Rochford District Council

Information Technology Code of Practice

CONTENTS

1 INTRODUCTION

1.1 Many of us deliver our services using information technology (IT). It is an important part of our day-to-day work. When we use the term 'IT', we mean computers and any systems we use to create, store or exchange information. This includes the Council's network, the intranet, internet, telephone system, the Essextranet and any extranets, bulletin boards, news and other services to which the Council subscribes or has access.

1.2 The purpose of this Code of Practice is to provide clear advice on what constitutes acceptable and unacceptable use of the Council's IT systems.

1.3 The Code of Practice applies to any use of the Council's IT systems by officers, Members, or representatives of external organisations such as auditors.

1.4 If you do not follow the standards in this Code of Practice, this could result in disciplinary action being taken against staff. The Council also reserves the right to report any illegal actions to the appropriate authorities.

1.5 These standards also apply if you are using or accessing Council equipment or networks at home.

2 USING AND CARING FOR INFORMATION

2.1 You must take all reasonable steps to make sure that:

- All information you are responsible for is safe and accurate.
- You only amend, remove or add information that can identify any living person if you have permission to do this.
- You only give information, including information about any person, to any people, groups or organisations who have authority to see that information and you have your line manager's permission.
- You do not produce, send or load onto the Council's IT equipment information that goes against Rochford District Council policy, breaks the law, or contains offensive, threatening, insulting, racist, pornographic or discriminatory information.

For more information, please refer to the Council's Records Management Policy Statement and Electronic Records Management Policy.

2.2 You must observe the eight principles of data protection at all times. In summary, these state that personal data must:

1. Be obtained and processed fairly and lawfully.
2. Only used for the purposes for which it is collected and not be disclosed for any reason incompatible with its original purpose.

3. Be relevant and adequate.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary.
6. Be made available to the individual concerned on request, and provision made for corrections.
7. Be kept secure from unauthorised access, alteration, disclosure, loss or destruction.
8. Not be transferred to any country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For more information, please refer to the Council's Data Protection Policy. The Data Protection Act can be found at:

http://www.hmso.gov.uk/acts/acts1998/19980029/htm

3 USING AND CARING FOR EQUIPMENT

3.1 You must:

- Only use computer equipment and systems for the purpose for which the Council has provided them.
- Take all reasonable steps to make sure that any IT equipment provided by the Council is kept in a safe working condition.
- Report any problem with your computer equipment to the Vivista service desk immediately.
- Log off all systems when you have finished using them.
- Switch off all PCs, monitors, printers, scanners and other IT equipment at night.
- Lock away all CDs, diskettes and other removable media when not in use.
- Ensure you have suitable backup of any CDs, diskettes or other removable media.

3.2 You must not:

- Install licensed or permitted software. This must be done by Vivista and not by anyone else.

- Install any unlicensed software or files of information which need a licence - because if you do you may be breaking copyright law and there is also a risk that a virus could be introduced onto the Council's system.

- Arrange for any hardware or communication equipment to be purchased or installed without authorisation from the IT Client Manager. All such installations must be carried out by Vivista and not by anyone else.

- Move any non-portable IT equipment. You may cause damage to the equipment, invalidate the warranty and the central inventory will be incorrect. If you require equipment to be moved, contact the Vivista service desk.

4 PASSWORDS

4.1 Passwords are one of the principal means by which the Council protects access to its systems.

4.2 You are therefore required to:

- Keep passwords confidential at all times; do not tell anyone your password or write it down.

- Once logged on to a system, you must not allow other staff to use your PC until you have logged off.

- Use the screensaver with a password to protect your screen whenever you are away from your desk.

- Change passwords whenever there is any indication that their confidentiality may have been compromised.

- Select passwords with a minimum length of eight characters.

- Change passwords at regular intervals of about 90 days, or as the application requires, and avoid re-using or “re-cycling” old passwords.

- Change temporary passwords at first log-on.

- Refer to Appendix 2 for best practice guidance on passwords.

4.3 You must not:

- Give other members of staff your password so that they can log in as you in your absence. If another member of staff is likely to require access to your system in your absence, this should be arranged in advance (see paragraph 6.10 for more details). If someone breaks this

Code of Practice whilst logged into a system as you, you could be held responsible.

- Include passwords in any automated log on process, e.g. stored in a macro or function key.

- Try to gain access to areas of any computer system or the network that you are not authorised to enter.

- Give any information or help to any unauthorised person or group that may assist them to gain access which they are not entitled to.

For more information on Passwords, refer to Appendix 2.

5 VIRUSES

5.1 Deliberate introduction of any damaging virus is a crime under the Computer Misuse Act 1990. Virus protection software is installed on all Council computer equipment. If you have a piece of equipment that does not have it installed, please report this to Vivista for immediate attention.

5.2 If material is inadvertently accessed which is believed to contain a computer virus, you should immediately break the connection, stop using the computer, and contact the Vivista service desk for assistance.

5.3 Please refer to "A Guide to Computer Viruses" on the IT Serv*ices* page of the Intranet for more information.

6 USE OF INTERNET AND E-MAIL

6.1 You are encouraged to use the internet and e-mail systems for work-related purposes. A limited amount of personal use of the systems is also permitted, but only in the circumstances set out in paragraphs 6.12 to 6.21 below.

6.2 Your use of the internet and e-mail may be subject to monitoring. However, such monitoring will only be carried out in a limited range of circumstances, which are described in paragraphs 6.22 to 6.28 below.

Limitations on the use of Internet and E-mail for work purposes

6.3 All staff should use the e-mail and internet in a responsible manner. You must observe the best practice guidance attached at Appendix 1.

6.4 You must not:

- Send, receive or publish any material that is obscene, factually inaccurate or defamatory or which is intended to annoy, harass or intimidate another person, goes against Council policy or breaks the law – you could be risking legal action against yourself and/or the Council, as well as breaching the Council's codes of conduct.

- Represent personal opinions as those of the Council.

- Send confidential information by e-mail such as:

  - personal data, as defined by the Data Protection Act;

  - passwords or other IT security information

  - Council credit card details, bank account details

  - any other confidential, sensitive or potentially sensitive information

  unless appropriate measures have been taken to encrypt or protect the data. Any such encryption or protection should be authorised in advance by your line manager and the IT Client Manager.

- Deliberately access, download or view web sites that contain material that is pornographic, obscene, racist, threatening or otherwise offensive in nature. It is recognised that web sites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading advertising or miskeying. Such occurrences will not constitute a breach of this Code of Practice. However, continued attempts to obtain access will be viewed as a deliberate action.

  If you do accidentally access this type of information, report it immediately to your line manager or the IT Client Manager.

- Disclose, or act upon, any privileged or confidential information contained within e-mails received in error. Instead, delete such e-mail and notify the sender that the message has been misdirected.

- Engage in any other unlawful or illegal activity in connection with the internet or e-mail.

- Use the internet in such a way that it has a detrimental effect on the Council's data network for example by downloading large image files or deliberately introducing viruses. The latter could lead to disciplinary action and criminal prosecution.

- Use the internet or e-mail in a way that would bring the Council into disrepute.

6.5 You must exercise caution when downloading web pages and documents for business use from the internet. This is important for the following reasons:

- The files may contain computer viruses which could infect the entire network (including the applications running upon it). Only download files (e.g. pdf files, Word files, Spreadsheets, PowerPoint files) from web sites of reputable organisations such as public bodies. All such downloads must be virus checked. Please refer to the Guide to Computer Viruses in the IT Services page of the intranet for advice on virus checking.

- You may be infringing the Copyright, Designs and Patents Act 1988 (see section 7 below). Unless a web site clearly states that a document can be downloaded free of charge, you must assume that its owner intends a charge to be paid. Free documents should only be downloaded from a reliable source, such as a government department.

6.6 You must not download software, including free software, games and screensavers, from the internet. If you need to download software for business reasons, you must first get permission from the IT Client Manager, and then the software must be installed by Vivista.

6.7 Carefully consider the implications of electronic transmission before entering into any new business processes.

6.8 You must notify your line manager or the IT Client Manager immediately if:

- You receive any illegal, obscene, threatening or offensive e-mail. Under no circumstances should you reply to such messages, as this could make matters worse.
- You are aware of any abuses of the e-mail or internet systems by colleagues.

6.9 You should always bear in mind that the internet is, for the most part, an un-regulated medium. Whilst it contains a wealth of valuable information, its accuracy can vary significantly. Consequently, you should only rely on information from reliable sources, such as Government web sites.

Dealing with e-mail during periods of absence

6.10 Please remember that your colleagues will not be able to access your e-mail when you are absent from the office. Problems can therefore occur if important e-mails cannot be retrieved or are overlooked altogether. If your absence is planned, arrange for incoming e-mail to be forwarded or copied to a colleague, or alternatively, use the *Out of Office Assistant* to notify senders that you are away and who they should contact in your absence. Contact the Vivista service desk if you require assistance in setting up these facilities. Do not give other members of staff your password in any circumstances.

6.11 You must only open the e-mail of a colleague when:

- Urgent access is required and the colleague is absent from work.
- The colleague has left no alternative arrangements.

- Authorisation has been obtained from a line manager. The IT Client Manager will need to see this authorisation before Vivista, via the service desk, is requested to grant temporary access to the e-mail account.

- The e-mail is work-related.

Personal use of the e-mail and internet systems

6.12 Limited personal use of e-mail and the internet is permitted.

6.13 It is expected that any personal use should be limited to a staff member's own time, that is, before starting work, during a lunch break or after work.

6.14 The rules in this Code of Practice apply to personal use in the same way as if you are using e-mail and the internet for work.

6.15 Staff should not use e-mail to have exchanges of a personal/social nature with other members of staff during working hours.

6.16 If you receive a personal e-mail that contains a non-work related attachment you must delete it. Under no circumstances should you forward it to other staff or other e-mail users, or save it onto the Council's systems.

6.17 As with all matters of conduct whilst at work, line managers have a responsibility for supervising use of e-mail and internet facilities, particularly as the unregulated nature of e-mail and the internet has the potential for wasting staff time and can be open to abuse.

6.18 When using the internet or e-mail system for personal purposes, you must not

- Download any files for personal use onto your PC, the Council's servers, or onto floppy disc or CD.

- Use the system for product/service advertisement, commercial activities or political lobbying.

- Send out private bulk mailings.

- Subscribe to non-work related web sites that send automated e-mails.

- Save attachments from private e-mails anywhere on the Council's network or on the hard drive of any Council PC or laptop.

6.19 The IT Client Manager reserves the right to limit or remove access to non-work related web sites without prior notice, if the Council's systems are being overloaded or otherwise adversely effected by internet use.

6.20 Access to web-based e-mail services (e.g. hotmail, yahoo etc) is for personal use only and must be agreed in advance by your line manager. Do not download any attachments from these sites as they pose a virus threat.

6.21 The IT Section cannot guarantee that personal e-mail sent on the Council's system is, or will remain, totally private and confidential.

Monitoring e-mail and internet usage

6.22 The IT Client Manager and Vivista will monitor:

- General e-mail and internet usage, e.g. total number of incoming and outgoing e-mails, file sizes, top ten visited web sites etc – such monitoring will be limited to summary, non user-specific data only.

- E-mail for names of known viruses in current circulation.

- E-mail for obscene, threatening, racist or otherwise unacceptable language/material including attachments that are likely to cause offence to the recipient.

- Internet logs for repeated attempts to access banned web sites.

- Both e-mail and internet usage, on an individual user basis, where there are reasonable grounds to believe that a breach of Council policy or UK law, has taken place. Such monitoring is a last resort, after conventional means of dealing with the problem have been exhausted.

- Periodically, logs of e-mail and internet usage to satisfy the Council that no serious abuse of the system is taking place.

6.23 The IT Client Manager and Vivista will not monitor:

- E-mail to or from a designated trade union or Human Resources email address, unless there are reasonable grounds to suspect that a breach of Council policy, this Code of Practice or UK law, has taken place.

- E-mail that is clearly personal in nature, unless there are reasonable grounds to suspect that a breach of Council policy, this Code of Practice or UK law, has taken place.

6.24 The IT Client Manager and Vivista will stop e-mail from being delivered in the following circumstances:

- To prevent the spread of a virus.

- To prevent the e-mail system from being damaged. The Council reserves the right to hold back e-mails that exceed 5Mb in size. E-mail that contains certain types of attachment, for example, executable files that often contain viruses, may also be stopped.

- At the wishes of the intended recipient of e-mail, for example, where an individual is receiving e-mail of an offensive or threatening nature. The express permission of the intended recipient will be required in such cases.

6.25 The Council reserves the right to access personal and shared areas on the servers in the event that a Head of Service, Corporate Director or the Chief Executive has reason to believe that there has been an abuse of this Code of Practice.

6.26 If the IT Client Manager and/or Vivista become aware of any issues that breach this Code of Practice, the information will be referred to the Head of Administrative and Member Services and the relevant Head of Service for consideration of appropriate action under the Council's disciplinary procedures.

6.27 If a line manager has good reason to believe that a member of staff is abusing the use of e-mail and/or the internet, s/he can request information about the e-mail and internet usage of that member of staff. To obtain the information, the written approval of either the Head of Service, Corporate Director or Chief Executive will be required by the IT Client Manager, before a call is logged with the Vivista service desk to release the information.

6.28 Internal audit may undertake checks on the operation of this Code of Practice as part of their auditing process.

7 COPYRIGHT INFRINGEMENT

7.1 Under the Copyright, Designs and Patents Act 1988 it is illegal to copy software without the owner's permission. These regulations are policed by the Federation Against Software Theft (FAST) and the Business Software Alliance (BSA) which carry out spot checks on local authorities.

Consequently, you must not

- Copy software.
- Share software with colleagues.
- Accept free software unless authorised to do so.
- Bring software from home to work.

7.2 Regular audits are carried out of software loaded on PCs and servers to ensure that valid licences are held. These audits are carried out via the network and you will not necessarily be aware that the checks are taking place. All inadequately licensed software will be deleted.

7.3 You must notify the Vivista service desk if you wish any work-related software or programs to be installed on to any Council owned PC or server. You must forward the original licence agreement and the CDs/discs to Vivista for inclusion in the register of licensed software. Vivista will then:

- Check the software to ensure that no viruses are present.
- Load the software onto your PC.
- Store the CD/disc in a secure cabinet.

7.4 The main risk of copyright infringement is from downloading files from the internet. It can also occur when text is copied into or attached to an e-mail message.

7.5 You should not copy information originated by others and re-post it without permission from, or at least an acknowledgement of, the original source, even if the text is modified to some extent.

7.6 The Council does not condone the illegal duplication of software. Employees who make, acquire or use illegal copies of software/files in connection with Council business or employees using Council facilities to do so will be subject to the Council's disciplinary procedures.

8 EXTERNAL CONNECTIONS TO THE IT NETWORK

8.1 All external access to and from the Council’s network is by way of secure telecoms connections. No other connections to the local area_network can be permitted. In particular, users should not connect modems to their PCs unless the written agreement of the IT Client Manager has been obtained.

9 INCIDENT REPORTING

9.1 Under the Computer Misuse Act 1990 (3) it is a criminal offence to:

- Gain unauthorised access to the Council’s systems, with or without intent to commit a further, serious offence.
- Make unauthorised modifications to the Council’s systems, or the data held upon them including the deliberate introduction of viruses.

9.2 Please report any IT security incidents, or any observed or suspected security weaknesses, immediately, to your line manager. If for some reason this is not possible report it immediately to your Head of Service or the IT Client Manager.

9.3 Please report any hardware or software malfunctions to the Vivista service desk immediately. You are also required to report any suspected malfunction caused by a suspicious piece of software, such as a possible computer virus.

9.4 The Council does not condone the illegal use of its computer systems. Employees who attempt to secure unauthorised access to, or make unauthorised modifications to any programme or data held in any of the Council's computer systems, or an employee who aids or abets another to do the same, will be subject to the Council's disciplinary procedures and may be reported to the appropriate Authorities.

10 DISCIPLINARY ISSUES

10.1 All breaches of this Code of Practice must be reported immediately to your line manager. If for some reason this is not possible report it immediately to your Head of Service or the IT Client Manager.

10.2 Contravention of this Code of Practice could result in disciplinary procedures and/or legal action being taken.

Any disciplinary action will be taken in accordance with the Council's disciplinary procedure which could result in:

- Informal warning.
- Denial of internet access for a period.
- Denial of internet access permanently.
- Dismissal for gross misconduct.
- Provision of information to the Police for possible criminal proceedings.

Appendix 1 - Best practice guidance on the use of e-mail

1. We are all suffering from e-mail overload! Consequently, don't use e-mail when it would be easier, and quicker, to deal with a matter by telephone or face-to-face contact. If the person replies straightaway to an e-mail they are at their desk so phone them or go and see them instead of sending messages back and forth.

2. Meet face to face or use the telephone instead of e-mail if the message is very important, controversial, or open to misunderstanding. Don't use e-mail as something to hide behind.

3. Don't express strong views in an e-mail, or use insulting or abusive language.

4. Do not use sexist, racist, violent, abusive or homophobic language. The Sex Discrimination Act (1974) and the Race Relations Act (1976) apply to e-mails as they do to any other form of contact.

5. Try to minimise the number of e-mails you send. In particular, limit your use of the 'All Exchange Users' or 'All Rochford Staff' e-mail distribution lists to e-mails that are very important and wholly work related. For all other general messages requiring a wide circulation, use the intranet notice board facility.

   If you have large non-confidential documents that you would like a number of staff to see, post them onto the intranet and send a message telling colleagues where the document can be found.

   Many of the Council's sections, and system users have e-mail group accounts. Use these to target a more specific audience. If there is a group you need to regularly target, set up a personal distribution list or ask Vivista to do it if you need a public one.

6. If you have an unavoidable need to send an e-mail to a large group of users, please use a Distribution List. Do not select the names individually from the Address Book. Long lists of e-mail addresses cause problems for users with sight difficulties, who rely on screen reader software to read their e-mails.

7. Don't feel that you need to respond more quickly to an e-mail than you would a conventional letter or memo. The same response targets apply to e-mail as apply to other means of communication, but you must log e-mail enquiries or complaints from residents in the same way as letters or telephone calls.

8. Keep e-mails brief and use meaningful subject lines.

9. Try using the following in the message headers:

   - MEMO – This is a formal memo and it should be kept Put the memo itself as a Word attachment and just use the e-mail to deliver it.

- FYI – for your information (The person receiving the e-mail does not need to take any action).

- EOM – end of message (It's all in the header, so there's no need to open the e-mail itself. This is handy if you're just confirming a meeting or saying 'thank you').

- SOC – social e-mail (for example, information about quiz nights or leaving parties)

10. Avoid

    - Typing e-mails in capital letters – such behaviour is regarded as the on-line equivalent of shouting!

    - High importance flags on e-mails – only add the flag if the message is genuinely very important.

11. Apply the same standards to e-mail as you would to typed letters or memos. Re-read messages before sending to check for clarity and to make sure they contain nothing that will embarrass the Council or leave it vulnerable to litigation. Also, don't forget to spell check messages.

12. Take appropriate steps to make sure you address e-mail correctly. If you find out that an e-mail has been received by someone other than the intended recipient, you must take steps to make sure this does not happen again.

13. Understand how to use, and don't mismanage, cc, only copy in people that really need to receive e-mail.

14. Never add an attachment unless it has been specifically requested and avoid sending them if you can include the text in the main body of the e-mail.

15. Archive effectively: use folders and only save relevant messages. However, you should ensure that your retention policy for e-mail is consistent with that for paper documentation.

16. Never reply to unsolicited “spam" e-mail. Report the receipt of 'spam' to the IT Client Manager.

17. Use the e-mail program's junk filter, taking care not to set the rules too high so that useful e-mail is lost.

18. Remember to use the 'Out of Office' facility if you are out of the office for half a day or more, or arrange for your e-mail to be redirected to a colleague.

19. Do not print e-mails (without a good reason)!

20. Remind friends and colleagues that they should not send you e-mails that are not in accordance with Council policy, and/or contain large attachments such as pictures etc.

21. Set the option that keeps original message text when you reply or forward a message. This means you only have to keep the latest version of any e-mail.

22. Save any attachments and delete the message. If you need to keep the text of the message, delete the attachment after you save it and just put a note at the bottom of the message indicating where it was saved.

23. Housekeep regularly and delete any messages you have sent or received that are no longer required. Don't forget to empty your deleted folder as well.

Appendix 2 - Best practice guidance on passwords

Passwords

Staff are issued with a user name and password which allows you to log on to the Council's network. Many of you also have secondary usernames and passwords that allow you access to various systems, databases, word processor files and spreadsheets.

Why do we have them?

Passwords are issued to ensure that unauthorised users to not gain access to systems that they are not entitled to use. These unauthorised users could be other employees or outsiders.

Why do they need to be kept secret?

It is very important that all of the passwords you use personally are kept confidential and not divulged to anyone, even work colleagues. If passwords are not kept secret then it could become possible for people to gain unauthorised access to our systems. Even if your password does not give them access to everything, it could still provide them with an entry point.

What sort of password should I use?

A good password should be:

- At least 8 characters long. Anything less is much easier to break.
- A series of random letters and numbers.

The following should not be used in passwords:

- Words that appear in the dictionary.
- Months of the year, days of the week or any aspect of the date.
- Proper names, especially your own, those of family, friends, pets, car registration numbers, favourite football teams, celebrities or anything from your immediate office surroundings that can be easily linked to you.
- Company names, identifiers or references.
- Telephone numbers or similar numeric groups.
- User ID, user name, group ID or other system identifier.
- More than two consecutive identical characters.
- All numeric or all alphabetic groups.

- The word ‘password’ itself.
- ******** (People use this as well!)

All of the above are very easy to break and standard techniques exist amongst hackers for so doing.

Passwords consisting of completely random letters and numbers can be difficult to remember so the following strategies could be used:

- Choose an eight letter word at random from the dictionary and replace one or more letters with a number or punctuation mark (avoid . or ,)
- You could also misspell the word before you replace some of the letters.

What else should I consider?

Never:

- Tell your passwords to anyone.
- Write them down especially on or near your PC.
- Let anyone else use systems that are logged in using your name and password.

Make sure you use different passwords for each system you have access to.

What are screensaver passwords?

You should always log out when you leave your PC. If however you are only going to be gone for a short period of time, engage your screensaver with password protection. Your screensaver can be set to activate when your PC is not used for a set period of time. However you can make it come on immediately on most PCs by clicking on its icon in the Office Toolbar.

Once the screensaver is on, no one can use it with out entering the password to deactivate it.

How often should I change my passwords?

Passwords should be changed at least every 90 days. On more sensitive systems they should be changed more often. They should also be changed if you think someone else has found it out. If in doubt, change it anyway. Ask Vivista or your systems administrator for guidance if you do not know how to change your passwords.