Internet and Electronic Mail

Code of Practice

Issued by: Sarah Bryant:- Head of Information Management & Technology
March 2005

The London Borough of Barking & Dagenham

www.barking-dagenham.gov.uk

COUNCIL CODE OF PRACTICE FOR INTERNET USAGE

Table of Contents

Page

COUNCIL CODE OF PRACTICE FOR INTERNET USAGE

SUMMARY

Purpose

This document details London Borough of Barking & Dagenham's policy on using the Internet and electronic mail (e-mail) services.

It describes what the services provide, what is good practice when using them and what is prescribed and must be avoided.

This Code applies to usage of the Council's Internet and e-mail services from whatever source – i.e. from laptops and PCs used remotely as well as from office workstations.

Responsibilities

It is the responsibility of **ALL** users of the Council's Internet and e-mail services to read, understand and comply with the contents of this Code of Practice and to use the facilities provided by these services in an acceptable and appropriate manner.

Managers are responsible for monitoring compliance with this Code.

Although the Code is written in a form that is directed at employees, the Code also applies to Members. Particular attention is drawn to Sections 10.2 and 20.2 and the monitoring arrangements in Section 9.

The Information Management & Technology Department is responsible for issuing this Code and reviewing it annually.

NB. Words that are underlined within sentences denote a link to other documents or information that is on our internal Intranet. Therefore, if you are viewing this document on your PC you can click on these items to immediately view further relevant information.

Monitoring

The Council will conform with the relevant legislation in force at the time, governing the use and monitoring of e-mail and the Internet, which principally involves: the Human Rights Act 1998, the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, Telecommunications (lawful business practice) (interception of communications) Regulations 2000 and The Freedom of Information Act 2000.

The Council reserves the right to monitor, at any time, all Internet usage, (including browser history files, storage of temporary Internet files and any downloads from an Internet site) and e-mails, including deleted e-mails, and the systems upon which such e-mails are stored and circulated. This right is reserved solely for the purpose of monitoring Internet usage or communications for business purposes as set out below.

The Council exercises the right to intercept e-mails and Internet access under the Telecommunications (lawful business practice) (interception of communications) Regulations Act 2000 (the Regulations) for the following reasons:

(i) to investigate or detect the unauthorised use of the systems, including that the provisions contained in this Code of Practice are being observed;
(ii) that no discriminatory or offensive content appears in e-mails, etc;
(iii) to maintain an adequate level of security for our computer systems;
(iv) to detect any computer viruses; and
(v) to check mailboxes of absent employees.

To exercise its right under the Regulations the Council is required to make all reasonable efforts to inform every person who may use the system that interception may take place. We believe that the communication of this Code of Practice to all employees meets this requirement and we will ask each employee and Member to sign a recognition agreement that this policy has been explained to him or her.

An appropriate statement will also be included in any automatically generated 'signature' to outgoing e-mails.

The Council is conscious of its obligations under the Data Protection Act 1998 as information derived from the interception of communications is covered by the data protection principles. The Council will therefore observe the guidelines laid down in the Information Commissioner's Employment Practices Data Protection Code Part 3 "Monitoring at Work", which are as follows:

- The Council will not monitor the content of e-mail messages unless it is clear the business purpose for which the monitoring is undertaken cannot be achieved by the use of a record of e-mail and Internet access traffic. If the traffic record alone is not sufficient to achieve the business purpose any further monitoring will, as far as possible, be strictly limited and targeted.

- The Council will only conduct detailed monitoring where an impact assessment shows that monitoring is justified, particularly taking account of the privacy of those using the systems, including those sending e-mails to the Council.

- Wherever possible, the Council will avoid opening e-mails, especially ones that clearly show they are private or personal (business use).

COUNCIL CODE OF PRACTICE FOR INTERNET USAGE

- E-mail monitoring will be confined to address/heading unless it is essential for a valid and defined reason to examine the content.
- Where reasonable and practicable, and unless this is obvious, ensure that those sending e-mails to employees, as well as employees themselves, are aware of any monitoring and the purpose behind it.
- If it is necessary to check the e-mail accounts or Internet usage details of employees in their absence, make sure that they are aware that this will happen

COUNCIL CODE OF PRACTICE FOR INTERNET USAGE

1. Introduction

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Access to the Internet is available over the Council's corporate network; this will give employees access to: -

- Electronic mail communication with people all over the world;
- Information and news.

The London Borough of Barking & Dagenham believes that the Internet's resources should be available, on an authorised basis, to its employees as the facilities it provides open up opportunities for resource sharing, learning, innovation and communication. Furthermore, the Council believes that the Internet can be used to develop links with other councils, partners and appropriate organisations. The fundamental aim of providing Council employees and Members with Internet access is to support the business purposes of the Council such as researching topics or products, learning about new initiatives and technologies, using on-line resources or keeping up with developments in a particular field.

There are many issues regarding the use of the Internet in a business context. For example, it is very important for users to understand the security implications of using the facility and to understand that use of the Internet on behalf of the Council implies moral and ethical obligations. For these reasons and others this Code of Practice has been established to guide users of the corporate Internet facility. Ultimately, the effective operation and exploitation of the facility relies upon the proper conduct of the end users. The principles incorporated in this Code are intended to outline the way in which employees and Members are expected to conduct their use of the Council's Internet facility. This document deals with the following key issues: -

- Applications for Internet Access;
- Management Responsibilities for Supervision of Users;
- Representation of the Council;
- The Council's Websites;
- Guidance on Copyright Issues;
- Security;
- Responsible Use of the Internet;
- Monitoring of Use of the Internet;
- Inappropriate Use of the Council's Corporate Internet Facility;
- Disciplinary Action; and
- Further Information and Support.

2. Internet Access

Access to the Internet can only be made using the Council's contracted Internet Service Provider (ISP). All Internet access permissions will be set up by Information Management & Technology for individuals

- sign to show that they have already read and understand this Code of Practice.

3. Management Responsibility for Supervision of Users

Local management has a responsibility for supervising access to and use of Internet facilities in their area. The following points are intended to help guide the management of Internet usage within departments: -

- The connection to the Internet to conduct departmental business is a management issue and as such should be authorised by management.
- Managers and supervisors of users should be aware of their employees' Internet usage.
- The unregulated nature of the Internet has the potential for waste of employees' time and can be open to abuse. Managers should ensure that appropriate measures are put in place to minimise the opportunities for personal or inappropriate use.

4. Representation of the Council

When using the corporate Internet facility employees are representing the Council in an 'electronic community' and they leave electronic fingerprints wherever they go. The following points should be observed by all employees when communicating over the Internet: -

- All employees shall behave in a proper, ethical, and legal manner (please refer to Section 11 of this code) consistent with the Council's Employee Code of Conduct when they use the Internet.
- Only employees authorised to speak to the Media or other similar third party organisations shall do so using the corporate Internet facility.
- Employees should be aware that Internet communication can be used for committal, contractual or financial transactions involving the Council (e.g. placing orders, agreements, payments, etc). Only employees expressly authorised may use the Internet for these purposes and when doing so the Council's Employees' Code of Conduct, Contract Rules and Financial Rules must be adhered to.
- Users are expected to abide by the generally accepted rules of Internet etiquette. These include, but are not limited to, the following: -
    - Be polite - messages must not be abusive or offensive to others.
    - Use appropriate language - do not swear, use vulgarities or any other inappropriate language.

5. The Council's Websites

5.1 The Council's Internet Website

One of the primary functions of London Borough of Barking & Dagenham's Internet website is to be a communications channel between the Council, local residents and visitors to the Borough; through it the Council provides information on environmental, learning, social, cultural and tourism issues. The website will also enable the delivery of electronic services to the local community. The Education Department is responsible for the Intranet and Internet Web Site development.

The following points should be observed: -

- There will be only one **London Borough of Barking & Dagenham** Internet website (its address is http://www.barking-dagenham.gov.uk/ (although other areas do operate their own specific sites).

5.2 The Council's Intranet Website

The Council also operates an internal Intranet website http://lbbd/ providing information for employees and Members. It is structured with pages for News, Members and corporate and departmental matters.

- Individual pages on the Intranet have specific contact points for suggestions, comments and updates

5.3 Publishing on the Internet and Intranet

The creation of Internet and Intranet web pages is the responsibility of individual service departments. Each department has nominated a content Manager who has the facility to create pages of information relevant to their department's service areas.

The Education Department has overall responsibility for the website and drives its development. Along with the designated content managers, they authorise the publication of pages created by the content authors. A list of content authors and managers can be found under the A-Z of Services on the Intranet.

Ideas and requests for publication should be directed to the relevant content author. Individual pages on the Intranet and Internet have specific contact points for suggestions, comments and updates.

6. Copyright Issues

Copyright of information and resources found in the Internet is a serious issue with much being protected by copyright laws. The following issues are intended to inform users of their responsibilities with regard to copyright of information and software which may be obtained from the Internet: -

- It is the responsibility of all users to respect the legal protection provided by copyright and licence to programs, data and other information that may be accessible over the Council's corporate Internet facility.

- Do not download any software (executable program code) from the Internet.
- Users will not knowingly breach copyright laws.
- If in any doubt about copyright then contact Legal Services in the Corporate Strategy Department.

7. Security

The following points are intended to protect the user and the Council from security problems associated with the Internet.

7.1 Virus Protection (including worms, Trojans and blended threats).

Please be aware that viruses can be downloaded from the Internet unintentionally. Virus checking software is in place on the Internet connection to automatically check files that you download. This software does not provide a guarantee against virus infection and the risk should be minimised by only downloading business related material. The downloading of screen-savers, games, computer software or audio files is therefore prohibited.

If you are in any way unsure about what you are about to download from the Internet or believe that you have detected a virus, contact IT Support on 2013 for advice.

7.2 Information Security

Internet communication cannot be considered to be totally secure. It can be forged, monitored and tampered with. Users are advised of the following guidance to protect confidential and sensitive information: -

- It is the responsibility of all users to respect the privacy of other users and not to seek information pertaining to other users without their explicit permission. This includes, but is not limited to, personal data, passwords and access to confidential files or modification of files belonging to other users.
- Do not reveal your personal address or phone number or the addresses and/or phone numbers of colleagues because of the public nature of the Internet.
- People's names, addresses and financial details must never be passed or publicised without their express permission.
- Confidential corporate information must be dealt with appropriately. If you are in any doubt as to whether the information is unsuitable for distribution over the Internet, then contact the Council's Data Protection co-ordinator on extension 3351.

7.3 System Security

If a user finds that they are able to circumvent system security, users have a duty to inform Information Management & Technology so steps can be taken to immediately prevent further occurrences.

7.4 Workstation

The workstation being used for Internet browsing should be appropriately secured to prevent unauthorised access. All passwords should comply with the standard defined in the Council's Password Policy and screen savers should be password protected. While connected, the computer should not be left unattended for extended periods. Alternatively the workstation should be locked if left unattended by pressing Ctrl+Alt+Delete and selecting Lock Workstation or you should log off.

8. Responsible use of the Internet Facility

When using the Internet users are expected to behave in the following manner to ensure least disruption to others when using the Internet:

- Do not use the Internet in such a way that you would disrupt the use of the network by other users. This includes, for example, the downloading of large images or large files. If you are at all unsure about what types of activity will cause disruption, then contact IT Support – Ext 2013.

9. Monitoring use of the Internet

Employees should not expect privacy regarding their Internet usage. Inappropriate use of the Internet may result in embarrassment to, or legal action against, the Council and the employee. Every connection made on the Internet can be traced back to the originator leaving a trail of 'finger-prints' easily tracked by others. Therefore:

- Do not visit any sites where you are reluctant to leave your "fingerprint".

- Sessions on the Internet are logged automatically in exactly the same way that telephone calls are logged in the phone systems, therefore: do not use the Internet for tasks that you would not want logged.

The Council reserves the right to monitor all user Internet communications and examine all information collected, created and/or generated as a result of using the Internet including any files, messages, printouts, CD's, diskettes, tapes, memory sticks, or other material in order to monitor users' compliance with this Code of Practice.

Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this Code has occurred. Surveillance may only be undertaken where it has been requested by the relevant manager, Head of Service or Director for valid reasons, or where it is requested by either the Head of Audit or the Council's Whistelblowing Officer.

Users should be vigilant when conducting searches of the information available on the Internet and should disconnect immediately if connected to a web site containing prohibited material.

10. Personal Use of the Internet

10.1 Employees

10.1.1 Employees must not use the Internet for personal purposes during the working day i.e. contracted hours, overtime or when accruing flexi-time.

10.1.2 Subject to 10.1.1 employees may use the Internet for personal use before 8.00am, during lunch breaks, or after 5.15pm provided that:-

(a) Such use shall not contravene the rules on inappropriate use set out in Section 11.

(b) The use does not result in the Council becoming liable for any payments.

(c) The use is in the employees 'own time' outside of an employees working hours, ie, no flexitime is claimed.

10.2 Members

10.2.1 Members may use the Internet for personal purposes at any time of day but subject to the same provisos as for Employees as referred to in (a) and (b) of paragraph 10.1.2.

11. Inappropriate Use of the Council's Internet Facility

11.1 Illegal use of the Internet for any purposes which break applicable laws, including, but not limited to: -

- Distributing, forwarding, mailing, posting or solicitation for the reception of illegal material such as child pornography, obscene, threatening, intimidating, offensive or harassing material or hate propaganda in any form. Or making public to the Council or other users any such materials or direct links to such locations elsewhere on the Internet;
- Use of the Internet to libel or slander other users, individuals or institutions;
- Posting or in any way compromising the personal information of others as prohibited by the Data Protection Act 1998;
- Pirating, violation of copyright, trade secrets or infringement of any patent or other proprietary interest including any activity that supports illegal distribution of software;
- Gaining or attempting to gain unauthorised access to any kind of network, service, information, communications or computing facility or resource through use of the Internet;
- Damaging/destroying the integrity of a computer system or the data or programs stored on a computer system.

11.2 Displaying, receiving or disseminating sexual, pornographic or offensive material, in any form, for personal or non-work-related use, regardless of the legality of the material.

11.3 Attempting to disable or circumvent security mechanisms or access restrictions, or uncover security loopholes or circumvent information/data protection schemes in

order to gain unauthorised access.

11.4 Disrupting service by using the Internet to interfere with or disrupt network resources, users, services or equipment. Examples of these include but are not limited to: the deliberate distribution of computer viruses, "worms", "Trojan horses" or other malicious code; sending electronic chain letters or inappropriate wide distribution e-mail; playing network based games; attempting to monitor or tamper with another user's electronic communications except for monitoring by security and systems administrators in the performance of official duties.

11.5 Unauthorised publishing or distribution of official information.

11.6 Uploading or downloading screen-savers, games, computer software, video and audio files.

11.7 Conducting vandalism. Vandalism is defined as any malicious attempt to harm or destroy hardware, data of another user, Internet, or any agencies or other networks that are connected to the Council's Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses.

11.8 Advertisements for money-making schemes shall not be posted including pyramid schemes or any other use for personal gain.

11.9 Any other use that could reasonably be regarded as being inappropriate.

12. Disciplinary Action

The use of the Internet is a privilege, not a right. Abuse of the Internet facility will be treated seriously. Failure to comply with this Code of Practice and its spirit and in particular Sections 10 and 11 may lead to action that may result in: -

- Prosecution according to law.
- Removal of access to the Internet and revoking of authorised user status;
- Request for payment of compensation for the misuse of resources.
- Disciplinary action in accordance with the Council's disciplinary procedures which could lead ultimately to dismissal and which will render any individual committing an act of gross misconduct liable to summary dismissal. These procedures are available from the Departmental Human Resources teams or from the Council's Intranet site.

In accordance the Council's Employee Code of Conduct, any member or employee discovering a breach of this Code will be expected to raise the matter with the appropriate level of management.

Any suspected fraud that could have an impact on the Council must be reported in accordance with the Council's Anti-fraud and Corruption Strategy and Financial Regulation

Users should be aware that the transfer of certain kinds of materials is illegal and punishable under the law. Users should understand that evidence of such incidents could be passed over to the police authorities.

13. Further Information and Support

Please contact the IT Support (ext 2013) if you have any questions, problems or concerns regarding your responsibilities for compliance with this Code of Practice.

Similarly, if you require any help when using the Internet, again please contact IT Support.

14. What is e-mail?

Electronic mail, or e-mail as it is more commonly known, is a paperless method of sending or receiving letters, notes, messages and files between individuals - or even many people at the same time - via the Internet or internal computer network. Electronic mail is very fast compared to the conventional methods of communication and messages can be sent at any time with the message being available whenever the recipients want to look at it.

15. Why do we need this Document?

This document is intended to help employees and Members who make use of the Council's e-mail as part of their job to do so in a manner compatible with the values and objectives of the Council.

16. Why do we need e-mail?

The London Borough of Barking & Dagenham believes that e-mail resources should be broadly available since the facility opens up great opportunities for communication and resource sharing. Furthermore the Council believes that e-mail can be used to develop links with other councils, partners and other appropriate organisations. The fundamental aim of providing Council employees with e-mail is to support the business purposes of the Council, such as communicating and accessing work related information.

17. To Whom Does This Policy Apply?

The following people are covered by the points discussed in this policy: -

- All London Borough of Barking & Dagenham Employees.
- All London Borough of Barking & Dagenham Councillors.
- All agency employees, consultants and contractors to the London Borough of Barking & Dagenham who use the Council's e-mail facilities.
- Students, volunteers and others who use the London Borough of Barking & Dagenham e-mail facilities.
- Partners and agencies who have access to the London Borough of Barking & Dagenham e-mail facilities.

All employees are responsible for understanding and exercising this policy when using the e-mail resources of the Council, since, ultimately, the smooth operation of the facility relies upon the proper conduct of the end users.

The guidelines provided in this document are intended to lay down the way in which employees are expected to conduct their use of the Council's e-mail facility.

18. How to request access to e-mail

All e-mail access permissions will be set up by Information Management & Technology Division for individuals.

- Applicants must sign to show that they have already read this Code of Practice.

19. Composing e-mail Messages

The rapid nature of e-mail has lent itself to very short and “to the point" kinds of communications. Therefore e-mails can be much less formal than letters or faxes and can be less structured. However, there are a number of key guidelines that should be used to help you compose messages to be sent via e-mail. The fundamental point to remember when using e-mail is that it is **not** a secure method of communication. An often stated comparison is “don’t write anything in an e-mail you wouldn’t be happy to put on a post-card”. This is particularly relevant with Freedom of Information in mind – e-mails may have to be provided to people who request certain information.

19.1 Content

- When quoting another person, edit out whatever isn't directly applicable to your reply. Don't let your mailing automatically quote the entire body of messages you are replying to when it's not necessary. Take the time to edit any quotations down to the minimum necessary to provide context for your reply. Nobody likes reading a long message in quotes for the third or fourth time, only to be followed by a one line response "yes, me too".
- Be professional and careful what you say about others; e-mail is easily forwarded. Never assume your e-mail messages are private nor can be read by only yourself or the recipient. In addition to Information Management & Technology services, owners at any intermediate system along the e-mail's path could conceivably read your e-mail; while this is rare, it should be noted. Do not communicate information via e-mail that you would not be prepared to say to the recipient if you were talking face to face.
- Employees should be aware that e-mail can be used for committal, contractual or financial transactions involving the Council (e.g. placing orders, agreements, payments, etc.). Only employees expressly authorised may use the e-mail facility for these purposes and when doing so the Council’s Employee Code of Conduct, Contract Rules and Financial Rules must be adhered to. Warning note – conversations over the Internet by e-mail can result in legally binding contracts.
- Where it is used to communicate with trading partners or customers, e-mail should be treated in the same fashion as other forms of business correspondence.
- Do not send e-mails that communicate sensitive or confidential information about another person. Sending an e-mail or attaching a file to an e-mail constitutes processing of personal data if there is any personal data on a living

individual within the e-mail or attachment. Such processing can only be undertaken if it is permitted under the Council's Data Protection notification.

- Do not send multiple unsolicited e-mails (known as spamming) as this constitutes a breach of the Data Protection Act if the recipients' details were not obtained fairly.
- You should not represent your views as being those of the Council as not everyone is authorised to speak for the Council.
- All electronic mail originating, arriving or in transit through any electronic mail system belonging to the Council is the property of the Council.
- For e-mail being sent outside the Council, use your electronic signature at the bottom of e-mail messages. Your signature should include your name, position, Department, address and telephone number. For example:-

  Sarah Bryant
  Head of Information Management & Technology
  Finance Department
  Room 12
  London Borough of Barking & Dagenham,
  Civic Centre
  Dagenham
  RM10 7BY

  Tel: 020 8227 2015
  Fax: 020 8227 2060

- A disclaimer must be included at the end of every external e-mail.

LBBD have a standard disclaimer that must be used:-

E-mail confidentiality notice.

This message is intended for the addressee(s) only.

It may be private, confidential and may be covered by legal professional privilege or other confidentiality requirements. If you are not one of the intended recipients, please notify the sender immediately on +44(0)20-8592-4500 and delete the message from all locations in your computer network.

Do not copy this e-mail or use it for any purpose or disclose its contents to any person: to do so may be unlawful.

This should be set up so that every e-mail contains a disclaimer. Contact IT Support on 2013 who will advise you how to do this.

19.2 Copyright Issues

The following are your responsibilities for complying with and protecting copyright when including information from others in your e-mails.

- It is the responsibility of all users to respect the legal protection provided by copyright and licence to programs, data and other information that may be transmitted over the Council's corporate e-mail facility.

- You must cite all quotes, references and sources and respect copyright and licence agreements.
- You must not knowingly breach copyright laws.
- If in any doubt about copyright then contact Legal Services in the Corporate Strategy Department.

19.3 Attachments

If you are attaching a file to an e-mail, think about the format of the attachment and its ability to be read by the recipient. All attachments should be clearly labelled.

If you are receiving an e-mail with an attachment, you need to ensure that it is from a reliable source as attachments can contain viruses.

19.4 If you receive an e-mail from an external or internal source that is inappropriate and/or offensive or has inappropriate and/or offensive attachments then you must inform your manager immediately.

19.5 If you continue to receive such e-mails and it is clear that the e-mails are part of a campaign then your line manager will deal with this issue with Audit Section and Information Management & Technology.

19.6 Inappropriate/offensive e-mails should never, under any circumstances, be responded to.

20. Personal use of the e-mail facility

20.1 Employees

20.1.1 Employees must not use the e-mail facilities for personal purposes during the working day i.e. contracted hours, overtime or when accruing flexi-time save in cases of urgency and with the approval of the member of employee's line manager.

20.1.2 Subject to 20.1.1 employees may use the e-mail facilities for personal use before 8.00am or after 5.15pm provided that:-

(a) Such use shall not contravene the rules on inappropriate use set out in Section 21.

(b) No impression is given that the member of employees is representing the Council.

(c) The use does not result in the Council becoming liable for any payments.

20.2 **Members**

Members may use their Council computers for private e-mail use as they wish subject to there being no inappropriate use, as set out in Section 21 below.

21. Inappropriate Use of e-mail

The following should be considered as inappropriate use of the e-mail system: -

- Sending a person or people lots of unwanted messages (commonly known as spamming);
- Using e-mail as a vehicle for harassment, victimisation, discrimination, extortion or racial abuse;
- Sending material of an inappropriate nature around the organisation (e.g. pornography);
- Forwarding or generating e-mail chain letters, pyramid letters or similar schemes;
- Forwarding software or information that would violate the terms of applicable software licensing agreements or copyright laws;
- Disseminating, mailing, receiving or solicitation for the reception of illegal material such as pornography, obscene, threatening, intimidating or harassing material or hate propaganda in any form or making public to the Council or other users any such material or direct links to such locations elsewhere.
- Use of the e-mail facility to libel or slander other users, individuals or institutions.
- Sending or in any way compromising the personal information of others which is prohibited by the Data Protection Act 1998 (for advice contact Data Protection Officer on Ext 3351).
- Posting advertisements for money-making schemes or businesses including pyramid schemes;
- Unauthorised distribution of official information;
- Distribution of computer viruses.
- Any other use that could reasonably be regarded as being inappropriate.

22. Security

The following points are intended to protect the user and the Council from security problems associated with using Internet e-mail.

22.1 Confidentiality

When we send an e-mail to someone outside the organisation we use the Internet to transmit that message. E-mail over the Internet is not as reliable or as secure as inter-office e-mail. Whenever the consent of a third party is required to make a disclosure, then that consent must be obtained before the information is sent via Internet e-mail (external to London Borough of Barking & Dagenham).
Sensitive personal information should not be sent via Internet e-mail.
Confidentiality notices must be appended to e-mail's sent to external bodies (see 19.1 above).

22.2 Viruses

Viruses can be transmitted via e-mail messages to many users at one time. Virus

checking software is in place to automatically check messages that you send or receive; do not disable this software. To reduce risk, the downloading, copying or transmission via e-mail of executable files (e.g. .EXE, .BAT, .VBS file extensions) is not permitted without the authorisation of Information Management & Technology. File attachments from suspicious or unknown sources should not be opened.
To guard against the accidental activation of a virus, the Preview Pane (found under View) should **not** be set also the *'display a notification message when new mail arrives*' box (found under Tools, Options, Preferences, E-mail Options) should **not** be ticked.
If you are at all unsure as to what these requirement means contact IT Support on extension 2013.

22.3 Using someone else's e-mail account

You are accountable for any actions taken by other persons using your e-mail. Be careful as to who you give access to your e-mail.
Do not use another individual's e-mail without written permission from that individual and keep track of sent items so that anyone using your e-mail without your consent can be identified.

22.4 Electronic mail disclosure

At times it may be necessary for the mail system to be accessed by others and disclose the contents of an employee's electronic mail message. Specific circumstances may include: -

- You have become ill and someone must temporarily carry out your duties.
- You cannot be reached and your manager needs to have access to your mail to resolve a business crisis.
- The Council is required by law to supply records of correspondence on a particular matter.

This is not an exhaustive list; please seek the advice of IT Support (extension 2013) in other circumstances.

Authorisation by Internal Audit or a manager's written authorisation will be required to access and disclose the contents of an employee's mail box. This authorisation should be sent to the Head of Information Management & Technology for action.

22.5 Workstation

The workstation being used for e-mail should be appropriately secured to prevent unauthorised access. All passwords should comply with the standard defined in the Council's Password Policy and screen savers should be password protected. While connected, the computer should not be left unattended for extended periods. Alternatively the workstation should be locked if left unattended by pressing Ctrl+Alt+Delete and selecting Lock Workstation or you should log off.

23. Enforcement of the e-mail Code of Practice

Self-enforcement by users and supervisors of this Code of Practice will be encouraged by Information Management & Technology through user education and notification. Furthermore user departments should include the recommendations made in this document within their local working procedures.

Users of e-mail should be aware that, in order to monitor users' compliance with this Code of Practice, the Council reserves the right to access all user e-mail communications and examine all information collected, created and or generated as a result of using e-mail including files, messages, printouts, diskettes, or other material.

Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this Code of Practice has occurred.

23.1 Management responsibility for supervision of users

The following points are intended to help guide the management of e-mail usage within departments:

- The use of the e-mail to conduct departmental business is a management issue and as such all use should be authorised by management.
- Managers and supervisors of users should be aware of their employees' e-mail usage.
- The unregulated nature of e-mail has the potential for waste of employees' time and can be open to abuse. Appropriate measures should be put in place to minimise the opportunities for such problems.
- The use of the **everyone** option when sending e-mails must only take place with the relevant Director's authority, or in their absence, the relevant Head of Service. In many cases it may be more appropriate to publish the information on the Intranet.

23.2 Disciplinary Action

Abuse of the e-mail facility will be treated seriously. Failure to comply with this Code of Practice and the spirit of the Code, in particular Sections 20 and 21, may lead to the actions resulting in: -

- Prosecution according to law.
- Removal of access to e-mail and the Internet and revoking of authorised user status;
- Request for payment of compensation for the misuse of resources.

Disciplinary action is in accordance with the Council's disciplinary procedures which could lead ultimately to dismissal and which will render any individual committing an act of gross misconduct liable to summary dismissal. These procedures are

available from the Departmental Human Resources teams or from the Council's Intranet site.

In accordance the Council's Employee Code of Conduct, any member of employees discovering a breach of this Code will be expected to raise the matter with the appropriate level of management.

Any suspected fraud that could have an impact on the Council must be reported in accordance with the Council's Anti-fraud and Corruption Strategy and Financial Regulation.

Users should be aware that the transfer of certain kinds of materials is illegal and punishable under the law. Users should understand that evidence of such incidents could be passed over to the police authorities.

24. Training, Education and Awareness

E-mail is a tool just like many other software tools and as such requires users to be trained to use it to the greatest effect. There are a number of avenues open to e-mail users for training and education. Ideally training should be given to users very soon after they have the software installed on their machine. It is the responsibility of individual departments to organise and arrange; standard Microsoft Outlook courses are periodically arranged by the Organisational Development and Employee Relations Division in the Corporate Strategy Department.

In addition to this, Information Management & Technology will enhance awareness of functionality and features of e-mail tools to aid their effective use via the following mechanisms:

- Bulletins.
- Tips via e-mail.
- Updates to the e-mail Code of Practice.
- General support and problem solving will continue to be provided by Information Management & Technology.

New employees to the Council should be given a copy of this Code of Practice during their induction to aid their awareness of the important issues about the use of e-mail at the Council.

25 Housekeeping

Each individual e-mail account has a specific amount of disk storage space allocated to it to hold e-mail messages. Whilst messages in general occupy a small amount of space, attachments can require a sizeable area. Once the allocated area has become full, no further messages can be sent or received until space is released; this can result in important e-mail messages being lost.
Therefore it is vital that:-

- E-mail users should regularly tidy their e-mail message boxes by deleting old messages or relocating them into other personal folders - N.B. when deleting messages also ensure that they are deleted from the Deleted Items folder.
- Personal folders can be set up within Microsoft Outlook to enable retained e-

mail messages to be organised for ease of reference; for advice on this, please contact IT Support on extension 2013.

- Important e-mails can be archived and kept for further reference.

26 Out of the Office

When an individual is known to be out of the office for more than half a day, the "Out of Office Assistant" feature of Microsoft Outlook must be set. This feature will enable a notification to be automatically returned to the senders of incoming messages to inform them of the absence.

Let the person know you are not available but to be very bland with the message, ie, not to say you have gone on holiday and give details of when you will return to the office. The automatic forwarding of all e-mail to another person's e-mail address is not recommended. There are privacy and Data Protection implications. Below is suggested wording to be used as an automatic reply

I am sorry but I am unavailable at the present time, I will return to the office on ??
If you have an urgent request please contact
my colleague A N Other 0208 227 …..

NB. You must first have your colleague's consent before using their direct line phone number or email address. It is also advisable to check that they are going to be available in your absence.

If you are available for contact but not through email, you should leave a telephone number.

If you are working from home, you should give contact details as would be available if you were at your desk.

For further advice, please contact IT Support.

27 Further Information and Support

Please contact IT Support (ext 2013 if you have any questions, problems or concerns regarding your responsibilities for implementing this Code of Practice.

Similarly if you require any help when using e-mail, please contact IT Support.