Rochford District Council

Information Communications Technology User Policy

March 2007

Contents **Page**

Definitions

RDC - Rochford District Council
Employees - Full-time RDC employees, part-time RDC employees, students, on site and off site agency staff
Other Users – Members, contractors, suppliers, external auditors, inspectors, customers, clients and other visitors
Users – Employees and Other Users
Policy – ICT User Policy
ICT – Information and Communications Technology
ICT system – RDC's Information and Communications systems including RDC's Servers, PCs, Laptops, devices, storage media, Local Area Network, Wide Area Network, e-mail system, Intranet, Web Site, external links and external access to its systems via Thin Client, Virtual Private Network or any other means.
Equipment – Any ICT equipment that belongs to or operated by SunGard Vivista or RDC

RDC is pleased to offer Users access to its ICT system. This Policy applies to anyone granted access by RDC to its ICT system. For RDC to continue making this access available, you must behave appropriately and lawfully. Upon acceptance of your account information and agreement to follow this Policy, you will be granted access. If you have any questions about the provisions of this Policy, you should contact the ICT Manager.

1. Personal Responsibility

By accepting your account password and related information, and accessing the ICT system, you agree to adhere to this Policy. You also agree to report any misuse to the ICT Manager. Misuse includes Policy violations that harm another person or another individual's property. You must take all reasonable steps to make sure that:

1.1. All information you are responsible for is safe and accurate;
1.2. You only amend, remove or add information that can identify any living person if you have permission to do this;
1.3. You only give information, including information about any person, to any person, groups or organisations that have authority to see that information and you have your line manager's permission;
1.4. You do not produce, send or load onto the Council's ICT 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 on the Intranet.

2. Terms of Permitted Use

Access extends throughout the term of your employment or involvement with RDC provided you do not violate this Policy. Note: RDC may suspend access at any time for technical reasons, Policy violations, or other concerns.

3. Purpose and Use

RDC offers access to its ICT System for business purposes. A limited amount of personal use of the ICT System is also permitted, but only in the circumstances set out in Section 10. If you are unsure whether an activity constitutes appropriate business use, consult the ICT Manager.

3.1 You must:

3.1.1. Only use the ICT System for the purposes that RDC provided them;

3.1.2. Take all reasonable steps to make sure that any Equipment provided by RDC is kept in a safe working condition;

3.1.3. Report any problem with Equipment to the SunGard Vivista service desk immediately;

3.1.4. Log off all systems when you have finished using them;

3.1.5. Switch off Equipment at night;

3.1.6. Lock away all DVDs, CDs, diskettes, USB sticks, memory cards and other removable media when not in use;

3.1.7. Ensure you have suitable backup of any CDs, diskettes, USB sticks, memory cards or other removable media.

3.1.8. Ensure you comply with all the related Policies mentioned in Section 12.

3.2. You must not:

3.2.1. Install licensed, permitted software including shareware and freeware. This must be done by SunGard Vivista and not by anyone else;

3.2.2. 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;

3.2.3. Arrange for any Equipment to be purchased or installed without authorisation from the ICT Manager. All such installations must be carried out by SunGard Vivista or other authorised contractor and not by anyone else;

3.2.4. Move any non-portable 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 SunGard Vivista service desk.

4. Passwords

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

4.2. You are therefore required to:

4.2.1. Keep passwords confidential at all times;
4.2.2. Do not tell anyone your password or write it down;
4.2.3. Once logged on to a system, you must not allow other staff to use your PC until you have logged off;
4.2.4. Use the screensaver with a password to protect your screen whenever you are away from your desk;
4.2.5. Change passwords whenever there is any indication that their confidentiality may have been compromised;
4.2.6. Select passwords with a minimum length of eight characters;
4.2.7. Change passwords at regular intervals of about 90 days, or as the application requires;
4.2.8. Avoid re-using or "re-cycling" old passwords;
4.2.9. Change temporary passwords at first log-on.

4.3. You must not:

4.3.1. 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 6.2 for more details). If someone breaks this Policy whilst logged into a system as you, you could be held responsible;
4.3.2. Include passwords in any automated log on process, e.g. stored in a macro or function key;
4.3.3. Try to gain access to areas of any computer ICT system or the network that you are not authorised to enter;
4.3.4. Give any information or help to any unauthorised person or group that may assist them to gain access which they are not entitled to.

4.4. For more information on Passwords, refer to "A guide to passwords" on the Intranet.

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 ICT equipment that requires it. If you have a piece of equipment that does not have it installed, please report this to SunGard 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 equipment, and contact the SunGard Vivista service desk for assistance.

5.3. For more information on Viruses, refer to "A Guide to Computer Viruses" on the Intranet.

6. System and E-mail Management

6.1. Users must use the ICT System appropriately and legally. RDC will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

6.2. Please remember that, other than in the circumstances detailed in paragraph 6.3, 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. See the Guide to E-mail Management on the Intranet if you require assistance in setting up these facilities. Do not give other members of staff your password in any circumstances.

6.3. You may only open the e-mail of another User when all of the following apply:

6.3.1. Urgent access is required and the User is unavailable;

6.3.2. The User has left no alternative arrangements;

6.3.3. Authorisation has been obtained from a line manager. The ICT Manager will need to see this authorisation before temporary access to the e-mail account is given;

6.3.4. The e-mail is work-related.

7. Banned Activity

The following activities violate the Policy:

7.1. Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials;

7.2. Making ethnic, sexual-preference, age or gender related slurs or jokes;

7.3. Engaging in illegal activities or encouraging or assisting others to do so. Examples include:

7.3.1. Selling or providing substances prohibited by RDC's employment policy;

7.3.2. Accessing, transmitting, receiving, or seeking unauthorized, confidential information about Users or any other person or organisation;

7.3.3. Conducting unauthorised business;

7.3.4. Viewing, transmitting, downloading, or searching for obscene, pornographic, or illegal materials. 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 Policy. 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 if you are an Employee. Other Users should take action appropriate to their relationship with RDC;

7.3.5. Accessing others' folders, files, work, networks, or computers. Intercepting communications intended for others;

7.3.6. Downloading or transmitting RDC's confidential information.

7.4. Causing harm or damaging others' property or encouraging or assisting others to do so. Examples include:

7.4.1. Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not marked with the copyright symbol, ©, Users should assume all materials are protected under copyright laws unless explicit permission to use the materials is granted or it is clearly stated that a document can be downloaded free of charge. Free documents should only be downloaded from a reliable source, such as a government department;

7.4.2. Using another User's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet;

7.4.3. Uploading a virus, harmful component, or corrupted data. Vandalizing the Network;

7.4.4. Installing or using software that is not licensed or approved by RDC;

7.4.5. Downloading 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 ICT Manager, and then SunGard Vivista must install the software;

7.4.6. Jeopardizing the security of access, the ICT System, or other Internet Networks by disclosing or sharing passwords and/or impersonating others;

7.4.7. Accessing or attempting to access offensive materials. Network and Internet access may expose Users to illegal, defamatory, inaccurate, or offensive materials. Users must avoid these sites;

7.4.8. Engaging in commercial activity not authorised by RDC.

7.4.9. Buying or selling anything over the Internet unless it has been authorised by RDC or as defined in paragraph 10.13;

7.4.10. Soliciting or advertising the sale of any goods or services unless it has been authorised by RDC or as defined in paragraphs 10.14 and 10.15;

7.4.11. Divulging private information including credit card numbers and other financial data about themselves or others unless it has been authorised by RDC or is for a personal transaction as defined in paragraphs 10.13, 10.14 and 10.15;

7.4.12. Wasting RDC's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send email copies to nonessential readers. Do not send e-mail to group lists unless it is appropriate for everyone on a list to receive the e-mail. Do not send organisation wide e-mails unless you are authorised to do so and you have your line manager's permission;

7.4.13. Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

7.5. Connecting peripheral devices that do not belong to RDC to the System. Examples of these include any USB, FireWire or other device.

7.6. Using media that do not belong to RDC on the System. Examples of these include CDs, DVD and memory cards.

8. Confidential Information

8.1. Users may have access to confidential information about RDC, other Users, or members of the public. If you have such access, Employees may use e-mail to communicate confidential information internally to those with a need to know. Others Users must act appropriate to their relationship with RDC. Such e-mail must be marked "Confidential." When in doubt, do not use e-mail to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

8.2. Under no circumstances should confidential information be sent over the Internet via e-mail or any other means. If you need to send such information, please seek guidance from the ICT Manager.

9. Monitoring and Privacy

9.1. Network and Internet access is provided as a tool for RDC's business. RDC has the legal right to monitor usage of the Network and the Internet, using the least intrusive method available.

9.2. E-mail, Internet usage and use of the System may be monitored on an individual 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. It has to be authorised by a Head of Service for Employees, and the Chief Executive or Corporate Director for Other Users. It will be treated in confidence.

10. Personal use of the e-mail and Internet systems

10.1. Limited personal use of the Internet is permitted.

10.2. Any personal use by Employees should be limited to the Employee's own time, that is, before starting work, during a lunch break or after work.

10.3. The rules in this Policy apply to personal use in the same way as if you are using the Internet for RDC business.

10.4. Employees should not use e-mail to have exchanges of a personal/social nature with Users or outside parties during working hours.

10.5. Users will be authorised to use send or receive attachments of particular types only if they have a business case to do so.

10.6. If you are authorised to receive attachments and you receive a personal e-mail that contains a non-work related attachment you must delete it. Under no circumstances should you reply to it, forward it to other Users, or save it onto RDC's systems.

10.7. Users who are authorised to send attachments should not send any of a personal nature via the System.

10.8. RDC uses software to alert it to e-mail attachments that may be unsuitable. This monitors internal, incoming and outgoing e-mails. SunGard Vivista, the ICT Manager and the User's Head of Service will know the content of personal messages that have attachments identified by this software.

10.9. As with all matters of conduct whilst at work, Employees' line managers have a responsibility for supervising use of Internet facilities, particularly as the unregulated nature of Internet has the potential for wasting Employees' time and can be open to abuse.

10.10. When using the Internet system for personal purposes, you must not:

10.10.1. Download any files for personal use onto your PC, RDC's servers, or onto floppy disc or CDs, diskettes, USB sticks, memory cards or other removable media;

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

10.10.3. Subscribe to non-business related web sites that send automated e-mails to a RDC e-mail address;

10.10.4. Use RDC e-mail addresses to receive receipts for goods or services bought on line.

10.11. RDC reserves the right to limit or remove access to non-business related web sites without prior notice, if RDC's systems are being overloaded or otherwise adversely affected by Internet use.

10.12. Do not download any attachments from web mail sites such as Yahoo or Hotmail as they pose a virus threat.

10.13. Users may use the Internet for personal transactions that do not involve the System in anyway other than to access the Internet.

10.14. Users may use the Staff Notice board on the Intranet to advertise Goods and Services. RDC reserve the right to withdraw any such service without reason.

10.15. Users may use the Intranet to advertise Goods and Services that do not involve the System in anyway other than to access the Internet.

11. Non-compliance

11.1. Your use of the Network and the Internet is a privilege, not a right. Violate this policy and, at minimum, your access to the Network and the Internet may be terminated, perhaps for the duration of your relationship with RDC. Policy breaches include violating the above provisions, and failing to report violations by other Users. Permitting another person to use your account or password to access the Network or the Internet including, but not limited to, someone whose access has been denied or terminated is a violation of Policy. Should another User violate this Policy while using your account, and if you have in some way facilitated this use, you will be held responsible, and in the case of Employees, both of you will be subject to disciplinary action.

11.2. If it becomes apparent that an Employee has violated the Policy, then the Council's disciplinary rules and procedures may be invoked. In serious cases, police or other authorities may be involved. According to the seriousness of the offence, this could result in action that could ultimately lead to dismissal. For certain offences the Employee may also be liable to criminal prosecution under the Computer Misuse Act or the Data Protection Act. All cases of non-compliance with the Policy will be raised informally (or formally depending on the seriousness of the violation) in the first instance by the line manager. Other Users will be treated as appropriate to their relationship with RDC.

11.3. If you know of Users who are violating this Policy in any way, you must report it to your line manager, Audit Team or Human Resources Team as appropriate.

12. Related Documents

Records Management Policy Statement
Electronic Records Management Policy
A Guide to Passwords
A Guide to Computer Viruses
A Guide to E-mail management
Linking Portable Devices to the Network Policy

13. Employee Acknowledgment

Note: If you have questions or concerns about this Policy, contact the ICT Manager before signing this agreement.

I have read RDC's Information Communication Technology User Policy and agree to abide by it. I understand violation of any of the above terms may result in discipline, up to and including termination of employment.

___________________________ Date:________________

14. Other User Acknowledgment

Note: If you have questions or concerns about this Policy, contact the ICT Manager before signing this agreement.

I have read RDC's Information Communication Technology User Policy and agree to abide by it. I understand violation of any of the above terms may result in action appropriate to my relationship with RDC being taken.

___________________________ Date:________________