# South Derbyshire District Council

# ELECTRONIC COMMUNICATIONS POLICY

## (INCLUDING TELECOMMUNICATIONS)

March 2003

Version 1.4

CONTENTS

## 1. INTRODUCTION

1.1 South Derbyshire District Council provides access to telephones, internal/external e-mail and to the Internet to help you do your job faster and more efficiently using the latest available equipment and software. This includes accessing up-to-the-minute government reports, downloading the latest software updates, researching particular products or subjects, and communicating electronically with colleagues inside and outside the Council.

1.2 The facilities to provide this access represent a considerable commitment of Council resources on telecommunications, networking, security and software. Access to the Internet means we have to protect the Council's systems and data from unauthorised external access by controlling and monitoring through computer 'firewalls', e-mail and telecommunications monitoring software.

1.3 Because of the risks associated with the Internet, the Council has to take special care to maintain the clarity, consistency and integrity of its image. Anything any employee publishes on the Internet could be construed as representing the Council's corporate position.

1.4 It is important that users understand the potential for making the most of the Council's IT equipment and systems. However, it is also important that users understand their rights, their responsibilities and the limitations on the use of that equipment and those systems. This document, therefore, includes the Council's policy and best practice guidelines on the use of electronic communications. It clearly defines the conditions when using any of the telephony or Internet facilities including e-mail, the world wide web – www, and the internal e-mail system and explains what you are allowed to do and what you are not allowed to do.

1.5 Although the purpose of this document is to help users, refusal to accept and implement the procedures outlined may result in restricted access to electronic communications (email, internet, telecommunications access) and could result in certain services being withdrawn from individuals.

1.5 The Council, in consultation with the recognised Trade Unions, have agreed this document. It may need to be amended in response to changing circumstances as Internet facilities etc develop. The contents of this document may, therefore, be reviewed at any time in consultation with the recognised Trade Unions.

## 2. THE LAW

2.1 This section gives brief information of some of the laws that may be applicable to computer use. Further information should be sought from either Legal Services or Personnel and Development.

2.2 The various pieces of legislation briefly described below covers:

- The contents of e-mail.
- Downloading information from the Internet.
- Privacy issues.

- Monitoring of communications and surveillance at work.
- Several aspects of employment relations.

**Rules of discovery**

2.3 Parties subject to legal action are entitled to inspect and copy electronic documents relevant to the action.

**Human Rights Act 1998**

2.4 This provides for the concept of privacy giving a "right to respect for private and family life, home and correspondence". This provision is directly enforceable against public sector employees. Case law suggests that employees have a reasonable expectation of privacy in the workplace.

**Regulation of Investigatory Powers Act 2000**

2.5 This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications.

2.6 There are two areas where monitoring is not unlawful. These are:

- Where the employer reasonably believes that the sender and intended recipient have consented to the interception.
- Without consent the employer may monitor in the circumstances set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

**Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

2.7 The employer may monitor communications in the following circumstances:

- To ensure compliance with regulatory practices e.g. Financial Services Authority requirements.
- To ensure standards of service are maintained e.g. in call centres.
- To prevent or detect crime.
- To protect the communications system. This includes against unauthorised use and the introduction of potential viruses.
- To determine the relevance of the communication to the employer's business i.e. picking up relevant messages when someone is away from work.

2.8 Employers are expected to make all reasonable efforts to ensure system users know that communications may be intercepted.

**Data Protection**

2.9 The Data Protection Act 1998 covers information held in electronic form about individuals. It is a criminal offence to collect and process personal data on your PC unless the use is registered with the Data Protection Commissioner. Details of registration should reflect Internet use. The Legal & Democratic Services Manager has copies of all the Council's Data Protection registrations and can give you advice.

2.10 The Data Protection Act 1998 considerably increases the obligation on users of personal data, such as:

- banning sending personal data to non-European Economic Area countries with inadequate protection for data subjects
- prohibition on processing certain 'sensitive data' such as someone's marital status or ethnic origin.

2.11 A Code of Practice has been published by the Information Commissioner concerning monitoring at work. This helps to clarify the monitoring and retention of records of e-mail and telephone communications. Relevant benchmarks in the Code can be cited by the Information Commissioner in connection with any enforcement action being taken. The Code suggests that any monitoring of e-mails should only be undertaken in circumstances where:

- It is for a specified business purpose.
- Employers make an assessment of the risk they want to avert.
- Monitoring is targeted and blanket monitoring is avoided.
- The level of monitoring adopted minimises the level of intrusion into the individual's privacy.

**Discrimination Law (sex, race, disability) and Protection from Harassment Act 1997**

2.12 E-mail communications and the downloading of inappropriate images/material from the Internet may contain language or graphics that are insulting, demeaning or unlawful. Whilst the perpetrator of the message or download may be legally liable for the damage caused, the employer may also have vicarious liability for the action of the employee.

2.13 As with any form of harassment under the anti-discrimination legislation, the intention of the perpetrator is irrelevant. It is the perception of the recipient that is important. The problem with e-mail is that, with the lack of visual cues, offence may be caused where none was intended.

**Defamation Act 1996**

2.14 The liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the Internet will be responsible for it and liable for any damage it causes to the reputation of the victim.

2.15 In addition to the liability of the individual who made the libellous or false statement, the Council may also be held liable. This could be either under the normal principles of:

- **indirect** liability because the Council is considered responsible – known as 'vicarious liability'
  or
- **direct** liability as a publisher because of providing the link to the Internet and e-mail system.

2.16 An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

2.17 Do not put anything in an e-mail, or an attachment, which you would not put in a normal letter on Council headed paper. Treat e-mail as you would a postcard going through the open post.

**Contract Law**

2.18 E-mail is generally regarded as an informal means of communication but it is, nevertheless, capable of creating or varying a contract in just the same way as it is orally or in writing. Employees need to be aware of the danger of inadvertently making contracts on behalf of the Council, or varying the terms of any existing contract.

**Copyright**

2.19 Although any material placed on the Internet or in public discussion areas is generally available, the originator still has moral and, possibly, legal rights over it. You should not copy it without acknowledging the original source and, where appropriate, gaining their permission. This applies even if you modify the content to some extent.

2.20 You should not forward anything sent to you personally to others - particularly to discussion areas - without permission from the originator.

2.21 Copyright and other rights in information posted to the Internet, like anything else you produce at work, belongs to the Council and not to you personally.

2.22 Copyright laws are different for each piece of software. In general, the copyright to every piece of software run on a system is owned by whichever company or person wrote it. The Council has a legal duty to make sure sufficient licenses of the correct type are present to cover the use of all software. You must be aware of these issues and make sure that the Council has correct licences for any software you are using.

**Obscene Publications Act 1959**

2.23 Publishing legally "obscene" material is a criminal offence under the Obscene Publications Act 1959. This includes electronic storing and/or transmitting

obscene materials e.g. the downloading of certain images from the Internet might subject an employee to charges of criminal behaviour.

**Computer Misuse**

2.24 The Computer Misuse Act 1990 covers unauthorised or malicious use of any computer system. It is the law used to prosecute hackers and people who write and distribute computer viruses deliberately.

2.25 It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access. This law protects against employers and members of the public who deliberately cause damage to systems or data. The Act also makes it illegal for an employee to deliberately delete data or sabotage systems to the detriment of the Council.

**Disclaimer**

2.26 Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the Council.

Always remember that any statement you make may still be construed as representing the Council.

## 3. SCOPE OF POLICY AND "BEST PRACTICE" GUIDELINES

3.1 This policy and the accompanying guidelines on best practice apply to all councillors, permanent and all temporary council employees, agency staff, contractors and sub contractors when working on South Derbyshire District Council's premises or using South Derbyshire District Council's equipment at home, or elsewhere.

## 4. RESPONSIBILITIES

**General**

4.1 Whilst the electronic communications offers many benefits, it can also present some significant risks to our systems and data if all users do not follow appropriate security procedures. Security must be a key concern for everyone. As use of the Internet and external e-mail expands within the Council, we all need to be fully aware of our responsibilities and what restrictions are placed on its use.

**Implementing the policy**

4.2 It is the responsibility of the Chief Finance Officer (and representatives) to:

- Ensure that this policy and guidelines are properly implemented.
- Keep this policy and guidelines up to date.
- Ensure the security of the Council's electronic communications systems.

- Monitor the Council's electronic communications systems and to report possible breaches of policy and problems.
- Liaise with Personnel and Development to ensure that the policy and guidelines (including amendments) are communicated to employees.
- Liaise with Personnel and Development should any training issues arise from this policy and guidelines.

**Employee's Responsibility**

4.3 Employees are required to comply with this policy and the associated guidelines on the use of telephones, e-mails and the Internet. It is part of your conditions of employment. It is, therefore, important that you read and consider this policy and the guidelines carefully. If you are unsure or fail to understand any part of it, it is your responsibility to ask your manager/supervisor to explain.

## 5. MONITORING OF COMMUNICATIONS

5.1 You need to be aware that the Council monitors all use of the Internet and logs and retains the records. We record or monitor:

- Details of web sites visited or attempted to be visited.
- Pages accessed.
- Files downloaded.
- Graphic images examined.
- E-mail correspondence.
- Any file attachments (e.g.: pictures or word documents).

The Council also scans for any potential viruses within any e-mail and Internet traffic passing within or outside the Council's systems.

5.2 The council also has the capability to monitor and record telephone calls and where the need has been identified this is done. Logs are kept of telephone calls and these may be checked.

## 6. MISUSE OF THE E-MAIL SYSTEM OR INTERNET

6.1 Any misuse of the telephone, Internet or e-mail system is considered to be a disciplinary offence by the Council. Misuse includes:

- Breach of confidentiality.
- Breach of security rules/guidelines.
- Sending inappropriate messages, for instance any that might cause offence or harassment on the grounds of gender, race, disability age religion etc.
- Deliberate accessing of offensive, obscene, or indecent material from the Internet, such as pornography, racist or sexist material, material likely to incite criminal behaviour.
- The importation of viruses through unauthorised downloading of files and programmes from external sources.
- Unreasonable use of the telephone system for private use.

This is not an exhaustive list.

6.2 Allegations of misuse by an employee of the Council will be will be investigated in accordance with the Council's Disciplinary Procedure and may lead to disciplinary action. Any misuse by agency staff, contractors, or sub-contractors will be referred to their employers.

## 7. PERSONAL USE OF THE COUNCIL'S TELECOMMUNICATIONS SYSTEM

7.1 For people working at Council premises who are directly linked into the Council's network, the Council allows reasonable, occasional personal use of telephone, Internet and the e-mail systems provided this personal use complies with all the requirements of this policy and associated guidelines. Personal use for employees is not allowed where that would involve any direct cost to the Council, such as dialling into the Council's network. This may be in such instances as using an external telephone (ie: home) to access computer services as this can involve costs using the Council's telephone system.

7.2 Reasonable occasional personal use is permitted provided that it:

- does not breach any of the provisions in paragraphs 7.1 and 9.1
- does not involve misuse of the Council's system (see paragraph 6.1)
- is not detrimental to corporate interests
- does not cause any disruption, disturbance, inconvenience or degradation of the service
- does not interfere with the work of the Council
- does not interfere with other employees doing their jobs
- is done outside your working hours - meaning before or after work, during your lunch break or during your flexi-time.

7.3 Any messages or information you send to someone outside the Council, are statements that reflect on the Council. This is either in a personal capacity or on business use, through an electronic network such as bulletin boards, on-line services or the Internet. Wherever appropriate, you must make it clear that the views expressed are personal and may not necessarily reflect those of South Derbyshire District Council.

7.4 You must not use anonymous mailing services to conceal your identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details.

7.5 Further guidance on the use of the Council's telephone system is included in Appendix 3 – Telecommunications Guidelines.

## 8. FURTHER INFORMATION

8.1 If you have any questions about access to the telephone or e-mail systems, or the Internet, or want copies of any other Information and Communications Technology security-related documents, please contact IT Services or a relevant departmental representative as outlined in Appendix 3 of this document.

## 9. GENERAL CONDITIONS – TELEPHONES, E-MAIL AND INTERNET

9.1 You must not use the Council's Internet access, telephone or e-mail systems for knowingly doing anything which is illegal under English law, or the law of any other relevant country, or for any of these purposes:

- promoting any commercial ventures, causes or organisations unless specifically authorised to do so by your Chief Officer
- promoting any private or personal interests such as selling personal possessions / property, or promoting a social activity not related to the Council
- publishing any material that, in whole or in part, appears to be designed to affect public support for a political party. This could take the form of political publicity, campaigning or lobbying
- sending, accessing, retrieving or storing any communications of a discriminatory or harassing nature, or materials that are offensive, obscene, pornographic, sexually explicit or which incite or depict violence
- using or transmitting abusive, defamatory, libellous, profane or offensive language
- describing techniques for criminal terrorist acts
- representing values which are contrary to any Council policies
- breaking through security controls, whether on the Council's equipment or on any other computer system
- intentionally accessing or transmitting computer viruses and similar software
- intentionally accessing or transmitting information about, or software designated for, breaching security controls or creating computer viruses
- knowingly, any activities that could cause congestion and disruption of networks and systems.

## 10. E-MAIL GUIDELINES

### E-mail address

10.1 Just like your phone number, your e-mail address uniquely identifies you from the millions of other users on the Internet and lets them send e-mail to you. The Council has adopted a standard lower case format for its e-mail addresses. If you have access to the internal e-mail system, you will also have an Internet e-mail address, which looks like this:

firstname.lastname@south-derbys.gov.uk

### Security and disclaimer

10.2 E-mail communications are not secure and you should not use e-mail to transmit private and confidential, personal or other sensitive information. In addition to the message referred to in paragraph 7.3, you should also, where appropriate, use a disclaimer saying ...

*The views expressed in this e-mail are personal and may not necessarily reflect those of South Derbyshire District Council, unless explicitly stated otherwise.*

*This e-mail and its attachments are intended for the above named only and may be confidential. If they have come to you in error you must take no action based on them, nor must you copy or show them to anyone; please reply to this e-mail and highlight the error.*

**This disclaimer is attached automatically on external e-mail.**

10.3 You must not send or knowingly open external personal e-mail during your working hours but you can do so before or after work, in your lunch break or when taking flexi-time.

10.4 E-mails to be circulated to all personnel & members of the Council (i.e.: 'All User' e-mails) should only be sent out with the agreement of your line manager, divisional manager or overall departmental head. E-mails of this type should not be used for personal matters.

10.5 Each one of us is responsible for the content of all text, audio or images that we place or send over the Council's e-mail system. You must not send e-mail, which hides your identity or represents the sender as someone else. All messages must contain your name.

10.6 Your system password(s) must be kept confidential and NOT shared.

10.7 You must not read, delete, copy or modify the contents of anyone else's mailboxes without their consent.

10.8 If you have the facility on your e-mail software, you must use 'AutoSignature' facility on your PC – which you will find in the 'Tools' menu - when sending external e-mail. In the interests of presenting a uniform corporate image this is the suggested format you should use ...

| | |
|---|---|
| Name | **Carl Veal** |
| Job title | **Networks/Systems Support Analyst** |
| South Derbyshire District Council | **South Derbyshire District Council** |
| E-mail | **carl.veal@south-derbys.gov.uk** |
| Tel +44(0)1283 tel number | **Tel +44(0)1283 595889 (Direct Line)** |
| Fax +44(0)1283 fax number | **Fax +44(0)1283 550128** |

## 11. INTERNET GUIDELINES

11.1 The Council uses special monitoring and control software for network connections to prevent access to the majority of undesirable sites. However, it

cannot always prevent access to all such sites because their design is ever changing. If you do accidentally access and/or download unsuitable material, you must disconnect from that site immediately and inform IT Services. This is both to protect yourself and so we can add it to the list of unsuitable sites. No action will be taken for genuine accidental access of such material and we will then immediately include such sites in the Council's 'filtered' lists.

11.2 Users of stand-alone connections must be aware of their responsibilities not to access undesirable sites.

11.3 You must not use the Council's Internet facilities to deliberately spread any virus, worm, Trojan horse, or trap-door program code or any other code or device that could cause disruption to the Council's or other people's networks and systems.

11.4 You must not knowingly use the Council's Internet facilities to disable or overload any computer system or network. You must not attempt to disable, defeat or by pass any systems intended to protect the privacy or security of another user, including the Council's firewall security systems.

11.5 No networked user may install additional Internet or e-mail related software, or change the configuration of existing software, without authorisation from IT Services Officer. This includes software and shareware available without charge or on a free trial. Most systems are however, disabled from being able to do this.

11.6 To help prevent unauthorised users from gaining access to the Internet, don't leave connections unattended for any length of time. During short periods of necessary absence, use a password protected screen saver if you work in an area where unauthorised users could easily access your PC.

11.7 Line Managers, Divisional Managers and Departmental Heads are responsible for immediately informing IT Services of any Internet users who no longer require their Internet access or e-mail for any reason.

## 12. FINANCIAL TRANSACTIONS

12.1 Although some organisations accept orders and payments for goods and services on the Internet, it is not generally the Council's policy to do this. Current views are that it is still not suitable for the conduct of secure financial transactions and you must not use it for this or for ordering goods and services without prior authorisation from IT Services. However, we will be introducing this as part of the drive forward on e-commerce once legislation and financial regulations have been amended.

## 13. VIRUS PROTECTION

13.1 You must comply with the Council's Virus Protection Policy.

13.2 Virus growth is accelerating at the rate of 35-400 new viruses each month. At the end of 1997 the number was estimated at 11,000. The most common

causes of virus transmission are through receipt of e-mail attachments, transfer of files via floppy diskette and downloading of files from the Internet.

13.3 The Council has installed a comprehensive virus scanning package which includes software designed to intercept any viruses in e-mail attachments, files downloaded from the Internet or discs loaded from external sources.

13.4 You are responsible for making sure that all data you send is virus free.

13.5 You can only run software that is approved. The Council's IT Services department, as part of a regular routine will audit all system to make sure that no unauthorised software has been loaded.

13.6 You are not permitted to load software applications directly on to any of the Council's systems. This may only be done by IT Services approved personnel, e.g. the Network Administrators.

13.7 IT Services will ensure that all data held on council servers is backed up. You are responsible for any data held locally on their systems. If you wish to have any data backed up then you must use the current backup procedures applicable to ensure your data is saved via a daily server backup. If you store data directly on your local workstation's hard drive then it is highly unlikely to be recovered in the event of the workstation having to be re-built. If you are unsure what the procedures are for saving your local data, please contact a member of IT Services for assistance.

13.8 Anti-virus software is deployed on all workstations, used within South Derbyshire District Council. You are not permitted to change the set up of this software.

13.9 You must notify the IT Services if your system reports the presence of a virus and must not switch off the system or attempt to delete the infected file until remedial action has been taken by IT Services personnel.

13.10 You must make sure all files, programs and e-mail attachments that you want to download have been virus scanned.

13.11 You must immediately report any incidents about virus detection in Internet files and/or e-mail attachments to the Senior IT Officer in IT Services.

## 14. DOWNLOADING AND UPLOADING FILES

14.1 You must only download software from the Internet for direct business use and with prior authorisation from IT Services. You must arrange to have downloaded software properly licensed and registered where required. You must not break copyright laws.

14.2 You must not knowingly use the Council's Internet facilities to download or distribute pirated software or data.

14.3 You must not use Internet facilities to:

- download entertainment software including games
- play games against opponents over the Internet

- download images or videos unless there is a clear business-related use for it.

14.4 You must not put on to the Internet, any Council data, which is not in portable document format (ie: a Word document or a pdf document for Acrobat Reader), or in a public document without clear authorisation from your Chief Officer.

14.5 Any data must be scanned to make sure it is virus free and only place it on the approved site and location. In most cases, data brought into the Council will be automatically scanned but if you are unsure then you must contact a member of IT Services for advice.

14.6 You must not download, copy or transmit to third parties the works of others without their permission as this may infringe copyright and the Data Protection Acts.

## 15. INTERNET NEWSGROUPS AND BULLETIN BOARDS

15.1 You need your manager's prior written permission before you subscribe to any bulletin boards, newsgroups or any other Internet service of any kind.

15.2 Approved newsgroup users may offer information and advice to others if that is appropriate to their job, or if it represents a reasonable return, in terms of effort involved, for the value they receive from the discussion. You must not offer help in areas, which are clearly the responsibility of someone else within the Council. Redirect or pass on enquiries to the appropriate person.

15.3 You must not participate in discussions that are politically sensitive or controversial, whether nationally or locally, and must not give advice or information, which you know to be contrary to the Council's policies or interests.

15.4 Remember that newsgroups are public forums. You must not reveal any confidential Council or service user information

## 16 COUNCIL WEB SITE

16.1 The Council has a corporate Internet site, which will provide information about all its services.

16.2 No part of the Council may establish a separate Internet site unless this is formally authorised by the Council or Chief Executive.

16.3 Each service page on the web site is the responsibility of a named person who will update it on an agreed frequency.

16.4 IT Services must approve any major new additions to information before it is put on the site.

16.5 As the web site develops, further additions will be made to this section

## 17. TELEPHONE USE GUIDELINES

17.1 The council provides telephone and mobile phone equipment to help employees conduct their council roles.

17.2 The telephone system also has the capability to record telephone conversations and logs of calls made/received, and in some sections this is practiced. Your manager or union representative should be able to confirm if this is carried out in your section. Recording of telephone conversations may be carried out for the following reasons:

- To ensure the integrity and quality of information is to an agreed standard.
- For training purposes for dealing with specific queries from the public or handling difficult calls.
- For security to ensure that staff and customers are treated fairly in the unexpected instance of disputes.
- To systematically check call logs eg: to detect use of premium-rate lines.

17.3 Where telephone monitoring is carried out, recordings will be held in secure storage with only authorised personnel having the relevant responsibilities given access.

17.4 Further guidelines are provided in Appendix 3.

# E-MAIL GUIDELINES

These guidelines apply equally to internal and external e-mail.

If you use the e-mail system, you must follow the requirements of the User Policy and these guidelines.

**Never . . .**

1. Use the e-mail system for knowingly doing anything illegal under English law, or for any of the purposes set out in paragraph 2.1 of the Internet and E-mail User Policy.

2. Transmit confidential, personal or other sensitive information on e-mail unless you can apply appropriate 'encryption' - putting messages into code - to protect it. Specifically, don't use e-mail for:

   - appointment letters
   - acceptances of appointment
   - receipt or authorisation of payments
   - legal notices
   - disciplinary notices
   - sickness certification
   - personal information about employees or service users

   unless you send it in a Word document, 'password protect' it and telephone the recipient to give them the password.

3. Abuse others - even in response to abuse directed at you.

4. Use e-mail to harass or threaten other employees, service users or anyone in any way.

5. Use anonymous mailing services to conceal your identity or falsify e-mails to make them appear to originate from someone else.

6. Access anyone else's mailbox unless they have given you proxy or authorisation rights. Unauthorised access is a breach of security.

**Don't . . .**

7. Use the 'Reply All' function unless everyone in the original message needs to know your response.

8. Print out messages unless they are really important.

9. Send large e-mails or attachments. It's not an economical or sensible way to handle large documents. It can halt the e-mail system.

10. Create e-mail congestion by sending trivial messages or by copying e-mails to those who don't need to see them.

11. Send out 'All User' messages without first obtaining authorisation from your Line or Divisional Manager.

12. Forward confidential or restricted items on e-mail sent to you personally without the originator's permission.

**Remember . . .**

13. E-mails may be read by a far wider audience than originally intended, because of the ease of forwarding messages to new recipients.

14. E-mail is not guaranteed to arrive at its destination within a particular time, or at all.

15. Not to send a message in capital letters. It is the electronic version of **shouting**.

16. Always put appropriate disclaimers on your messages.

17. Any advice you give on e-mail has the same legal standing as any other written advice.

18. Before sending an e-mail, ask yourself how you would feel if your message was read out in Court.

19. Not to assume that the message has been read just because it has been sent.

20. You can make reasonable occasional personal use of the system - see paragraph 2.3 of the E-mail and Internet User Policy.

21. Avoid sending graphics - it may look nice but it takes up valuable computer storage space and increases processing time.

22. It's easier to change and distribute messages and documents in the e-mail environment than it is in a purely paper-based one. Use these two categories to indicate the confidentiality of the message or document being sent. Put the category at the start of the 'subject' line. Most messages and their attachments don't need a confidentiality status. If no category is given, the assumption is that the message and/or document has no confidentiality status and can be changed and forwarded as required.

    **Confidential** Message and/or document marked 'confidential'. This should not be freely copied. Distribution should be limited to a 'need-to-know' basis.
    **Restricted** Message and/or document marked 'restricted'. Printing, copying and distributing of the document should be closely monitored by the originator and the recipient, and should not happen without the originator's consent. Editing should only be done with the originator's consent.

**Do . . .**

23. Maintain your e-mail mailbox properly:

    - open all e-mails at least daily or make sure that an `out of office' message or re-direction is set up if you are away from the office for more than a day. If the system you are using can't do this, you must authorise a colleague to send a reply back stating that you are unavailable
    - only keep messages that are necessary for current business needs
    - store all e-mail messages necessary for permanent business records in your personal folders according to current record retention policies
    - delete insignificant, obsolete and unnecessary messages, return/read receipts and attachments, daily. Clear your `deletion' folder daily to get rid of unwanted items. We will eventually have an automatic system, which will clear your 'waste basket' of any mail, which is seven days old, and delete all unopened mail after 30 days.

24. Use a password protected screen saver if your PC is in an area where unauthorised users could easily access it.

25. Make sure you use the correct address when sending mail. If the e-mail fails to reach its destination, it may be lost or fall into the wrong hands. Double check the address when you send important messages.

26. Always get confirmation of receipt for important e-mails.

27. Make and keep hard copies of very important e-mails sent and received.

28. Reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will or should be sent.

29. Only print an e-mail if you need a hard copy for filing - don't waste paper.

30. Develop orderly filing systems for messages you need to retain.

31. When responding, concern yourself only with your response. Don't reproduce the message sent to you unless it is really necessary. This makes messaging more effective and conserves network resources.

32. Keep messages brief and to the point. Some people find it harder to read from the screen than they do from paper.

33. Always enter a subject title to your e-mail. Make sure that the 'subject' field of the message is meaningful. This helps everyone file and search for their messages more effectively.

34. Try to use one message for one subject. Multiple subjects within a single message make it difficult for the recipient to respond effectively, and to file the message.

35. Think whether all your intended recipients really want or need to receive the message and any attachments.

36. Make use of the bulletin board we will be providing on the Council's Intranet.

**If in doubt . . .**

Contact:

The Networks and Operations Manager, IT Services
Telephone Extension 5785
or

The E-Government & IT Strategy Manager, IT Services
Telephone Extension 5889

**APPENDIX 2**

# INTERNET GUIDELINES

If you use a connection to the Internet, you must follow the requirements of the User Policy and these guidelines.

**Never . . .**

1. Use the Council's Internet access for knowingly doing anything which is illegal under English law, or the law of any other relevant country, or for any of the purposes set out in paragraph 2.1 of the E-mail and Internet User Policy.

2. Divulge personal information such as addresses and telephone numbers over the Internet.

3. Use the Council's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

4. Knowingly use the Council's Internet facilities to disable or overload any computer system, network, or equipment or attempt to disable, defeat or circumvent any systems intended to protect the privacy or security of another user, including the Council's 'firewall' security systems.

**Don't . . .**

5. Leave Internet connections unattended for any length of time - use a password protected screen saver if you work in a vulnerable area.

6. Release protected information through a newsgroup or chat line - whether or not the release is inadvertent, it comes under all the penalties under existing data security policies and procedures.

7. Order or pay for Council goods and services on the Internet.

**Remember . . .**

8. You can make reasonable occasional personal use of the Internet - see paragraph 2.3 of the E-mail and Internet User Policy.

9. You must not provide false information to any Internet service which requests name, e-mail address or other details.

10. If you accidentally access unsuitable material, you must disconnect from the site immediately and inform the senior officer in IT Services.

**Do . . .**

11. Only use Internet browser software provided and configured by the Council, and only use officially provided access mechanisms.

12. Restrict your work use of the Internet for research and information, which directly relates to your job.

13. Immediately report any security problems or breaches to the systems administrator and/or your line manager.