

WAVERLEY BOROUGH COUNCIL COUNCILLORS ACCEPTABLE USE OF ICT EQUIPMENT AND SYSTEMS POLICY

Section 1. Who does the policy apply to?

This policy applies to all Councillors who are users of Waverley Information and Communication Technology (ICT) equipment and systems and is an addendum to the Waverley Code of Conduct for Councillors. It applies whether Councillors are working at the Council's offices or designated sites, their home or other off-site locations.

There are two distinct categories of Councillors who make use of Waverley's IT facilities. The first are Councillors who are provided with Waverley IT equipment such as a PC, laptop, printer etc along with Waverley owned software. All sections of the Acceptable Use Policy will apply to this group of Councillors.

The second category is Councillors who use their own equipment and to whom the following Sections do not apply:

- Section 3 - Using Waverley Equipment
- Section 4 - ICT Security
- Section 6 - Internet use
- Section 7 - Monitoring, intercepting and recording
- Section 8 - Private use of business systems
- Section 9 - Care of your computer

However all Councillors are reminded of the risks of maintaining personal or sensitive Waverley data on their PCs whether their equipment is privately owned or supplied by the Council.

Section 2. Introduction

2.1 The purpose of this policy is to:

- advise and protect Councillors;
- manage and secure Waverley ICT systems;
- protect Waverley ICT services and systems from misuse.

It is a requirement that you understand and follow this policy. You need to be aware of the risks involved in the inappropriate use of Council ICT systems. In certain instances failure to follow this policy could lead to IT facilities being withdrawn. It could also lead to criminal or civil action if illegal material is involved or if legislation, for example the Data Protection Act 1998 and the Human Rights Act 1998, is contravened.

Users must not misuse IT facilities by taking any action which is contrary to the Code of Conduct or which could bring Waverley into disrepute, cause offence, interfere with Waverley work or jeopardise the security of data, networks, equipment or software.

In general, much of the information contained in this policy is simply best practice and good advice. It is designed to assist you enjoy trouble-free use of the ICT systems provided by the Council.

The policy is divided into the following sections to assist you.

- Section 3 - Using Waverley computer systems
- Section 4 - ICT security
- Section 5 - E-mail use
- Section 6 - Internet use
- Section 7 - Monitoring, intercepting and recording
- Section 8 - Private use of business systems
- Section 9 - Care of your computer

2.2 The Council's ICT equipment and systems are intended to provide business applications to support the provision of services and to promote efficient communication within the office and with other organisations and customers. This policy gives advice on the appropriate use of the Council's ICT based business systems including, but not limited to, PCs, laptops and PDAs, memory sticks, mobile phones, ICT operating and telecommunications systems (including e-mail and the Internet).

Section 3. Using Waverley Borough Council computer systems

This part of the policy covers the use of ICT equipment and systems. It also covers information created, held, stored and accessed by those systems. The policy sets out your responsibilities when using these systems. For the purposes of this policy the term PC will be used to mean all desktop or handheld ICT devices designated for your use (whether shared or not).

3.1 Equipment

Only approved IT equipment may be used and no third party equipment (including wireless equipped systems) may be physically connected to Waverley IT networks or systems except with the written approval of the Head of Customer, IT and Office Services, IT Operations Manager or IT Development Manager.

Computer systems supplied by the Council must not be tampered with or modified in any way. Councillors should not attempt to repair or alter computer equipment or install additional equipment themselves. Contact the IT Help Desk for assistance when required.

All ICT equipment and systems supplied to Councillors are the property of the Council. You should remember at all times that these systems are intended to primarily be used for Council business purposes. All information stored on the Waverley network or PC's, is controlled by the Council.

When a Councillor leaves the Council, any computer system and user rights put in place specifically for that Councillor will be returned to the default arrangements for that system. All equipment must be returned to the Council.

3.2 Software

Do not use any software on your PC other than that pre-installed or on the approved software list for Councillors. Only software and systems on the approved software list may be used on the Council's network and ICT systems. Do not access any remote software or systems via your PC unless you are authorised to do so by the Head of Customer, IT and Office Services in conjunction with the Head of Democratic and Legal Services.

3.3 Licensing

Software issued by the Council for your use is licensed to the Council and is subject to licensing agreements controlling its use. Only legally compliant licensed software may be used on the Council's IT systems. It is illegal to make copies or distribute the software that you use in the course of your duties except where expressly authorised in writing by IT or Democratic Services to do so. Contravention of licensing agreements could leave you and/or the Council open to legal action. Councillors should note that software installed on Waverley provided PC's and laptops is considered to be "Business Use". Software that is free for "personal use only" is not licensed on Waverley owned equipment.

3.4 Data protection

All Councillors have responsibilities under the Data Protection Act 1998. All Councillors have the responsibility to ensure the confidentiality of all information held on Council systems. If you become aware that information you have access to in the course of your work may have become compromised or accessed inappropriately you must inform the Head of Democratic and Legal Services as soon as possible.

3.5 Protection of information

The IT Section uses software to control the applications and settings on Waverley's IT. This helps to protect systems from inappropriate use and keep systems operating efficiently.

No personal memory sticks or other removable devices such as DVDs, CDs, disks, SD cards etc are to be used to transfer data to or from equipment without the specific authorization of the IT Section.

3.6 Laptops

Councillors need to be aware of the risks of storing sensitive information on laptops and in order to mitigate the risk of the loss of sensitive or personal data that could arise from the theft or loss of a Waverley laptop the following provisions must be followed:

- All Waverley laptop users must use a 'power on' password on their laptop.
- Laptops must not be loaned to other people for use including family members.
- Laptops should not be left unattended in cars.

Section 4. ICT Security

4.1 Viruses and malicious software (malware)

Anti-virus software is installed on all computers supplied to Councillors. This software is maintained daily and will stop the majority of PC virus problems. But it is still necessary for Councillors to be vigilant when receiving new documents or files from outside the Council and to notify the IT Help Desk if you have any concerns.

Downloading from the Internet or opening e-mails are the most common source for viruses. Introducing software programs or documents by means of computer discs, DVDs, CD-ROMs, memory sticks or any other media can also introduce dangerous and potentially destructive viruses or other software threats. All software programmes and documents must be virus checked before installation or viewing on Waverley systems

If you have to send electronic information to an external recipient it must be labelled with a disclaimer for virus protection purposes – this is automatically provided on Lotus Notes mail. For guidance on virus checking please contact the IT Help Desk.

If you receive a warning message about a virus or you have reason to believe that you may have a virus on your system, notify the IT Help Desk (01483 523160) immediately.

4.2 Passwords

Passwords protect you and the systems you use. Keep your personal password confidential and change it when prompted. Do not allow your PC to be used by an unauthorised person. If anyone asks you for your password the answer must be 'No'.

You will be prompted to change your password regularly. Avoid using personal data or common words for your password. Do not use password generators (as found on the internet) to make passwords. Some of these systems are malicious and used by criminals to lure people to use passwords that are later used to attack organisations.

You must not enter or use any system using another person's password and log on to access information. The IT Help Desk does not have access to users passwords and cannot supply them under any circumstances but is able to reset passwords when required.

Section 5. E-mail

This part of the policy covers use of e-mail, and documents linked to an e-mail (attachments). The Council recognises that internal and external e-mail systems and the internet are integral to the Council's operations and are essential to provide services required by customers.

The e-mail system is a business tool and therefore should be used in an appropriate business like manner. However it is accepted that some personal use of the Council's e-mail system will take place and this is acceptable except in connection with personal transactions such as shopping. All external e-mails have a notice appended to them showing they were sent by Waverley Borough Council. Please bear in mind that outgoing e-mails sent from your PC bearing 'waverley.gov.uk' will adversely affect the Council's reputation or put the Council at risk of legal or other action if the content is inappropriate.

5.1 E-mail standards

Messages sent on the Council's e-mail systems are to be written in accordance with the standards of any other form of written communication. The content and language used in the message must be consistent with best Council practice. Messages should be concise and directed to those individuals who need to know about their contents and are affected by them. Do not send anything by e-mail that you would not be prepared to send on the Council's headed letter paper and remember that the worst case could be that e-mails may be used in court.

You must not use e-mail to harass colleagues or other recipients by sending messages that are insulting, or phrased in such a way that will cause distress to the recipient ("flame mail"). In accordance with the Waverley Code of Conduct for Councillors you are responsible for promoting a working environment which is free from intimidation, humiliation and harassment or which violates peoples dignity.

You must not pass on any junk e-mail or spam received, except to forward to the IT Help Desk or Internal Audit to block their receipt.

5.2 Receiving e-mail

Dealing with inappropriate e-mails

If you receive any such inappropriate e-mail material either in your inbox or junk mail post box you must take these actions:

- a) delete it – ideally without reading it first where the e-mail is obviously spam (unsolicited junk e-mail). In Lotus Notes deleted emails are stored in the 'Trash' area and will also require deleting from there;
- b) if the sender is known to you or is not an obvious source of spam, then reply to the sender saying that you do not wish to receive such material in the future;
- c) delete your copy of the incoming material. Never forward inappropriate material, externally or internally, unless requested by the IT Help Desk for further action by them;
- d) if your actions have failed to prevent the inappropriate material arriving, you should draw this to the attention of the IT Help Desk who may be able to block it.

5.3 Access to e-mail

You must not attempt to access an e-mail not addressed to you unless you are authorised to do so by the user for official purposes. You may only send e-mails from your own login ID and may not send any e-mails other than under your own name unless you are authorised to do so by the other user.

The unauthorised reading of e-mails that are not addressed to you could constitute a criminal offence.

Should you receive an e-mail message which has been wrongly delivered to your e-mail address, you should notify the IT Help Desk. If the e-mail message contains confidential information you must not disclose that

confidential information to external bodies such as the media, members of the public, contractors, suppliers or customers, who have no business knowing it. Should you receive an e-mail which contravenes this policy, the e-mail should be brought to the attention of Democratic Services.

5.4 E-mail mailing lists

You must not use your e-mail account to subscribe to mailing lists unless you obtain the prior consent and they relate to Council matters or are of professional interest.

5.5 Sending e-mail

E-mail signatures

E-mail messages should include contact information so that the recipient(s) are aware of who the sender is and how to contact them. This will usually include your name, Council address, telephone number(s) and link to the Council's web site and confidentiality clause.

5.6 Group e-mails

Group e-mails are any e-mail addressed to a Lotus Notes group usually made up of numerous e-mail addresses. General e-mail messages to a wider group such as "All Users" should only be used for urgent business purposes or in an emergency such as flood and fire. Sending attached documents to 'All Users' must be avoided.

5.7 E-mail attachments

Incoming e-mails and their attachments may carry dangerous or potentially damaging viruses for the Council. All e-mails received by the Council are checked for viruses and other problems. Never open an e-mail attachment from an unexpected or untrustworthy source or if, for any reason, it appears suspicious (for example, if it ends in .exe). If in doubt contact the IT Help Desk.

5.8 Confidential e-mail

The public e-mail system is not confidential. E-mails sent from the Council can pass through many systems in many countries before arriving at their destination. Ideally, confidential information should not be sent by e-mail. Confidential information (including personal data or sensitive personal data) should not be sent to external bodies by e-mail. If confidential information must be sent by e-mail it should be encrypted or otherwise protected. For guidance on how to protect data please contact the IT Help Desk.

You should ensure that the transmission of personal data, outside the Council does not infringe the principles of the Data Protection Act 1998 and the Council's Data Protection guidelines.

5.9 Legal action against the Council

Messages sent by e-mail can create legal obligations on the part of the Council and could give rise to legal action against the Council. Claims of defamation, breach of confidentiality or contract could arise from a misuse of e-mail. It is therefore vital for e-mail messages to be treated like any other form of correspondence. Do not regard e-mails as, in any way a form of communication that carries less standing than a letter on Council letter headed paper.

You must not agree to terms or enter into contractual commitments or make representations by e-mail. You are also reminded that messages are disclosable in any legal action taken against the Council. Before you send an e-mail, think carefully about its content and ask yourself how you would feel if you received that message or knew that it may be disclosed in Court. It can be used as evidence in industrial tribunals and formal enquiries, including internal disciplinary and grievance hearings.

Section 6. Internet use

6.1 Information quality

The internet contains a vast array of information. However not all information on the internet is accurate, complete or reliable and you should always critically evaluate its validity before using it.

6.2 Downloading from the internet

You must not download any graphics, software or any other programme from the internet except that software listed and specifically approved.

6.3 Copyright

Copyright exists on all published material by default. If you download or otherwise reproduce copyright information, text or other materials, you must adhere to any licensing conditions to ensure compliance with the Copyright, Design & Patents Act 1988. It is usually best to assume that copyright restrictions exist and that you cannot reproduce information unless there is an accompanying statement specifically providing permission to use material. Even then, use may be restricted or require payment and acknowledgement of source.

6.4 E-mail and internet misuse

Misuse

Misuse of the e-mail system or internet system by the intended or negligent viewing, downloading or transmission, distribution or receipt of any material or images listed below (without limitation), may constitute a breach of the Waverley Code of Conduct for Councillors.

The material must not be:

- defamatory;
- offensive, pornographic or obscene. This includes not only indecent or obscene materials which it is an offence to possess or/and publish, but also materials which anyone in the office might reasonably view as distasteful or likely to give offence to others;
- untrue or malicious;
- in breach of copyright;
- in breach of confidentiality of Council information;
- harassment on grounds of sex, age, religion, religious belief, race, disability, sexual orientation or political belief;
- for personal business activities;
- illegal;
- bullying; or
- in breach of security of ICT equipment and systems.

Section 7. Monitoring, intercepting and recording

The Council routinely logs the use of the ICT equipment and systems. Specialist automated software assists in this activity. The Council may need to monitor, intercept and record the use of ICT systems, including your Waverley owned PC or laptop, to ensure this use is not placing Council systems and services at risk or is otherwise inappropriate.

7.1 Monitoring and recording

To ensure that it complies with its own legal obligations the Council may monitor and record:

- a) frequency, times and patterns of e-mail use, e-mail addresses to which you have sent e-mails and the size of attachments and content;
- b) general statistical and system logging information relating to the management and operation of ICT systems.

The reason for the monitoring, intercepting and recording is to:

- to check that use of the ICT equipment and systems is legitimate and complies with the Council's rules;
- to find lost messages caused by computer failure;
- to investigate misconduct and to comply with any of the Council's legal obligations in accordance with legislative requirements such as the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Computer Misuse Act 1990, the Data Protection Act 1998 and the Human Rights Act 1998.

Even deleted e-mails and other data files may be retrieved or reconstructed for these purposes.

Section 8. Private use of business systems

The Council does not object to a reasonable amount of use of its Microsoft Office business system for creating private documents on a Waverley owned equipment.

Section 9. Care of your computer

You must take care when using any of the IT equipment and systems to avoid causing any damage to it. In particular, you must avoid allowing food and drink into contact with the equipment or allowing small objects such as paper clips and staples to fall onto the keyboard. Ensure that there is always good ventilation around the monitor and PC. If you become aware of any damage or fault with your PC you should report it immediately to the IT Help Desk. Do not attempt to repair or modify any computer system yourself.