February 1998

Email policies considered

Jay Forder
Bond University, jay_forder@bond.edu.au

Patrick Quirk
Bond University

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder and Patrick Quirk. (1998) "Email policies considered".

E-Mail policies considered
by Jay Forder & Patrick Quirk, Consultant Editors

The worldwide electronic mail system is a part of, and yet quite distinct from, the Internet. It has a broader coverage than the Internet and has capabilities beyond mere communication between humans (e.g., it can be used to produce automatic responses between computers). The previous issue of "Law & Technology" considered legal liability for e-mail and highlighted the need for a corporate policy. We now consider what a sensible policy might contain.

A successful e-mail policy must serve many purposes. Above all it must educate a workforce and it must give specific directions on corporate behaviour. In addition, it will set the tone for corporate communication and could even provide a defence in case of legal action, such as proceedings brought under the Trade Practices Act (Cth). The practical wisdom contained in such a policy will enhance the overall success of the business. A poor policy, or failure to draw one, could have the opposite effect.

Following are some of the issues relevant in developing an effective e-mail policy.

**Monitoring issues**

This should deal with who may monitor company e-mail and for what purpose. Failure to notify employees that their e-mail is being monitored could lead to complications in the event of a dispute or termination. A delicate balance must sometimes be struck between employee privacy and company security and industrial laws implying that parties treat each other with "mutual trust" should be considered in this context.

A sample clause drafted by a US attorney which achieves this purpose is set out below:

"2.3 Electronic information created and/or communicated by an employee ... will not generally be monitored by the company, and we respect our employees' wish to work without 'Big Brother' looking over their shoulder. However, the following conditions should be noted:

2.3.1 The company routinely monitor usage patterns for both voice and data communications (e.g., number called or site accessed; call length; times of day calls). Reasons include cost analysis/allocation and the management of our gateway to the Internet."
2.3.2 The company also reserves the right, in its discretion, to review any employee's electronic files and messages and USAGE to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other company policies.

2.3.3 Employees should therefore not assume electronic communications are totally private and confidential and should transmit highly sensitive information in other ways. 4

If e-mail is to be monitored then this should be brought to users' attention clearly and frequently e.g. some companies do so each day upon first access to the network.

Retention policy
This should cover what records of e-mail are to be kept and by whom. Who may access these records from within the organisation should also be dealt with, especially since e-mail may be the subject of discovery in future litigation. The use of message digests could also become crucial here. A message digest is an algorithm which can be applied to any set of data (for example, e-mail messages for Corporation X for the month of January) to produce a very small electronic result.5 This result can only be reproduced by applying the algorithm to exactly the same set of data, thus enabling one to tell easily whether the original set of data has been altered. The ATO's Tax and the Internet Report (August 1997)6 illustrates how message digests can be used to verify financial data. An audit of archived e-mail could also be authenticated in this way.

Security
Important matters include what level of encryption (if any) is to be observed for internal and external e-mail as well as the type and size of files which may be uploaded to and downloaded from the company system. Filtering programs which "sniff" for viruses as well as unacceptable words, phrases or files can also be employed here.

Password training and security must also be dealt with. The fundamental rule for the former is "change passwords often and don't use your dog's name". For the latter there must be a clear statement of employee responsibility for password confidentiality.

Forwarding & copying policy
This can often be overlooked. Unnecessary forwarding and copying can clog the system and breach confidences. On the other hand, failure to forward or copy could leave gaping holes in company communications. A good test is: if this were a letter or memo, how would it be managed? The same rule should then apply to e-mail.

Training and network etiquette (netiquette)
E-mail should be treated like any other corporate communication and appropriate modes of address and response developed. Electronic mail is not an appropriate mode of communication in all cases and this should be made clear. Some issues are better dealt with by phone or face to face – delicate communications seldom travel well via e-mail. Other hints for e-mail users might include a list of common courtesies and practices observed by all users of the Internet e.g. providing phone and postal details with all e-mails, as well as ensuring that enclosures are readable on the intended recipient's computer. The Netiquette Home Page is one source of information on this topic. 8

Advertising and junk
Internal and external sources of junk e-mail must be monitored. An internal "for sale" listserv may solve the problem of clogging the network with irrelevancies, though some employers would prefer to keep their network entirely clear of such messages. Reducing one’s exposure to external junk e-mail (spamming) is also a matter which must be addressed and proper Web page design can make it harder for scavenger bots to "harvest" your e-mail address (and then sell it to someone else!). 9

The above concerns can apply in reverse for companies which use e-mail for marketing purposes. Careful consideration should be given as to when and how e-mail is used for business promotion purposes and a consistent and ethical set of instructions should be issued to employees.

Compliance with the law
The fundamentals of the law on defamation, intellectual property, privacy and contract should be brought to the attention of e-mail users. Special laws applying to particular sectors should be considered e.g. duress laws for salespeople, confidentiality laws for bankers and lawyers, trade secret and patent laws for engineers etc. etc. Appropriate guidelines for using e-mail "tag lines" and "CONFIDENTIAL" or "PRIVILEGED" headings should be developed and publicised.

E-mail (digital) signatures
In a commercial situation, who may sign e-mail can be very important. Internal authorisation procedures should be considered as well as digital signature law in the relevant jurisdictions.

Insurance
Depending on the importance of e-mail to one's business, it may be prudent to insure against loss incurred as a result of misuse or failure of the corporate e-mail system. The Australian insurance industry has yet to offer such cover on a wide scale.

Sample policies
To sample a comprehensive email (and IT) policy relating to a University with a large number of e-mail users, see those at the Queensland University of Technology. 7 Adam Conti's generic e-mail policies also provide useful guidance. 10

---

1 For further technical discussion of e-mail see The Internet Report, prepared by CSIRO for the Australian Taxation Office as part of the Electronic Commerce Project, June 1997, para 3.2.6.

2 e.g. the "due diligence" defences under section 65 of the Trade Practices Act (Cth). The presence of a corporate compliance program can also lower penalties under the TPA.

3 Useful legal guidelines for e-mail use in the USA can be found at www.gigleg.com (Gordon & Glisson P.C. Attorneys at Law); Readers interested in Europe & the UK should look at http://www.bakerinfo.com:80/publish/ surl/sp2002092599123html ; "An Employer's Staff Email and Internet Policy" (Boeker & McKenzie, London, 1996).

4 Adam Conti's Internet Law Office; see http://www.comlaw.com/policies.html (clauses slightly abridged).

5 See CSIRO Report (above) at 4.3


7 A mixture of letters and numbers is always best.


9 See further tips on this at www.junkbusters.com.

10 See previous article in this series "E-mail Liability - Postcards from the Edge".


12 Adam Conti's Internet Law Office; see http://www.comlaw.com/policies.html.