E-Mail guidelines for solicitors

Revised November 2004

Adapted with permission from the *Email Guidelines* published by the Law Society of England and Wales

Important Note

The Law Society's *E-mail Guidelines* are intended to assist solicitors achieve good practice in relation to e-mail. However, the Guidelines do not create, or extend or define the scope of any duties of professional conduct. To determine the conduct requirements in relation to any issue described in the Guidelines, reference should be made to the relevant rules and principles in the *Hong Kong Solicitors' Guide to Professional Conduct* ("*Guide*")
(See the section "Professional Guide": The Law Society of Hong Kong.)

1. **CONTEXT**

The use of e-mail exposes businesses, including law firms, to new risks including:

- risk of non-compliance with various statutory requirements (e.g. data protection legislation)
- threats to the security of IT systems – distribution of viruses.

2. **PURPOSE**

2.1 These guidelines have been drawn up to assist principals, or others in solicitors' firms, responsible for drawing up or approving a firm's e-mail policy.

2.2 To ensure the proper management and supervision of the practice including compliance with rules of professional conduct and statutory requirements.

2.3 An e-mail policy which firms can tailor to their requirements is set out in Annex A. Guidance on e-mail security is offered in Annex B.

3. RULES OF PROFESSIONAL CONDUCT

Introduction

3.1 The Solicitors' Practice Rules and the Solicitors' Practice Promotion Code are subsidiary legislation under the Legal Practitioners Ordinance. The non-statutory principles in the *Guide* are also binding on solicitors. Both sets of requirements need to be considered when drawing up an e-mail policy. The material can be found on the Law Society's website.

Supervision and Management of the Practice

3.2 Rule 4A of the Solicitors' Practice Rules: the principals in a practice must ensure that their practice is properly supervised and managed so as to provide for:

(a) compliance with the *principal* solicitors' duties at law and proper supervision of staff both professional and general;

(b) effective *management* of the practice generally.

3.3 A written e-mail policy will help provide for the proper supervision and management of staff in relation to e-mail.

3.4 A written e-mail policy should be brought to the attention of all partners, consultants and staff, temporary and permanent and it should be enforced. It should be reviewed regularly and it should be linked to other relevant policies, e.g. IT security policies.

3.5 A policy is of particular importance if firms intend to monitor employees' communication. Firms should note the guidance in the *Code of Practice on Human Resource Management* published by the Office of the Privacy Commissioner for Personal Data ***Code of Practice on Human Resource Management*** *("Code")*.

Section 1.4.6 of the *Code* states:

"As a matter of good practice, the policy …… should include matters such as:

- *Whether the use of the E-mail system by employees for sending and receiving personal E-mail is permitted and any special arrangements that employees should adopt for segregating personal E-mail from work-related E-mail.*

- *Whether the employer reserves the right to access and read E-mail sent and received by employees using the E-mail system.*

- *Specific rules that apply to the distribution of incoming or outgoing E-mail and the erasure of unnecessary E-mail that contain personal data or have an attachment that includes such data."*

3.6 Firms should review the *Code* and future revisions to ensure that they are aware of the Privacy Commissioner's views.

Mandatory information in solicitors' correspondence

Principles

3.7 Rule 2A of the Solicitors' Practice Rules and the Solicitors' Practice Promotion Code and Law Society Practice Direction D8, requires a firm's correspondence to include:

- The name of the firm **(See Solicitors' Practice Rules : Rule 2B)**
- The firm's address
- The names of the firm's principals which will be provided upon request. **(See Law Society's Practice Direction D8)**

Confidential and legally privileged correspondence

3.8 Professional solicitor correspondence is generally confidential and may attract legal professional privilege.
(See the *Guide* Chapter 8)

3.9 Many firms already include a warning to this effect in fax messages because of the risk that these could be sent to the wrong person by mistake. Firms should consider adopting similar confidentiality warnings for e-mail.

3.10 While automated confidentiality warnings are unlikely to impose any legally binding duty on an unintended recipient, many recipients may be expected to heed them, and the warnings may therefore help prevent a mistake from causing loss. For example, a solicitor must normally disclose to a client all relevant information received by the solicitor but 'where it is obvious that privileged documents have been mistakenly disclosed to a solicitor, the solicitor should immediately cease to read the document, inform the other side and return the document.'
(See the *Guide* Principle 8.03, Commentary 6)

3.11 This specimen warning can be adapted for use:

"Information in this message is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender, and please delete the message from your system immediately."

3.12 E-mail servers can be configured to add a warning to all outgoing e-mail. Alternatively, a warning could form part of a signature block. Automatic inclusion of a warning is recommended. Firms could also prepare a template for use by their staff as and when needed. Where firms allow their staff to contribute to public mailing lists, or chat forums, confidentiality or privilege warnings are inappropriate on such messages.

3.13 Solicitors should note that legally privileged information in solicitor-client correspondence may cease to be privileged if the message is sent to others, (e.g. if the message is accidentally sent to a mailing list).

Timely response

3.14 A solicitor should deal promptly with communications relating to the matters of a client or former client.
(See the *Guide*, Principle 5.12, Commentary 5)

3.15 Firms are familiar with handling incoming letters, faxes and telephone calls during the absence of the intended recipient. E-mail presents new problems because it can arrive unseen by other members of staff. A limited number of people, (a secretary and a colleague, for example) should have access to an absent person's inbox, and all staff should be made aware that this may happen, and check the contents regularly to deal with urgent e-mails.

3.16 It is also recommended that firms use automated out-of-office responses when staff are away from the office for a day or more. Where possible, an automated out-of-office message should be sent only once to any e-mail correspondent (most e-mail systems allow this).

Records

3.17 Most firms print e-mails and file a copy in their paper records. Advanced electronic storage solutions are available that retain the metadata – the cost of the software will obviously be a consideration.

3.18 Firms should take a pragmatic and common sense approach to e-mail records. Significant and substantive e-mails (including e-mails that are subject to statutory retention periods) should be printed and stored, but those that are ephemeral can be left to expire from electronic storage in the ordinary course of events.

(**See Law Society Guidelines on Storage and Destruction of Old Files 02-384)**

3.19 Where some correspondence about a matter is stored electronically and the rest is on paper, firms should ensure that none of the material will be overlooked if responsibility for a matter is transferred, (perhaps temporarily). Firms should also be confident that they know what information their systems record. If not, an audit may be appropriate.

3.20 Firms should note that electronic storage media can become inaccessible for a variety of reasons, including the obsolescence of, or changes to, equipment and software. Useful advice is provided in the UK's National Archive's Digital Preservation Guidance Notes on the preservation and management of electronic records.
http://www.pro.gov.uk/about/preservation/digital/guidance

4. STATUTORY PROVISIONS

The Personal Data (Privacy) Ordinance ("PDPO")

4.1 E-mails containing personal data must be processed in accordance with the principles of the PDPO. These include a requirement to process personal data fairly and lawfully, (i.e. explaining the purposes of the processing and who might see the data, unless it is obvious). Data controllers are also required to meet one or more statutory conditions for processing. The conditions include consent. Data subjects are generally entitled to request and receive a copy of the personal data held on them by the firm's data controller. This can include personal data in e-mails including some 'deleted' e-mails.

4.2 Special rules apply to personal data relating to offences, disclosures made in connection with legal proceedings, and to processing for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights.

4.3 Data protection rules are complex and you are advised to allocate the responsibility for compliance to someone in the firm. This person should become familiar with the provisions of the PDPO. In addition, data subjects broadly have the right to ask for copies of their personal data. This person can also ensure subject access requests are dealt with appropriately and within the statutory time limit of 40 days.

4.4 Firms need to review the correspondence of fee-earners and other staff to ensure that professional standards are maintained (subject to the rules on monitoring discussed below). If advice is given by staff via e-mail, firms will need to be able to check the accuracy of the advice.

4.5 Normally this will be done by a review of paper files, but cases may arise where firms will wish to check communications on their way to or from a member of staff.

4.6 Where the use of the firm's system for private communications is permitted, such checks may intrude on the privacy of staff members. Firms with offices abroad should be aware that such checks may not be lawful in all jurisdictions.

4.7 It may be possible to exclude private e-mails, where these are allowed, from any monitoring undertaken by the firm. If it is not possible, and private e-mails may be intercepted and read, the freely given consent of staff to such monitoring should be sought. It is permitted, however, to monitor e-mail solely for the purpose of determining whether it is a business communication or a personal one. Firms should consider the implications of consent being withdrawn.

4.8 Monitoring and recording e-mail will also generally involve the processing of personal data under the PDPO. Section 1.4 of the *Code* sets out guidance for businesses to consider when monitoring or recording e-mails in the work place. Firms should review this guidance carefully before undertaking any monitoring or recording of e-mails in the workplace.

5. BEST PRACTICE

Professional undertakings

5.1 Professional undertakings may be given by unsecured e-mail but firms should be cautious when accepting them: it is not difficult to fake both content and sender.

5.2 The act of typing a name into an electronic document, including an e-mail, is a form of electronic signature. The use of digital signatures may also provide assurance for the recipient of the authenticity of e-mail. If encryption is widely adopted it might bring with it the additional benefit of improved confidentiality.

5.3 In the meantime, firms receiving a professional undertaking by e-mail should check that the context provides reasonable assurance of its authenticity and should consider verifying it came from its purported sender.
(See the *Guide* Chapter 14)

Copyright

5.4 Sending copyright works by e-mail which have been copied without the consent of the rights-owner is likely to constitute a copyright infringement. It is easy to attach copyright material to e-mails and to cut and paste material from other e-mails. There is an additional risk that original copyright warnings (if any) will be lost when only the attachment to an e-mail is copied. Firms should ensure that e-mail policies prohibit copyright infringement.

Unsolicited bulk e-mail: Spam

5.9 Unsolicited bulk e-mail or, as it is generally known, 'spam' can be a significant problem. Most large organisations find that much e-mail traffic is unnecessary and time-wasting. Users often send e-mails about trivial matters and use large copy lists. The solution is proper training and guidance in the use of e-mail. But this does not solve the problem of spam – which is usually a form of advertisement. Spam can add significantly to the general problem of e-mail overload. Up to fifty per cent of unfiltered e-mail on the Internet can be described as spam.

5.10 Filtering software is available to reduce the amount of spam arriving in users' inboxes. It is increasingly used. However, firms should note the risk of filtering out legitimate client correspondence using spam filters. If firms use spam filters they should explain that important communications should always be followed up with a phone call, fax or printed copy by post.

5.11 Firms that run their own mail-servers (or whose Internet service provider will offer this service) should consider deleting unsolicited e-mail. If a message is sent back the issuer of spam can use the information to their advantage and confirm the subject of gratuitous spam.

ANNEX A

SAMPLE E-MAIL POLICY

Important Note

- This is a generic policy on the use of information technology. It should not be used before being reviewed and amended to cover the specific circumstances of your firm.

- The policy does not cover disciplinary procedures which might arise as a result of breach of the policy, which should be added to this policy or dealt with separately.

- This policy was drafted in ……..2004. The laws affecting e-mail and internet usage and market best practice (e.g. security standards) are in a state of flux. You should regularly review your e-mail policy to take account of legislative change and developments in best practice.

(NAME OF FIRM)

POLICY ON THE USE OF INFORMATION TECHNOLOGY

Introduction

The purpose of this policy is to provide a short guide to the rules to be observed by users of the Firm's Information Technology (IT) systems. By IT systems we mean telephones, Blackberry and other such devices, computers including (without limitation), PDAs and other telecommunications equipment supplied by the Firm. This policy is intended to contain guidance on your conduct. You are expected to exercise professional judgment at all times.

Comments on the policy are welcome; they, together with any requests for clarification, should be addressed to ***(insert position)***

Security

All members of staff are responsible for the security of the IT terminal(s) allocated to them, and must not allow them to be used by another person unless permitted by this policy.

Passwords, or other security access devices electronic or biotechnical devices ("security keys") are unique to each user, and must not be made available to any other member of staff unless authorised by ***(insert position)***. For the avoidance of doubt, upon the termination of your employment (for whatever reason) you are required to provide details of your password/security keys to the Firm.

Inappropriate use of the Firm's Equipment and IT Systems

Access is granted to the world wide web, and to other Firm systems, only for legitimate business purposes. Incidental personal use is permissible provided it is in full compliance with the Firm's rules, policies and procedures, such as this policy and its disciplinary rules, ***(insert any other relevant policies).***

Under no circumstances should the Firm's equipment or IT systems be used to send, receive, browse, download or store material which may be illegal, offensive or cause embarrassment to others. This includes [without limitation] the use of the office systems to send, receive, obtain access to, download or store pornographic material and material inappropriate web-sites. Please refer to the section on the world wide web below.

Monitoring

You should bear in mind that, for business reasons, your use of office systems including the telephone and IT systems may be monitored. You should also be aware that other members of the Firm have access to your system and the data stored or may oversee what you are doing.

You should be aware that the system provides the capability for other people to monitor e-mail, voice-mail, world wide web and other communications traffic. The Firm reserves the right to monitor e-mail, voice-mail and any other data held on its IT systems, including workstations and laptops owned by the Firm.

Personal Use of Firm Facilities

The minimal use of the Firm's IT facilities to send personal e-mail or to browse the world wide web is acceptable provided that usage:

(a) is minimal and takes place substantially out of normal working hours;

(b) whenever it takes place, it does not interfere with client or office commitments;

(c) does not commit the firm to any marginal costs [at present the marginal cost of sending emails or browsing the web may be taken to be zero]; and

(d) complies with the Firm's policies.

This policy on personal use is designed to be liberal, but its continuance is, of course, dependent upon its not being abused or overused and may be withdrawn or amended.

E-mails Generally

Take care in what you say in e-mail messages. Improper statements can give rise to personal or Firm liability. Work on the assumption that e-mail messages may be read by others, particularly by people who do not usually work for you, such as temporary secretaries, and do not include in your e-mails anything which would offend or embarrass any such reader, or would embarrass the Firm if it found its way to the public domain. Specifically:

(i) Never send abusive, obscene, sexist, racist, harassing or defamatory messages. If you receive such a message, do not forward it to anyone. Report it to ***(insert position)***. If a recipient asks you to stop sending them personal messages then always immediately stop.

(ii) Never send messages from another member of staff's computer or under a name other than your own name (although secretaries are permitted to send e-mails in their own name on behalf of any of the solicitors they work for, if instructed to do so by their solicitor provided they use the e-mail tool which automatically states, at the top of the e-mail, that it is sent on behalf of the relevant solicitor).

(iii) Never send confidential messages by e-mail without getting the recipient's agreement.

(iv) Never open an e-mail attachment from an unexpected or untrustworthy source or if, for any reason, it appears 'suspicious' e.g. if attachments end with ".exe". Most viruses are propagated by e-mail. If you suspect you have been sent a virus inform ***(insert position)***.

(v) Remember that e-mail messages are documents which must be disclosed in legal proceedings if relevant to the issues unless protected by privilege, therefore, always exercise the same caution in what you say in e-mails as you would in more formal correspondence.

(vi) Never send or forward private e-mails at work which you would not want a third party to read.

(vii) Do not create e-mail congestion by sending trivial messages or unnecessarily copying e-mails to those who do not have a real need to have them.

(viii) Do not send or forward "chain-mail" e-mails as they have a propensity to over-load the system.

(ix) Do not advertise by e-mail or send messages about lost property.

(x) Always remember that text, music and other content on the Internet are copyright works. Never download or e-mail such content to others unless you are certain that the owner of such works allows this.

(xi) If sending important information by e-mail, always obtain confirmation of receipt (either a reply to your e-mail or by following up with a telephone call).

(xii) Never agree to terms or enter into contractual commitments or make representations by e-mail or non encrypted email without having obtained proper authority. Remember, when you type your name at the end of an e-mail, this act is just as much a signature as if you had signed it personally.

(xiii) Do not copy software from the firm's computers and IT Systems.

External E-mails

Never send strictly confidential messages via the Internet, or by other means of external communication which are known to be unsecure. If requested to forward information over the Internet, make sure that your client knows that it is not totally secure and is willing to accept that risk. Printed copies of all significant business e-mails should be retained on file.

The World Wide Web

Please remember that web sites can track visitors to their sites. We store recently accessed web pages in our own system, to improve access times. This is called "caching" web pages. If you visit a site, you may well leave a "calling card" which will enable the site owner to work out who has visited. If you are visiting a site for proper purposes, such as gathering evidence on a fraudulent website, consider accessing it other than from the Firm's systems if this could prejudice your investigation. If the web site is an inappropriate one, that calling card could embarrass the Firm. If you access, download, store or forward inappropriate material others might be offended. In some cases you may be committing a criminal offence if, for example, the material is pornographic in nature. For these reasons, you should adhere to the following policies:

(a) See the rules on personal use referred to above;

(b) Do not access from the Firm system any web page which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. This definition is intended to be interpreted very widely;

(c) The same rule applies to any files (whether documents, images or other) downloaded from the web.

Security – Home Software

Security issues encompass the need to ensure that the Firm is protected both against misuse of others' copyright material, for example by loading onto office machines programs that are not properly licensed, and against computer viruses, for example by loading onto office machines programs or files which have not been checked properly for viruses. Accordingly, you may not without permission load onto office machines any software which has not been provided by the Firm.

ANNEX B

E-MAIL SECURITY

1. It is often said that the Internet is inherently insecure. In fact, Internet applications like e-mail can be used in both secure and insecure ways. Consideration should be given to the security features available to you and, particularly where you are processing personal data; you should be careful to take appropriate technical and organisational measures to ensure that your e-mail communications are safeguarded.

2. Bear in mind that messages may pass through the hands of unregulated service providers; the networks used by the Internet are vulnerable to hacking; and governments can undertake interception on a substantial scale.

3. Human error is the most likely cause of confidential e-mails being received by an unintended recipient : the sender typing in the wrong e-mail address. Less likely, but still technically possible, is the risk of an e-mail message being accidentally misrouted to the wrong recipient or intercepted intentionally by a third party. Law firms that carelessly expose sensitive communications to these risks may be liable for breach of professional conduct rules for breaching client confidentiality. They may also be exposed to civil claims for breach of confidence.

4. The internal threats are, generally, greater than the external threats. A disgruntled employee may deliberately forward sensitive information to a competitor or to his home or private e-mail account if he is intending to become a competitor. Employees may also hack into private areas of a firm's network or into the e-mail account of other employees. Systems administrators and other IT staff employed by, or contracted to, a firm are in a particularly privileged position as regards access to confidential material. They should all be carefully vetted before being taken on, which is a requirement of the Personal Data (Privacy) Ordinance. Encryption of sensitive documents may be necessary to prevent technical support staff accessing them. Ensure that technical staff do not have a back-door route to access (e.g. by logging on as a user).

5. Although the threat of a successful and serious external breach of system security or interception of e-mails by a third party is not as high as the risk of an internal security breach, the number of attacks is rising. The vulnerability of systems with 'always-on' (broadband) connection to the Internet is far greater than systems with dial-up access. On average, it takes 17 minutes from first connection for an 'always-on' system to be attacked. Such systems should be protected with properly configured firewalls.

6. External threats include:

- the activities of hackers, who seek to obtain access to systems and networks;

- attacks on web sites, including the use of clone or mirror web sites to trawl for intelligence; appropriating content from your web site and attacks on your image or brand by defacing or altering the web site;

- denial of service attacks, where a web server is flooded with useless information to prevent legitimate traffic getting to its destination. The types of attack include bandwidth consumption and resource starvation;

- virus attacks where a virus runs on your system without permission, including terminate and stay resident file viruses, parasitic viruses, overriding viruses, stealth viruses and polymorphic viruses (this list is not exhaustive);

- the use of worms that can systematically eat through and destroy stored files before moving on by sending a copy of itself to other machines to replicate the process;

- the introduction of malware (malicious software) such as a Trojan horse, that permits a remote user to take control of a machine over the Internet to download files, change system configurations to permit easier access when entering on later occasions, see what is on a user's screen, reboot the computer and capture passwords;

- the monitoring of your network by others, called a "sniffing attack", that involves deploying a piece of code on the network that monitors all traffic, looking for passwords, key words or numbers (often, the first few digits of common credit cards) and other information.

7. Firms should not include confidential information in non-encrypted e-mail without the informed consent of clients, whether corporate or individual. In the case of individual clients, solicitors are advised to ensure that their clients fully appreciate the risks being described above. The latter can be ensured verbally or through e-mail correspondence or engagement letters.

8. Firms are recommended to adopt systems that:

(a) provide the facility for retrieving (and automatically decrypting) encrypted incoming mail; and

(b) automatically encrypt all outgoing e-mail to those offering similar facilities.

9 Firms should keep private cryptographic keys securely under their own control. They should not rely on the use of encrypted communication links for which service providers control the cryptographic keys.

10. Firms should be aware that encryption software using strong cryptography is widely available, and that such software is available on the Internet free for non-commercial use. (This may enhance the willingness of clients to take advantage of it where use by the client would be non-commercial, as in most criminal, family and residential conveyancing cases).

11. E-mail can bring viruses and malicious software into firms' systems. As well as damaging those systems and interfering with service to clients, such viruses and software can distribute confidential information or allow unauthorised access to it.

12. Firms should maintain up-to-date technical precautions against such risks and ensure that users are alert to the importance of complying with associated procedures. Measures that may be taken in order to manage the security risks include conducting regular inspections of employee e-mail logs for breaches of security (subject to the rules on monitoring discussed above), the logging of access to private areas of the firm's network and communicating the firm's policies to all staff by way of an IT usage policy. Implementing and enforcing an IT usage policy which is drafted to be consistent with industry best practice, will also help to mitigate the risk of successful claims being brought against firms for breaches of confidence committed by their staff.

13. Firms should ensure that all relevant devices including laptops, PDAs and home computers used for business-related work are brought within the scope of their IT and e-mail security policies.

80423