ELECTRONIC COMMUNICATIONS POLICY

1 INTRODUCTION

This Practice Note provides Members with a guideline of what is acceptable practice when using the firm's electronic communications system. Originally drafted following an Employment Court case where staff members were dismissed on the basis of inappropriate and damaging use of electronic mail (Email) (see Appendix 1), this practice note has been updated to capture current policy around useage.

Having a policy on the use of Email and the use of a computer network in general, is a vital part of a firm's Quality Management System. It must be accessible and made clearly available to all staff members who use computers and Email. All staff must be willing to sign a statement to confirm they have read and understand the policy.

Staff will use Email and computers for personal communication in the same way that they may use the telephone. Because the electronic communications systems are a means of business communication, a policy around its use should clearly define employee's responsibilities.

2 CONTENTS

Every staff member who is given access to the firm's electronic communications system is responsible for using it in accordance with the firm's policy. This Practice Note outlines the areas that should be included within a Policy.

It should be noted however that it is a guideline only. ACENZ does not accept any responsibility for the completeness or suitability of these suggestions for any particular member's electronic communications system.

2.1 Introduction

Some firms have a combined Electronic Communications Systems policy which incorporates the various forms of electronic communication, including but not limited to Email, telephones, video conferencing, voice mail, facsimiles, intranet and external Internet connections. Others prefer to make it more specific and have and company email and Internet use policy. An explanation of why there is an Email policy and who it applies to (presumably everyone).

> *The Policy applies to all users of John Doe Ltd's computer network including any person who may be working on contract to the firm and to any person who has been employed by the firm to work on the computer network.*

Identify where the Policy is located (i.e. as a part of your Quality Assurance documents)

This policy forms part of John Doe Ltd Quality Management System. The most up-to-date copy is located on File X.xx. A copy of the Guidelines to use of Email is posted on the notice board.

2.2 Violations of Policy

It is important to articulate the consequences of not complying with the Policy. It should simply state that any user who violates any part of the policy will be subject to discipline, up to and including termination.

2.3 Permitted and Non-permitted activities

Be as specific as possible. It may however be useful to have two tiers of Guideline here:

a) The formal Policy that sets out exactly what staff may and may not do;

b) Some quick-reference Guidelines on Email "etiquette"

Include the extent of the Policy.

For the purposes of this policy, Email includes any of the following services that Jon Doe Ltd may make available to you:

- *sending and receiving Email over the Internet*
- *using Internet Email to send or receive files or software*
- *using Email services such as mailing lists*

This policy also applies to the following services, which may be available to you:

- *access to the Internet*
- *Live messaging services*
- *etc… as appropriate to your network.*

2.4 Privacy Act

Make sure that *you* comply with the principles of the Privacy Act. Advise employees that the employer (or certain staff) may access all Email or may review backup facilities for the purposes of ensuring the Policy is adhered to (and for any other purpose that may be relevant). This may not stop someone writing to their mother but would probably deter them from sending defamatory material about their manager.

John Doe Ltd owns all rights relating to the network. Please note that John Doe Ltd has access to and may monitor all information on the network. This includes business file's personal files and Email messages.

By processing or storing any personal material on the network you accept that you are subject to this policy.

John Doe Ltd disclaims any responsibility for any loss or damage to personal files.

2.5 Acceptable Uses

these may include such as:

- Appropriate use for work – e.g. sending files and messages internally and to clients/colleagues
- Appropriate use for CPD – e.g. Internet learning resources

- As authorised by supervisory staff (provided it does not breach the un-authorised uses)
- It may include a statement about reasonable use for personal use, possibly with restrictions:
    - Unless it is unduly time consuming
    - Not during working hours
    - Not to prevent others using the network or not so it affects performance of the network
    - Limit on where personal files may be stored – e.g. a specific file location on a network, or on removable storage devices
- Company not to take responsibility for personal Emails
- Requirement to follow procedures or practice for opening and responding to Email (e.g. within two days)

2.6 Un-Acceptable Uses

These should be spelled out clearly. They may include:

- Not to use the network to create, store, access, display, copy or distribute material or a file, or send or solicit an Email, that is (or contains material which is):
- Defamatory
- Frivolous
- Harassing
- Objectionable
- Copyright, if you do not have a legal right to reproduce it
- Related to a business other than [the Company's] business
- Related to selling or marketing anything (unless connected to the business)
- Not send excessive amounts of Email
- Not to copy a file or an Email from the Internet unless:
- Required to do so in the course of your work
- In order to work at home, at another company office or at the offices of a client, for their work
- Unless expressly authorised to do so by the Network Manager, not to:
    - Install software on the network
    - Copy software off the network
    - Must not breach the terms of any software licence (for example, using pirate software)
    - Release your password, or allow anyone else to discover your password
    - Must not access (or attempt to access) parts of the network or files which are not required as part of your job.
    - Must not use the network to access (or attempt to access) another computer, or files on another computer, that you are not authorised to access by the owner of that computer.
    - Not send any digital (or other) material to any other party that is not authorised by the firm, to receive it
    - Not send anonymous Email.
    - Not send Email when specifically request not to by the recipient
    - Not send Email which appears to the recipient to have been sent by someone other than you, unless authorised not do so by that other person.
- Not read (or attempt to read) Email another employee has sent or received unless:
    - They sent it to you or posted it to a newsgroup or service to which you have a right of access
    - They, their Section Head or your Section Head have authorised you to do so.
- Must not deliberately adversely affect (or attempt to adversely affect) the normal operation, performance or administration of the network.

- Must not allow the misuse of computer systems by others.
- You must not use the network to gamble or do anything which is illegal.

Although the above are mostly common sense, they must be included in the Policy and read by staff to be defensible.

Staff may be limited to sending personal messages – for example only outside office time, or by ensuring the message is identified as a personal (i.e. not company) message.

3 RESPONSIBILITIES

3.1 Staff Responsibilities

Set out rights to a personalised Email address

> *All rights relating to the Internet/Email address that John Doe Ltd has established for you are owned by the John Doe Ltd. You may only use that address while you are employed by John Doe Ltd. If you leave employment John Doe Ltd has no obligation to allow you use of that address and has no responsibility to forward or reply to personal Internet Email sent to you.*

Advise staff that you are not responsible for the contents of any Email sent to them nor the contents of any newsgroup posting read.

Include a procedure or practice that requires staff not to send *confidential or commercially sensitive* material by Internet Email (unless it has been encrypted). This would probably apply to formal approvals, contractors etc.

It may also (or alternatively) be appropriate to include a confidentiality notice to outgoing Email, such as on the foot of a fax form (see also Practice Note on Transfer of Data, B42).

3.2 Accepting Responsibility

As for procedure under the Health and Safety Act, you should ensure that all staff read and sign off as having read, understood and accepted the Policy.

4 GUIDELINES

The following are guidelines, which essentially follow the principals of a policy as described above, but appear less threatening than “thou must not” statements. They are short and can easily be posted above each station.

GUIDELINES FOR USING EMAIL

John Doe Ltd allows you to use its network and Email systems. By using these you have agreed to comply with these Guidelines and the company’s Email Policy which you have signed as read.

COMPANY USE	The Email system is primarily for company business Minimal personal use is tolerated but should be kept to reasonable limits as stated in the Policy
WRITING MESSAGES	Emails are a form of communication with your clients. Write your Emails as you were writing a letter or fax. **Do not include jokes, or frivolous material in your Emails. Check your spelling.**
REPLYING TO MESSAGES	Be selective to whom you send Emails. They can readily be forwarded or re-distributed. Do not forward an Email without checking any attachments.
RECORDS	Emails that contain material to clients or contain information such as quotes, should be printed out and filed. Note that this includes Email messages that you have *sent* as well as *received*
JUNK MAIL	All forms of junk mail are considered a misuse of the Email. Do not circulate junk mail received
EMAIL TO ALL STAFF	Email to all staff should be at the discretion of the Computer Services manager *[this policy varies widely in the writer's experience]*
PRIVACY	All Email can be accessed by the Network administrator and may be checked for misuse of the Policy. Note that if your computer is attended or not adequately password protected, other network users could access your Email – take steps to ensure confidentiality
CONFIDENTIALITY	Do not send confidential information or files by Email [or – Only end confidential information or fields by Email if it has been encrypted – refer to Network administrator]
DEFAMATORY MESSAGES	You must not send Emails that could reasonably be construed to be defamatory, harassing, objectionable or illegal to any other address. You must not send such messages under any other user's name and/or address. You should report any such messages that you received from any other staff member
SENSITIVE INFORMATION	No commercially sensitive information should be sent by Email. Email or copies of material must not be sent to people who are not entitled to receive it.

5 ACKNOWLEDGEMENTS

This Practice Note has been prepared by referring to two Members' Email Policies (both of which included all the above points) and to an article reproduced in the May 1997 edition of "Employment Today". Acenz has implemented a Policy within its own office.

- -

APPENDIX 1
CASE STUDY: DISMISSAL DUE TO UNACCEPTABLE USE OF EMAIL

The convenience of Email has resulted in it becoming a common workplace communication tool. However as it has grown in use, it has also become the centre of a debate over the extentd to which employees should have free and private use of their employer's Email system.

Although some employees consider personal Email their private property, ACENZ would consider that when received at a work place, it is only private property in as much as would be private telephone call or private letter. Most employers are reasonable in allowing an employee the occasional private call or letter.

However when the communication deals in illegal material (eg pornography) or offensive material (e.g. discriminatory as under the Human Rights Act), then it becomes a different matter.

The case described below relates to *Clarke v Attorney General* in 1997.

The employer's Email Policy included the following points, which had been made clear to staff during a training course:

- Email was a business tool for exchange of information
- An electronic notice board was available for public messages
- Offensive language was not to be used on the Email

Three employees were dismissed on the basis of misuse of Email:

- One after sending over 600 non-work Emails over a period of two months – he had previously been warned regarding misuse of Email
- Two others exchanged derogatory messages about their manager
- One of these used another employee's PC to send a pornographic Email

The three staff subsequently took a case of wrongful dismissal to the Employment Court claiming that they had been treated differently from others, and that the Policy had not been presented to them in such a way as to make it clear that a breach could result in summary dismissal.

Although the Employment Court held that the dismissals had not been handled correctly, the employees were ultimately unsuccessful in their claim when the Court came to consider overall justice of the case.

The Court replied that *"those who seek equity must do equity, and … the plaintiffs have not done equity to the women of whom they have spoken in such condescending and disrespectful terms."*

The following points were cited by the Court:

- As public servants they were expected to maintain high standards of conduct [a situation that ACENZ would also expect of its members]
- The context of the messages was derogatory and breached the employer's code of conduct concerning sexual harassment
- Using another person's PC caused an innocent party to be seen as responsible
- They had been told not to use offensive language during the training course
- Messages could have caused harm to others
- The messages were written rather than oral and hence indicated a degree of "premeditation"
- The employees held front-line positions dealing with customers, some of whom were referred to in the messages.

- There was a risk that the attitude evidenced in the messages could be conveyed to the women referred to.

The case demonstrates that inappropriate use can be the subject of disciplinary procedures. The same considerations of fairness should be observed in any disciplinary action.

To minimise any conflict, a clear policy should be implemented.

[Comments based on an article in "Employment Today"]

APPENDIX 2
DEFINITIONS

The following definitions may be useful in defining a Policy

Defamatory means anything which may (or the Company believes may) injure the reputation of any person, company or other organisation.

Harassing means material which is (or the Company believes is) intimidating, hostile or offensive to another person. It includes:

- Sending Email to a person who has requested you not to do so
- Sending Email messages to a person that are unreasonably large or unreasonably frequent

it does *not* include one employee sending a message to another as part of the Company's usual supervision or disciplinary procedures.

Objectionable means anything which describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that its availability is likely to be injurious to the public good, or which the Company believes does nay of those things.

For the purpose of these guidelines, "objectionable" includes anything which:

- Is (or the Company believes is) sexually explicit
- Is (or the Company believes is) demeaning of any employee
- Promotes, suggests or encourages a criminal or unlawful act, or which the Company believes does aky of those things
- Suggests (or the Company believes suggests) that any employee (or class of persons that an employee belongs to) is inherently inferior because of their sex, marital status, religious belief, ethical belief, colour, race, ethnic or national origins, disability, age, political opinion, employment status, family status or sexual orientation
- Is deemed to be objectionable for the purposes of the Films, Videos and Publications Classification Act 1993

Personal Email means an e-mail that you send or receive and which does not related to your job.

Personal File means a file that you can create using the network or comply on to the network that does not relate to your job.