ICT

Code of Practice

Table of Contents

1 Overview

Information Technology (IT) is an increasingly integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees will use Council Information Communication Technology (ICT) in the course of their duties.

This policy is designed to enable the Council to:

- get the best return possible for the investment it has made in technology
- gain maximum benefit from email and the internet
- comply with the law
- minimise legal and other risks associated with the use of technology
- ensure effective running of the Council's business
- minimise the risk of disruption caused by computer viruses and inappropriate use of IT; and
- provide clear information to employees and to increase ICT skills of our employees and residents.

This Code of Practice sets out the Council's policy on using its computers and networks, including all devices such as telephones, mobile phones; blackberrys; faxes; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is, for clarity of understanding, referred to throughout this policy as the Systems.

This policy applies to all Council employees who use the Systems. It also applies to other people using the Systems such as agency workers and contractors' staff. Note there is a separate parallel Code for Councillors.

It provides a summary of the detailed ICT Security Policies available on the intranet. It is based on the Government Connect Code of Connection and the ISO27001 / BS7799 standards for information management and security and is designed to provide a safe and secure environment for the use of technology.

Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose.

If you are unsure about how a rule or requirement applies, first check the detailed policies on the Intranet. If you are still unsure, contact CEC ICT Security for advice.

All users are required to read and accept this Code of Practice.

2 Email Policy

Emails form part of the Council's corporate records and E-mails sent or received while on Council business or using Council facilities are the property of the Council.

- Managers should ensure that staff use email in accordance with this Code.
- The sending and receipt of personal email messages is permitted as long as it does not interfere with work commitments. See section 8.
- Personal home email accounts should not be used to conduct Council business with the public or external organisations.
- Users must not set up 'automatic' forwarding arrangements for any messages from their work account to one outside the authority, e.g. at home. Automatically sending Cheshire East emails to external accounts increases the risk of disclosure or interception.
- Each user is responsible for the context of all text, audio and images that they send. They should ensure that private emails cannot be mis-interpreted as the views of the Council and do not contradict our policies or interests.
- No email or other electronic communications may be sent which misrepresents the sender as anyone else.
- The email service should not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use.
- The sending or forwarding of chain letters or other unauthorised mass mailings, regardless of the subject matter, is not allowed.
- Treat suspect email or that from a dubious source with caution. Do not reply or forward (even to ICT) a message if there is any doubt. Similarly do not open attachments or click on web links on suspect emails, as this could activate computer viruses or other malicious processes.
- The sending of unwanted messages can constitute harassment. Careless use of language can lead to a bullying tone and can also be considered harassment.
- Do not send (or forward) email containing derogatory statements, potentially libellous, defamatory, comments likely to cause offence, gossip, hoaxes, or jokes to others inside or outside the Council. See section 11
- Use 'shortcuts' or hyperlinks wherever possible, instead of attaching documents to emails. Large attachments (i.e. over 5Mb) should be avoided.

3 Use of the Internet

Users are granted access to the internet for business purposes and light personal use (see Section 8). Users must ensure that they comply with the provisions set out in this Code of Practice.

- Managers should maintain an awareness of staff Internet usage.
- Access to gambling, pornographic sites and sites of a similar nature, is not allowed under any circumstances. .
- Council information which is intended for internal use only, must not be placed on a system or website that is publicly accessible via the Internet.
- Staff should only enter personal information, e.g. credit card numbers, log in passwords etc. to websites if access to the site is encrypted, i.e. a 'padlock' symbol is shown in the bottom corner of the screen.
- The Internet is an insecure medium, therefore confidential or sensitive documents should only be sent by methods agreed to be secure. Guidance can be sought from ICT Security.
- Staff indicating their affiliation with the Council, e.g. via an email address, or any other identifier, on social networking sites or other non work related sites, must clearly indicate that the opinions expressed are their own, and not necessarily those of Council.
- It can be difficult to verify the true identity of a third party on the Internet. For your own safety and security and to protect the Council, information should not be shared with other users unless their identity is certain.
- Care must be taken using Social Networking sites in and out of work. The same care must be taken when posting information as sending email or writing official letters (see Social Networking Guidance on the Intranet)
- The Council does not accept liability for any loss or damage arising from use of the Internet to make personal financial transactions.

4 Passwords and security

Passwords protect information against accidental or malicious disclosure, modification or destruction. Information is an important and valuable asset of Cheshire East Council which must be managed with care.

- Users should follow password good practice
  - A password should be at least seven characters in length.
  - Contain characters from three of the four categories: uppercase; lowercase; 0 through 9; or special characters (*&^%$£"! etc.).
  - Not contain two of the same characters consecutively.
  - Be difficult for anyone else to guess.
  - Be kept confidential and not shared with anyone, not written down, and not included as part of an automated routine e.g. stored in a macro.
  - Be changed regularly and not used again for at least 12 months

- Users must 'log out' of systems fully or use the 'lock computer' command when leaving a workstation unattended.
- Managers should ensure that their staff have appropriate system access rights to undertake their roles, and that when an employee leaves or moves from their department that their system access rights are revoked (This can be done via the ICT Service Desk.).
- At least once a year, Managers should review with staff members, their system access rights and check that they are still appropriate.

5 Mobile Working

Mobile working, whether at home or away from normal business locations, brings with it additional threats to data security. Mobile equipment is also more vulnerable to theft, loss or unauthorised access.

While the other provisions of this Code apply equally when working on Council data or equipment while outside Council premises, additional requirements apply to Blackberries, mobile phones, laptop and desk-top PCs.

- Managers should maintain records for the booking out of equipment.
- All corporate laptops must be encrypted. This should be arranged via the ICT Service Desk. Users should not defeat this security by using un-encrypted removable media e.g. USB memory sticks. Instead corporate encrypted Memory sticks must be used.
- Always ensure that equipment and media are powered off when left unattended and preferably locked away.
- Equipment must be carried as hand luggage when travelling. If carried by vehicle, the equipment must be locked out of sight. It should not be left in an unattended vehicle, even if locked out of sight, for any length of time e.g. overnight.
- Ensure that only equipment belonging to the Council is connected to a Council PC or the network.
- Users should seek guidance from ICT Security on the use of equipment abroad.

Further considerations apply to Mobile Phones

- Managers should ensure all mobile phones can be accounted for and that where there is a pool the allocation is recorded and phones not in use kept securely.
- Mobile phones must be kept securely at all times.
- Report any phones lost or stolen to the appropriate Mobile Phone Co-ordinator immediately.
- Ensure appropriate use of personal and work mobile phones containing cameras in the work place.
- Seek guidance from ICT Security should you wish to use the mobile outside of the UK.

If you have been provided with a mobile phone/Blackberry for business purposes, you are allowed to use this phone for light personal use with the following conditions:

- You should have permission from your line manager.
- You should note the time spent on the call.
- Log the detail with your Local Administrator who holds an "Honesty Box".
- Make the appropriate payment according to the current tariff.

Further details see the link *Reimbursing personal Mobile Phone calls.*

6 Software and Virus protection

The Council adheres strictly to software licence agreements.

- Managers should ensure that all software is purchased through ICT Strategy and that the suppliers' conditions of use are followed.
- Users should not copy software nor use unlicensed copies of software.
- Care should be taken to prevent and detect the introduction of viruses and other malicious software by adhering to the Code of Practice and ICT Security Policies.

However, if you suspect a virus on any Council equipment:

- Contact the ICT Service Desk, and follow their professional advice.
- Unplug the network cable to isolate the PC
- Prevent anyone from using the PC.

7 Readable Information

Information from ICT systems is made readable on printed reports and computer display screens

- Managers should ensure that where the public have access to council buildings computer screens should be located out of the view of the public, in order to protect confidential or sensitive information.
- Users should make sure that when using a mobile phone or laptop away from the office, including use at home, that unauthorised individuals are not able to view or overhear confidential or sensitive information.
- Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially outside working hours.
- Prints of sensitive information should be cleared from printers immediately.
- Where a printer is not within the view of the user, it is recommended that, where possible, "locked" or secure printing is used, i.e. it is necessary to enter a code or user name into the printer before the document is printed.

8 Personal Use

- The Council recognises that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the Council permits you to use the Systems for personal use.
- However, you must not allow personal use of Systems to interfere with your day to day duties Excessive non-job related use of the Systems may be subject to disciplinary action.
- Please be reminded that the internet and email service should not be used for transmitting, accessing, retrieving or storing any communications of a

discriminatory or harassing nature or that are racist, offensive, obscene, pornographic, or sexually explicit. This applies to both business and personal use and is not allowed under any circumstances. Failure to adhere to this will result in disciplinary action (see section 12).

- As mentioned above, all Council Systems, including the internal and external e-mail system and internet usage may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose.
- You are responsible for any non business related file which is stored on your computer.

9 Ownership rights

You should note that all information and files created, received, stored or sent by you while on Council business or using Council facilities form part of the Council's corporate records and remain property of the Council.

10 Health and Safety – Display Screen Equipment (DSE) Regulations

All employees have responsibility for Health & Safety in the workplace, and this will be reflected in the manner that IT is used. Employees and Managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation and that the presence of technology in the office is not a cause for concern.

There are specific requirements for Display Screen Equipment (DSE) users and, so far as the Council is concerned, an employee falls within the requirements of the DSE regulations if they use equipment for continuous spells of an hour or more (on average) every day. All such employees are required to complete a DSE risk self-assessments. These risk assessment forms, along with additional advice and guidance, can be found at:

http://centranet.ourcheshire.cccusers.com/HR/Pages/HealthandSafetyPoliciesGuidance.aspx

11 Harassment and Abuse

The use of technology to harass and abuse others will not be tolerated. The Council has a clear and fundamental commitment to equal opportunities and the welfare of its employees, Councillors and others; and will not tolerate harassment in any form. This commitment is made explicit in the current 'Dignity at Work Policy which can be found at:

http://centranet.ourcheshire.cccusers.com/HR/Documents/Dignity at Work Policy.doc

Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action will be taken as appropriate. This applies whether it is another employee, a councillor, or a member of the public who is subject to the harassment or abuse.

If an employee experiences harassment in any way they are urged to contact their Manager, Union representative and/or Human Resources for advice and assistance.

12 Disciplinary Implications

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the *Computer Misuse Act 1990*, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages.

13 Acknowledgement and Consent

For your protection and that of the Council please read this Code of Practice carefully: Should you be in any doubt about the contents of this policy you should discuss this with your line manager. You are required to agree to all the terms and conditions of the Council's policy before you can have access to any Council ICT equipment and Systems. You will also be asked to confirm that have you have read, understood and agree to be bound by the terms of this policy when you log on to Council Systems, on a regular basis. In addition or as an alternative to, depending on circumstances you may be asked to complete this paper acknowledgement and consent form.

I confirm that I have read and understood the ICT Code of Practice (April 2010) and agree to be bound by its terms.

Print name:……..

Service Unit:…….

Signature:……..

Dated:…….