

## **The Importance of An Effective Internet Use Policy**

*- by Sylvia Low & Serena Lim*

### Employee's Use of Email / Internet

Law Firms today use e-mail as a standard form of communication both within the office and with clients. Employees regularly have access to the Internet and use it as part of their daily routine. Are your employees using the Internet to communicate with family and friends? (of course!); surfing for pleasure? Which sites are being downloaded unknowingly into your office servers? Employees have even been known to use the office email to run their own sideline businesses. Employers are faced with potential liabilities for misuse of the office Internet access by their employees and find themselves grappling with issues of how much access to allow their employees and how to monitor Internet use within the firm.

### Potential Liability for the Law Firm

Potential liability for misuse of email may arise from regulations and laws as diverse as breach of solicitor-client confidentiality and professional negligence to defamation, obscenity and sexual harassment. Another consequence of Internet misuse that has potentially serious implications for law firms is downloading computer viruses (and transmitting the virus to contacts in your law firm address book).

### The Problem with Email

The problem with emails is the way they are used – with the throw-away informality of a telephone conversation. Potential risks arises from the glaring fact that email messages, unlike oral communication, is not “throw away” at all. Conversely, the permanence of email communication and the ease with which email messages can be sent to a mailing list of contacts with one click of your mouse carries enormous potential to create dire consequences for the sender (and his employer). Cautionary tales of email abuse within the legal industry abound but everybody's favourite must surely be the notorious rake (associate lawyer from Norton Rose) who forwarded an email from his girlfriend containing intimacies about their relationship to his buddies who, with customary high jinks, sent an embellished version of the email to their own contacts list. Within a week several thousand other people across several continents in the English speaking world had received a copy of the email and the story (with excerpts from the regrettable email) had broken in the tabloid press.

Firstly, once a statement is in print, the reader's perception of the “communication” subtly shifts; something said in jest may very likely be perceived as holding out a more dubious intention on paper. The clearest example of the difference with which the law treats oral and written communication lies in the law of defamation. A person is liable for defamation for statements made orally only if there is proof of actual loss flowing from the alleged defamatory statement whereas written statements attracts liability simply on the basis that the statement was made. Secondly, printed matter is open to the process of “discovery” in an action against the firm. “Confidential” memo from one executive to another containing business strategy to undercut the competition or to withhold critical information from your opponent will not make your law firm look good when publicly known.

While most lawyers understand the wisdom of the adage – Don't send by email anything you wouldn't want to read about in the newspapers – its quite another thing to expect your employees to take these lessons to heart. So what can a responsible employer do about Internet abuse in the office? A total ban on personal Internet use turns all your employees into routine regulation abusers and alienates the management; and it might actually be more efficient and less disruptive if employees could arrange their personal matters by email instead of using the phone. Monitoring emails has proven an effective deterrent

against routine abuse but implementing a monitoring system (whether automated – in the form of “mail sweeping” software that will pick up unrecognized addresses or certain words - or manual, through random spot checks) may prove inefficient and burdensome.

### Internet Use Policy

What you need is an effective and enforceable Internet Use policy that educates (and reminds!) employees of the potential dangers and consequences (personal as well as for the law firm) of improper use of the Internet in the office. A well conceived policy which the employee is asked to sign his acceptance of as part of his contract of employment may enable you to avoid liability as a consequence of breach by an employee. Better yet, it may prevent the misuse from occurring in the first place. An effective internet use policy should serve as a reminder to your employees that email is a permanent record (even clicking “delete” merely removes its map from the sender’s desktop directory but does not eradicate it from the office email servers) and may show up in the employees performance evaluation or in court.

### Issues in an Internet Use Policy

While different law firms are likely to take different approaches on these issues, an effective Internet Use Policy should state clearly and unequivocally –

1. that the employer has a right to monitor everything that is written and sent out on the office email system;
2. the extent of access to the Internet for personal use – including a description of prohibited sites;
3. the prohibition of defamatory, lewd or unlawful material in emails;
4. enforcement mechanisms and penalties for violations of the policy.

Other issues and operational procedures that should be addressed in a comprehensive Internet Use Policy are –

- Workstation security including restrictions on third party access to the employee’s passwords and desktop;
- Use of Company headers, signature templates and appropriate confidentiality notices in all office emails;
- Desktop housekeeping processes including routine archiving and “empty trash/delete” functions;
- Activation and routine operation/update of Anti-virus software and procedures.

### Sample Internet Use Policies

Some excellent sample Internet Use Policies can be found in the following sources –

<http://www.llrx.com/features/internetpolicy.htm>

<http://personal.law.miami.edu/~mc4388/emailpolicy.html>

<http://www.out-law.com> (for members only)

<http://www.weblaw.co.uk/art080998.htm>

### Conclusion

As email use becomes the medium of choice for business communications, law firms must adopt effective risk management strategies or they leave themselves exposed to liabilities. Or recommendation of an effective strategy comprises an Internet Use Policy that addresses the security issues discussed above, an appropriate level of supervision, disciplinary measures for violations and breaches of security; and finally, the will to implement both.