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 Usage - User Good Practice Guide

Use of the Firm's electronic systems must be in line with the separate guide covering the Acceptable Usage Policy. This guide serves as a best practice usage guide and should be read in conjunction with the overall policy.

Although electronic transmission is reliable it is not guaranteed. Problems with delivery or receipt may occur in elements outside the control of the firm in much the same way as can occur with post.

Personal Use

A limited amount of personal use is acceptable but this should be kept to a minimum. Please be aware of the restrictions to this in the overall policy as contravention of these can be a dismissable offence.

When using the firm's email system for personal use it is essential that you do nothing which is out of keeping with the firm's reputation. You must also make clear that the email is entirely personal and in no way represents the views of the firm or in no way makes a commitment in the name of the firm.

When accessing personal email accounts, hotmail etc, through the firm's systems there is a risk arising from attachments containing viruses. The same principles must be applied in not opening any files which may expose the firm's systems to any element of risk.

Attachments

When sending email with attachments, thought should be given to the size of the attachments. In particular presentations, photographs or documents containing pictures or spreadsheets including extensive calculations are more likely to have large file sizes. Where the sender or recipient has a restricted mailbox size such files may prevent the receipt or sending of other mail. It should also be noted that when sending these externally they may exceed the parameters set for the recipient company's acceptable incoming file size.

Some types of attachment may also be subject to restrictions both outgoing and incoming because of the increased likelihood of containing viruses. Files with the extension .exe or .pif for example. Although it may be frustrating when you are waiting to receive a legitimate incoming file of this nature it is an essential safeguard within the system and your co-operation and support is appreciated.

Sending Email

In sending email or replying to email consider carefully the number of people who you choose to cc. Although it is very easy to send email to a wide audience if those people do not genuinely need to be included you are not only creating unnecessary email traffic and storage but wasting a significant amount of working time when multiplied across the number of people reading the mail to determine it is not relevant.

If sending an email to multiple parties outside the firm, a circular or information sheet for example, you should always blind copy the recipients (so all the other recipients details cannot be seen) to ensure that you do not risk breaching data protection requirements with regard to disclosing information on other people.

If you require a recipient to take action they should be included in the “to” box of the email. Recipients included as “cc” only should regard the email to be for information only.

When addressing email be careful to select the correct recipients. Do not assume that within the firm’s address book there is only one person with the surname you select. Always ensure the email is correctly addressed before sending.

Be careful when sending confidential or sensitive information. Email can be viewed by a number of parties at both the sending and receiving end and may be accessible in between. Information which you are not happy to send in this way should be encrypted or sent in password protected documents. Please note that protected documents may give rise to some issues as these cannot be virus checked automatically as they are received. Some email gateways may detach or delete attachments which cannot be opened.

If you are forwarding an email for a recipient’s “information only” mark it as such.

If correspondence would normally be reviewed or approved by someone more senior before being sent the same should apply to email.

The use of read receipts should be kept to a minimum. They should not be used as an acceptable “big brother” practice but only where the sender genuinely needs to know when the recipient reads the mail. It should be noted when sending email externally that very few providers support the return of read receipts. It should also be noted that if the recipient has set up for another person to have access to their mail and they open the email, the read receipt will be activated even though the intended recipient has not yet seen the email. If you have used a read receipt the acknowledgement should not be retained “as evidence” that your mail has been read by the right person as that may not be the case.

Only use the “high priority” marking where a message needs to be dealt with as a matter of priority and use it sparingly.

Where the information in an email requires a response within a given time and is no longer relevant after that time, use the options to set the email to expire after that point to save the recipient wasting time.

Where a notice is of general but not necessarily immediate interest please use the firm’s noticeboard rather than emailing all the users.

Receiving Email

Should you incorrectly receive an email that was not intended for you please notify the originator and delete the copy you receive.

If you receive any unsolicited “junk mail” or “spam” do not reply. At best this will confirm back to the sender that they have hit a valid email address. If it is obviously spam from the header, delete without opening the email to prevent the return of any read receipt providing confirmation of your address.

Frequency of Checking / Time Away from Office

Read your email regularly and where appropriate reply to it within a reasonable time.

When away from the office and unlikely to be checking email at least twice a day set your out of office reply to notify senders that you are not likely to be reading their mail and provide an alternative contact point should they have an urgent issue.

When away from the office make arrangements for someone to check your email (by giving them access to your mail box, not by giving them your password) in the same way that you would expect post to be dealt with. Be aware that it is advisable to show only that you are out of the office, do not give information that suggests you are away from your home as this information may present a security risk to your property.

The immediacy of email can lead to a compulsion to be available at all times. Employees should remember that email is not dissimilar to post. If you would not need to deal with post out of your working hours or whilst on holiday you should not feel the need to treat email differently. Although you should check and respond to email regularly (i.e. at least twice per day) you should not allow it to control the flow of your other work.

Email Etiquette and Protocol

Although email may be seen as a more informal form of communication you should not write anything you would not previously have been happy to include in a letter sent on company paper.

Take into account email protocol and in sending email the use of bold, capitals or red text in inappropriate places may be regarded as shouting. Due to its impersonal nature email can come over as being abrupt or aggressive. In circumstances where you are aware that the tone of an email may be harsh try to use the telephone or personal contact in order to avoid antagonising the recipient.

Email can be a very impersonal means of communication. It should not be used to deliver difficult personal messages.

Email should not be used as a means of avoiding talking to people.

When using colour within email particularly to differentiate comments and replies be aware that if printed most documents will be printed in black and white and the differentiation may be lost. Bold text or use of different fonts can be more practical in these circumstances.

Should you subscribe to an internet “email group” please ensure that you are familiar with the appropriate etiquette of the group. This is likely to cover points such as: Acceptable material for the list to cover. In some instances this may involve replying to specific points offline rather than through the group. Unsubscribing when away from the office if you set an out of office reply in order that each email received does not give rise to a response.

Security

Ensure that you keep your password confidential. Leaving your email accessible to other may lead to email being sent fraudulently on your behalf. In addition to this be aware that if the sender of email to you has not safeguarded their own system there is a risk that email you receive may be being sent fraudulently. Some viruses when propagated have the ability to spoof an email address. If you receive a suspicious item from an apparently known source do not assume that the source is legitimate. If necessary use another means of communication to check the source before opening or actioning the email.

It is the firm’s policy not to include external addresses within the global address list. In the event of any virus being successful in penetrating our systems this minimises the likelihood of it being inadvertently sent onto our clients or other third parties.

Managing Current Email and Email History

In managing email, it is helpful to keep in the inbox only those emails which need to be dealt with. Emails which need to be kept for future reference are more effectively managed by moving to separate folders. This can also be the case with emails where action is required but only on a future date.

Carry out regular housekeeping to your mailbox. Remove deleted items and delete irrelevant or duplicated emails and email chains. In doing this, treat email in the same way as other documents, remember to follow the legal requirements with regard to document retention. *[Insert details of your firm's recommendation / requirements with regard to archiving email]* Be aware that hard copy of emails is not accepted as reliable evidence in court. To be accepted the electronic audit trail must also be available.

If you have a document management system you should store relevant emails together with other correspondence and treat it in exactly the same way.