



## LITIG EMAIL PROJECT – JAN 04

*[This document was originally produced by LITIG for use by any firm. No responsibility is accepted for any errors or inaccuracies. The document has been created in an anonymous style - any firm intending using this as a basis for their own email policy should amend or delete any sections in italics].*

### Email Acceptable Usage Policy (AUP)

Use of the Firm's e-mail systems must be in line with the separate guide covering the E-mail Usage User Good Practice Guide.

#### 1. General

The e-mail system is a business tool and should therefore only be used in an appropriate business like manner (even in the case of personal use). Outgoing e-mails bear the firm's name and if the contents are inappropriate it may affect our reputation or put us at risk of legal or other action.

**The firm takes the use of the email system and this acceptable usage policy seriously. Abuse of the email system or contravention of this policy may constitute Gross Misconduct. Disciplinary action can lead to summary dismissal without prior warning.**

The golden rule:

**If you wouldn't say it in public or send it by post – DON'T e-mail it**

#### 2. Monitoring of E-mail Use

The firm monitors the use of the email system. All e-mail traffic is monitored automatically with a view to identifying inappropriate and excessive personal use contrary to this policy as well as trying to protect the firm's IT resources. E-mails may also be monitored if you are absent from work due to sickness or while you are on holiday to check whether communications received by e-mail are relevant to the business and to enable appropriate action to be taken.

To enable us to enforce this policy it may be necessary on occasions to read the content of e-mails sent and/or received. However, we will not read e-mail messages that are clearly private unless absolutely necessary.

E-Mail must not be used to make defamatory or offensive comments. Profanity checks are carried out on all outgoing messages.

Additionally most organizations have a gateway between their e-mail system and the internet. Your e-mails will be subject to additional scanning and monitoring at their destination.

#### 3. Security

You must not disclose your E-mail system access password to anyone else, provide e-mail access to an unauthorised user or access another user's e-mail box without authorisation. You must not impersonate any other person when using e-mail or amend the content of any messages received. If

you need to provide access to a colleague to monitor your e-mails (for example while away from the office) then you should give them the appropriate access via proxy.

Informal or inappropriate communications with those who work for competitors or clients can put us at risk. If in doubt do not send anything by e-mail that you would not be prepared to send on the firm's headed notepaper. Under no circumstances should you use e-mail messages to communicate personal details.

If you suspect that you have received an e-mail containing a virus you must immediately contact the IT helpdesk (rapid action is required to contain the spread of computer viruses). Do not forward the suspected e-mail to anyone. Failure to report viruses promptly (whether or not any damage is caused) will be treated as gross misconduct.

Colleagues must not pass on any chain letters, junk email or spam (unsolicited messages) received, except to forward to IT Helpdesk or, in exceptional circumstances, alert colleagues to a problem (e.g. 'Nigerian fraud' type frauds).

It is now considered that password protecting documents does not provide sufficient security and does not meet the requirements of the policy, so this approach should not be used.

*Insert any firm's rules on encryption here.*

#### **4. Legality**

Any offer and acceptance conveyed by E-Mail regarding contracts must only take place after all the parties involved have agreed to the terms of electronic trading. An e-mail can constitute a contract so you must ensure that the language used in any message does not indicate a commitment that you cannot keep or are not authorised to make

You should ensure that the transmission of "personal data", for example, databases, spreadsheets, outside the firm does not infringe the principles of the Data Protection Act 1998 (DPA). A spreadsheet containing information such as a person's name, age, address etc is covered by the DPA.

Any information, software or graphics from any published format (books, magazines, brochures and the Internet) are likely to be protected by copyright law, regardless of whether a copyright notice appears on the work. As solicitors we will be taken to know this. Any breach of copyright will be taken very seriously.

Whilst we may be assiduous in housekeeping our e-mails, recipients may keep a record that is discoverable in the future. You must therefore treat all e-mails sent internally and externally as a permanent record (i.e. like a letter or a fax). Further, copy e-mail transmissions may be disclosed in litigation. Before you send an e-mail, think carefully about its content and ask yourself how you would feel if you received that message or knew it may be disclosed in Court. Your e-mails can be "discovered" in future by outside parties if relevant to litigation

#### **5. Inappropriate Use**

For the purposes of this policy, inappropriate, offensive, obscene or pornographic material is material (whether text, jokes, graphics, programmes, data, pictures, video clips, photographs or other images) that we consider (in our absolute discretion) to be racist, sexist or otherwise discriminatory, which contains nudity or images of a sexual nature or which does or could cause offence to people or material that is illegal or defamatory.

Inappropriate use includes:

- Excessive chat or unproductive usage;
- Any personal financial or commercial dealings;
- Regular transmission and/or receipt of large files for example photographs, video clips and/or other images;
- Breach of confidentiality of the firm's information;
- Sexual, religious or racial harassment;
- Bullying;
- Defamation;
- Illegal use;
- Professional misconduct;
- Viewing or circulation of obscene or discriminatory material, or other content deemed unacceptable by the firm;
- Breach of security of the firm's IT systems;
- Circulation or use of unlicensed software.

### **Receipt of Inappropriate E-mail**

Incoming e-mail may contain inappropriate, offensive, obscene or pornographic material (as previously defined) which then lies in our records and can be forwarded or otherwise propagated. You should therefore only provide your e-mail address to bona fide business contacts or known contacts. If you receive any inappropriate e-mail material that you consider to be discriminatory or view as being inappropriate you must:

- Where the e-mail is obviously spam (unsolicited junk e-mail) simply delete it – ideally without reading it first.
- If the sender is known to you or is not an obvious source of spam then reply to the sender saying that you do not wish to receive any such material in the future. You should keep a hard copy of your reply so that you can demonstrate that you have taken the appropriate action;
- Delete your copy of the incoming material. Never forward inappropriate material, externally or internally;

- If your actions have failed to prevent the inappropriate material arriving, you should draw this to the attention of your line manager/team co-ordinator and the IT helpdesk (who may be able to block it).

## **6. Personal Use of the E-mail System**

You may occasionally use the e-mail system for necessary, brief and reasonable personal use provided that it does not interfere with the performance of your duties. Where possible, such use should be limited to your lunch break or outside normal working hours. Excessive personal use may, depending on the circumstances be treated as gross misconduct.

The firm does monitor the use of our e-mail system. The purpose of such monitoring is to ensure that workers are not breaching the rules and conditions set out in this policy. You should be aware however that if the monitoring reveals other information that we cannot be reasonably expected to ignore (e.g. criminal activity, gross misconduct etc) then that information might be used against you.

Private use can never include private profit - nothing may be sent from the firm which is in relation to another business activity being promoted by the sender

All outbound e-mails will have the firm's disclaimer and other details attached. If your e-mail is personal then you should make it clear that this is so.

Colleagues must not participate in 'net abuse', a phrase which includes any anti-social use of the Internet or the firm's IT resources. Net abuse includes, but is not limited to, spamming (generating a significantly higher volume of outgoing email than a normal user).

### ***Disclaimer:***

*The LITIG group provides members with a forum for sharing information and experience and exchanging views. The views, recommendations, policies and other comments are those of the individual members to which they are attributed and are not to be construed as being those of the firms or organisations which those members represent. For the avoidance of doubt, all such views, recommendations, policies and comments are made or given on an informal and non-binding basis, for the purposes of LITIG and not for any other reason, and accordingly neither LITIG nor the member in question shall have any responsibility or liability for any loss or damage arising from the use of or reliance on such views, recommendations, policies and comments.*