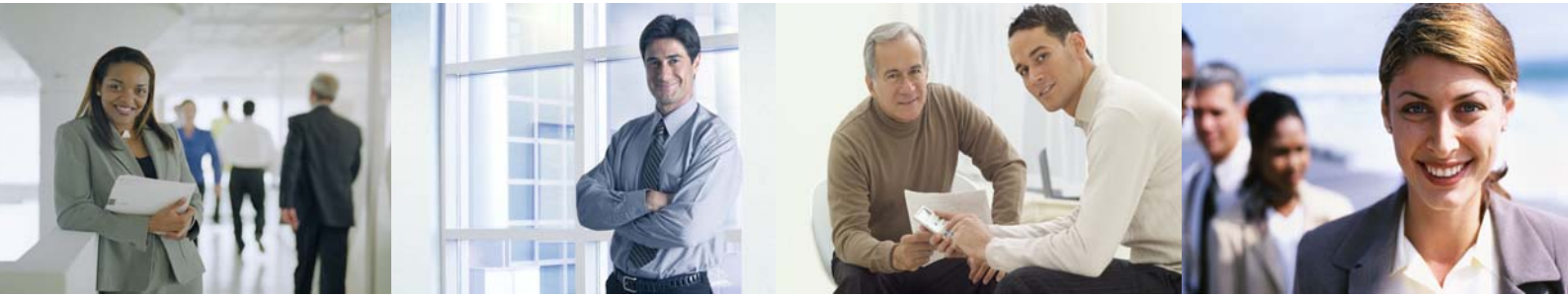


Email and Internet Liability Issues



There are a number of areas in which the improper use of company email and internet access can result in legal liability for your company. Here we look at some of the areas of concern and offer some ideas for protecting your company from the nightmare of a legal battle.

Defamatory Emails

Organisational email is a business tool. Anything sent from a corporate email address is effectively written on electronic company letterhead. As a result, any views, quotes, or discussions made via company email can be seen to be representative of the company.

The use of profanity in business email has obvious implications for a business's reputation. Additionally such emails can have more concrete repercussions as well. There have been several lawsuits involving sexual harassment in the workplace, based on lewd comments sent by email. In many cases the organisation has been held responsible for not controlling their email content so as to avoid offensive exposure to employees.

- Norwich Union Insurance was forced into an out of court settlement of £450,000 for alleged defamation by e-mail against a competitor, Western Provident Association.
-

Organisations are always at risk that employees representing them may make inappropriate comments, thus giving a false image of the company. Defamation, racist comments, political views, offensive material - all of these facets of employee indiscretion can have serious legal and reputation implications for the entire business.

WHAT YOU CAN DO

- Appending a legal disclaimer may reduce legal liability with respect to employee comments made on company email correspondence - expressly state that the views expressed in the email do not constitute the views of the organisation.
- Your professional indemnity liability policy may also cover defamation.

Offensive Emails

Additionally there is the threat of employees causing offence, intentional or otherwise, through the sending of internal email. This could be because of obscene language, jokes, images or comments which cause offence, or even threatening remarks made.

- In 1995, the Chevron Corporation paid \$2.2 million to four female employees to settle a lawsuit in which the women claimed they suffered sexual harassment through receiving e-mail jokes.

Conducting Interviews

WHAT YOU CAN DO

Establish an appropriate email usage policy and purchase Internet Filtering software, which will allow you to quarantine and block email messages containing profanity and other offensive words both in the body of the email and attachments.

Offensive Website Images

Inappropriate Web use also has potential legal liability implications. Offensive images displayed on a computer screen may count as harassment, and such images are easy to find on the Web.

WHAT YOU CAN DO

- Introduce an Internet Usage policy which prohibits employees from using the internet to access offensive or unsuitable websites, and monitor internet usage using one of the numerous spyware software solutions available.
- Use Internet Filtering Software to limit employee Web browsing to sites which meet company policy, and to control the download of potential offensive material/images.
- Adapt network settings to prevent access to barred sites.

Viruses and Spam

Another area of concern is when company email systems are inadvertently or maliciously used for Spam relay, and then infect other companies with email viruses. This can result in loss of reputation, systems effectively being 'shut down' by denial of service attacks, and million of dollars in damage and lost productivity.

WHAT YOU CAN DO

- Ensure your network is protected with effective anti-virus software
- Run daily anti-virus scans on individual PCs
- Set up spam filters
- Ensure sure employees are aware of risks and are vigilant when opening email
- Appending legal disclaimers to auto signatures can also reduce legal liability.

Online Defamation

Another defamation risk comes from online bulletin boards which enable disgruntled employees to broadcast complaints, justified or not, about a company's people, practices, and products.

WHAT YOU CAN DO

If you perceive this as a real potential threat, consider a periodic monitoring of sites and bulletin boards with a view to deleting any problematic material. Purchase adequate defamation specific indemnity insurance.

Sabotage

If an employee leaves on bad terms it is possible that they may attempt to misuse passwords to get into online systems either to retrieve information or sabotage systems remotely.

WHAT YOU CAN DO

- Conduct exit interviews with all employees, taking time to discuss grievances with disgruntled employees to forestall any malicious attacks.
- Change all passwords as soon as an employee leaves to prevent unauthorised access.
- Make sure you have an effective disaster recovery plan in place which covers this eventuality.

