to reinforce the seriousness of the problem).

4. Definitions: a definition of what is appropriate business and personal Internet usage if an Internet connection is provided for business use. This should include details of sites which should never be accessed using business facilities and time; a clear statement on whether the company allows private web based email, and if so, under what circumstances (e.g. no attachments, video or music files; only for making arrangements, times of day, costs, and so on).

5. Business Materials: company policy on the circulation of business materials, in particular those likely to be generated in an employee's own field of work; potential pitfalls in the circulation of materials (how to avoid accidental distribution of confidential information).

6. Lost Productivity: how to avoid this and what the consequences might be.

7. Forbidden Files: what types of files may not be circulated via email, or uploaded or downloaded via the web.

8. Data Theft: how to avoid it (Cyberwoozles, cookies and how to spot them).

9. Viruses: how to spot and avoid them.

10. Acknowledgement: a form to sign acknowledging that the employee has seen and understood their obligations, making adherence to the policy part of their terms and conditions of employment.