



The Law Society

The Law Society

E-mail guidelines for solicitors

November 2005

Important note

The Law Society e-mail Guidelines are intended to assist solicitors achieve good practice in relation to e-mail. At points they refer to duties which exist in professional conduct.

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 of professional conduct (see www.guide.lawsociety.org.uk) and not to these Guidelines.

1. Context

- 1.1 E-mail is the most popular application on the Internet. About 15 billion e-mails are sent every day and the number is growing. The benefits to businesses and individuals are incalculable.
- 1.2 E-mail has also exposed businesses, including law firms, to new risks. These include the risk of non-compliance with various statutory requirements (for example, data protection legislation) and threats to the security of IT systems. Over eighty per cent of viruses are distributed via e-mail.

2. Purpose

- 2.1 The purpose of these guidelines is to assist principals, or others in solicitors' firms, responsible for drawing up or approving a firm's e-mail policy.
- 2.2 It is important that firms consider having a written e-mail policy; it will help 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.

For alternative formats, e-mail alternativeformats@lawsociety.org.uk, or telephone 0870 606 6575.



3. Rules of professional conduct

Introduction

- 3.1 The Solicitors' Practice Rules 1990 (the Practice Rules) and the Solicitors' Publicity Code 2001 (the Publicity Code) are made under statute and statutory rules respectively. The non-statutory principles in The Guide to the Professional Conduct of Solicitors (the Guide) are also binding on solicitors. Both sets of requirements need to be considered in drawing up an e-mail policy. They can all be found on Guide Online (www.guide.lawsociety.org.uk.)

Supervision and management of the practice

- 3.2 Rule 13 of the Practice Rules requires that (1) The *principals* in a practice must ensure that their practice is supervised and managed so as to provide for:
- (a) compliance with *principal* solicitors' duties at law and in conduct to exercise proper *supervision* over their admitted and unadmitted staff;
 - (b) adequate *supervision* and direction of clients' matters;
 - (c) compliance with the requirements of sections 22(2A) and 23(3) of the Solicitors Act 1974, section 9(4) of the Administration of Justice Act 1985 and section 84(2)(c) of the Immigration and Asylum Act 1999 as to the direction and *supervision* of unqualified persons;
 - (d) 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 link to other relevant policies (for example, equal opportunities or IT security policies).
- 3.5 A policy is of particular importance if firms intend to monitor employee communications (see paras 4.7-4.14 below). Firms should note the Information Commissioner's consolidated Employment Practices Data Protection Code. Part 3, Monitoring at Work, recommends that:



'if monitoring is to be used to enforce the organisation's rules and standards make sure that the rules and standards are clearly set out in a policy which also refers to the nature and extent of any associated monitoring. Ensure workers are aware of the policy.

Section 3: Monitoring: Good Practice Recommendations

- 3.6 Firms should review the Code (and future revisions) to ensure that they are aware of the Information Commissioner's views.

Mandatory information in solicitor correspondence

- 3.7 E-mails which do not include a solicitor's letterhead should not, in themselves, be considered as letters. However, if an e-mail takes the form of a letter, then the requirements relating to professional stationery, set out in the Solicitors' Publicity Code 2001 s.2, will apply. Similarly they will apply to an electronic copy of a letter sent as an attachment to an e-mail.

Confidential and legally privileged correspondence

- 3.8 Professional solicitor correspondence is generally confidential and may attract legal professional privilege. (See Chapter 16 of the Guide).
- 3.9 Many firms already include a warning to this effect in fax messages because of the risk that these will 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 '[w]here 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' (the Guide 16.06).

- 3.11 The following specimen warning is offered for adaptation:

"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. Alternatively, firms could prepare a template for use by their



staff as and when needed. Where firms allow their staff to contribute to public mailing lists, 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 (for example, 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 (the Guide, 12.10).
- 3.15 Firms already know how to handle incoming letters, faxes and telephone calls in the absence of the intended recipient. E-mail presents new problems because it can arrive unseen by other members of staff. Arrangements should be made to check incoming e-mails. 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, although by doing so, evidence contained in the email header is lost.¹ Electronic storage solutions are increasingly becoming available that retain the whole email — and firms should consider actively monitoring the availability of such systems, because greater use of electronic communications will continue to expand by both firms and their clients, and the cost of storing e-mails on paper will outweigh the cost of storing e-mail correspondence in its native format. Firms tend to use them to back-up paper files and only a few firms are wholly electronic.
- 3.18 Firms should take a pragmatic and risk-based approach to records of e-mails. That is, significant and substantive e-mails (including e-mails that are subject to statutory retention periods) should be stored in a suitably managed electronic storage system or printed and stored, but those that are ephemeral can be left to expire from electronic storage in the ordinary course of events.

¹ The header includes a trail of the computers from which the email was sent, through which it has been routed, times and other information. These may be relevant if, for example, there is a dispute about whether and, if so how, an email was delayed in transmission, or about which hands it has passed through en route. Usually a paper print contains none of these details.



- 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 In the longer-term, firms should be aware that electronic storage media can become inaccessible for a variety of reasons, including the obsolescence of, or changes to, equipment and software. The National Archive's Digital Preservation Guidance Notes provide advice on specific topics related to the preservation and management of electronic records (www.nationalarchives.gov.uk).

4. Statutory provisions

The Data Protection Act 1998 (DPA)

- 4.1 The Information Commissioner (www.informationcommissioner.gov.uk) maintains a public register of data controllers and data controllers must notify the Information Commissioner of certain registrable particulars.
- 4.2 Solicitors will generally be required to notify as data controllers under the DPA. If, exceptionally, a firm having examined the DPA considers that it does not need to notify then it is strongly advised to record the reasons in writing. The Information Commissioner's website provides extensive guidance on notification (and other data protection issues) as well as an online self-assessment tool to assess whether or not notification is necessary. Processing personal data without notifying the Information Commissioner is an offence.
- 4.3 E-mails containing personal data must be processed in accordance with the principles of the DPA. These include a requirement to process personal data fairly and lawfully (ie: 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 data controllers. This can include personal data in e-mails including some 'deleted' e-mails but a mere mention of someone in passing in an e-mail will probably not be personal data. The Information Commissioner's website contains guidance particularly on the Court of Appeal's decision in *Durant v The Financial Services Authority* [2003] EWCA Civ 1746 which contains detailed guidance on the meaning of 'personal data'.



- 4.4 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.
- 4.5 Firms should also note that the seventh data protection principle requires data controllers to take steps to secure personal data. Most unencrypted e-mail is vulnerable to unauthorised access and alteration as it passes over the Internet. Firms should consider this issue in evaluating their DPA compliance and in drawing up the firm's overall IT security policy.
- 4.6 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 DPA, ensure that the firm notifies the Information Commissioner of its processing and ensure that personal data is only processed in accordance with the data protection principles. 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.

The Regulation of Investigatory Powers Act 2000 (RIPA)

- 4.7 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 by e-mail, firms will need to be able to check the accuracy of the advice.
- 4.8 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.
- 4.9 Where the use of the firm's system for private communications is permitted, such a check may intrude on the privacy of members of a firm's staff. Firms with offices abroad should be aware that such checks may not be lawful in all jurisdictions.
- 4.10 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.
- 4.11 RIPA creates several offences and a statutory tort of interception of a communication in the course of its transmission without lawful authority. The offences and tort potentially apply to a firm's monitoring and recording of e-mail communications sent and received by staff. The Telecommunications (Lawful Business Practice) (Interception of



The Law Society

Communications) Regulations 2000 set out various circumstances in which monitoring and recording of e-mail for business related purposes is deemed to have lawful authority. Firms should review this legislation when establishing e-mail monitoring and storage policies and practices.

- 4.12 Monitoring and recording e-mail will also generally involve the processing of personal data under the DPA. Part 3 of the Information Commissioner's consolidated Employment Practices Data Protection 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.
- 4.13 Solicitors should also be aware that the developing area of law under the Human Rights Act 1998 is relevant to monitoring activities in the workplace. In particular, article 8 of the European Convention on Human Rights (ECHR) provides that "everyone has the right to respect for his private and family life, his home and his correspondence". The right to privacy extends to the workplace. Whilst solicitors' firms are not public authorities and therefore the Human Rights Act 1998 does not apply to them directly, the Courts are such a body and are increasingly taking human rights cases into account in their decisions.
- 4.14 Employment tribunals considering any claim made by a disgruntled employee are required to have regard to the articles of the ECHR in the course of their decision making.

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 the need for a check by telephone or fax that it came from its purported sender.

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.

Special rules applicable to e-commerce

- 5.5 Directive 2000/31/EC (the E-Commerce Directive) applies to solicitors' services provided electronically from or within the EU, except for litigation and notarial work. It also applies to electronic advertising, including websites. The E-Commerce Directive affects the rules which apply to electronic services and advertising. Broadly:
- The Law Society's rules will apply to the exclusion of other professional rules if a solicitor's office in the UK provides electronic services (even an e-mail sent from a lap-top on a holiday beach in Spain).
 - If a solicitor based at an office in an EU state other than the UK provides electronic services (even an e-mail sent from a lap-top on a visit to London) the professional rules of that EU state will apply, to the exclusion of the other professional rules.
- 5.6 The E-Commerce Directive requires solicitors providing services electronically or advertising electronically to provide customers with certain information:
- (i) name, address, e-mail address and VAT number;
 - (ii) where price is referred to, clear indications of price;
 - (iii) professional details, as follows:
 - If the office is in the UK, the client must be told that the service is provided by solicitors of England and Wales, regulated by the Law Society, and how to access the Society's rules. This can be done by providing a link to www.guide.lawsociety.org.uk.
 - If the solicitor is based at an office in another EU state, the client must be told that the service is provided by a solicitor of England and Wales, registered with (for example) the Athens Bar, and how to access the rules of that Bar.

The extent of the requirements in the E-Commerce Directive (and the UK's implementing regulations) is not entirely clear. Firms are recommended to ensure that the information at (i) - (iii) above always appears either in the communications by the firm that constitute electronic services or electronic advertising, or in a terms of business letter sent to the client. In particular, a reference (or link) to www.guide.lawsociety.org.uk is important and these items should always appear on a firm's website.



5.7 If electronic trading is carried out, (very unlikely in the present context) suppliers must provide a description of:

- (i) the technical steps required to enter into the contract;
- (ii) how end users may correct any inputting errors; and
- (iii) how end users can access and store the terms of the contract made.

5.8 Further information can be found on the Department of Trade and Industry's website at <http://www.dti.gov.uk>.

Unsolicited bulk e-mail (Spam)

5.9 Unsolicited bulk e-mail or, as it is generally known, 'spam' can be a significant problem for firms using e-mail. 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 50% 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 warn clients not to assume that every e-mail will be received. 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 returning unsolicited e-mail to the sender. This prevents spammers knowing that the address they e-mailed was genuine and provides an opportunity to tell legitimate senders that their mail was blocked². The returned e-mail could include a message along the following lines:

Your message below was blocked by our filter because it was categorised as unsolicited bulk e-mail. If this was a mistake, we apologise. In that case, please send the message again, including in the header the access code *****. This will ensure that your message is not blocked and that the address from which you sent it is automatically recorded as one that should not be blocked in the future.

5.12 Firms who are themselves considering e-mail marketing campaigns should familiarise themselves with the requirements of the DPA, the Electronic Commerce (EC Directive) Regulations 2002, SI 2002 No.2013, the Distance Selling Directive (Directive 97/7/EC)

² Distinguish manual response by a user which does indicate that an address is genuine.



The Law Society

and the Privacy and Electronic Communications (EC Directive) Regulations 2003. Guidance on the latter (which has special rules for unsolicited direct marketing by e-mail) was published on the Information Commissioner's website in November 2003. Firms will wish to note that the DTI recently amended the distance selling regulations (www.dti.gov.uk/ccp/topics1/ecommm.htm). Firms must also consider relevant professional rules of conduct.

Conclusion

- 6.1 These guidelines end where they began, by emphasising the great benefits that e-mail can bring to professional practice. Their aim is to ensure that the risks of e-mail are well managed so as to ensure that its full benefits are realised.



Annex A

Example e-mail policy

Important notes:

- ***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 refers to other policies which firms should have in place (e.g. anti-harassment policy).***
- ***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 last reviewed in 2005. 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 that the Firm requires to be observed by users of the Firm's Information Technology (IT) systems. By IT systems we mean telephones, computers including (without limitation) PDAs and other telecommunications equipment. This policy is intended to contain guidance on your conduct. You are expected to exercise professional judgement 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 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 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 Equal Opportunities Policy, its Anti-Harassment Policy, its disciplinary rules, ***[and 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 which is racially or sexually offensive. You should therefore refrain from visiting inappropriate web-sites. Please refer to the section on the world wide web below. Please refer also to the Firm's Anti-Harassment Policy.

Monitoring

You should bear in mind that, for business reasons, your use of office systems including the telephone and IT systems will 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:

- (i) the usage is minimal and takes place substantially out of normal working hours;
- (ii) whenever it takes place, the usage does not interfere with client or office commitments;
- (iii) the usage does not commit the firm to any marginal costs (at present the marginal cost of sending e-mails or browsing the web may be taken to be zero); and
- (iv) the usage complies with Firm policies.



The Law Society

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 it 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. Please take note of the Firm's Anti-Harassment Policy.
- (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 lawyers they work for if instructed to do so by their lawyer provided that 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 lawyer).
- (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' (for example, if it ends in .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 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.

External e-mails

Never send strictly confidential messages via the Internet, or by other means of external communication which are known not to be secure. 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. Copies of all significant business e-mails should be retained.

The World Wide Web

Please remember that web sites can “know” who has visited them. 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. You should cross refer to the Firm's Anti-Harassment Policy. For these reasons, you should adhere to the following policies:

- (i) See the rules on personal use referred to above;
- (ii) 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: content may be perfectly legal in the UK yet in sufficient bad taste to fall within this prohibition. Sometimes the content may be against the law. As a general rule, if any person within the Firm (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that the Firm's software has accessed the page might embarrass the Firm if made public, then it may not be viewed;



The Law Society

- (iii) 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 properly virus checked. Accordingly, you may not load onto office machines any software not provided by the Firm without the permission of [*insert position*].



The Law Society

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. The most likely cause of confidential information in an e-mail being received by an unintended recipient is human error: 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 Data Protection Act 1998. 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 (by logging on as a user for example).
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.



The Law Society

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.