ICT Code of Practice for Members

1 Introduction

This Member Code of Practice is based on the ICT Security Policies, the Government Code of Connection requirements and ISO27001 standards for information management and security. It has been developed to assist members meet their responsibilities and should be used in conjunction with the associated HR and ICT Policies.

This Code of Practice is split into three areas; the first providing guidance on using Council systems, the second detailed guidance on using Council equipment and the third specific direction on using non-Council equipment to access systems.

Failure to adhere to this Code of Practice may be reported to the Council's Standards Committee.

For further guidance on any of the points set out below please contact the ICT Service Desk Contact x88888 or 0845 7603456.

2 Guidance when using Council Systems

2.1 Passwords

Passwords protect information against accidental or malicious disclosure, modification or destruction. Members must ensure that passwords are kept confidential and used in line with the ICT Security Policies. The main requirements being:

- 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

2.2 Email

- Each Councillor is responsible for the context of all text, audio and images that they send, and should not contain derogatory statements, potentially libellous, defamatory, comments likely to cause offence, gossip, hoaxes, or jokes to others inside or outside the Council.
- Be aware that data contained within email could be subject to the provisions of the Data Protection Act.
- Automatic forwarding arrangements for any messages from the work account to one outside the authority, e.g. at home must not be set up. Automatically sending Cheshire East emails to external accounts increases the risk of disclosure or interception.
- Confidential or sensitive information sent outside of the Council network via email must be encrypted using approved methods only – Contact the ICT Service Desk for additional information.
- Do not forward or reply to suspicious emails or chain letters, similarly do not click on attachments or web links within suspect emails. If in doubt contact the ICT Service Desk for advice.
- Be aware that a disclaimer is included automatically in all outgoing emails stating that is was sent in confidence for the addressee only, may be legally privileged and any views expressed are not necessarily those of Council.

- Email correspondence may be monitored inline with the ICT Security Policies.

2.3 Internet

- Councillors should only enter confidential 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. Council information which is intended for internal use only, must not be placed on a system or website that is publicly accessible.
- Members indicating their affiliation with Council, e.g. via an email address or other identifier, in bulletin boards, special interest groups, forums or other public offerings, in the course of their business must clearly indicate that the opinions expressed are not necessarily those of the Council.
- Care must be taken using Social Networking sites. The same care must be taken when posting information as sending email or writing official letters (see Social Networking Guidance on the Intranet).

2.4 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.

- Care should be taken with devices that have in-built cameras to ensure appropriate use. E.g. phone camera within a Children's Centre environment.
- Equally it is important to ensure that unauthorised individuals are not able to view or overhear confidential or sensitive information. All sensitive or critical business information should be kept secure when not required.
- Additional confidentiality issues arise when using equipment abroad. See Using Portable Electronic Devices Abroad.

3 Guidance when using Council equipment

3.1 Use and Protection

- Members may use their Council provided computers for official business activities and those related to other public bodies or organisations on which they are the Council's representative or nominee, e.g. Housing Trust, Parish Council.
- Members should not use the ICT facilities improperly for political purposes such as the promotion of a political party, a candidate or group of candidates in an election or in connection with a party political campaign. Receiving email on a separate private email account from a member's group or party would not be regarded as improper.
- Personal use is allowed providing the ICT security policies are adhered to.
- Members must 'log out' of systems fully or lock the computer when leaving a workstation unattended.
- All information and files created, received, stored or sent while on Council business or using Council facilities form part of the Council's corporate records and remain property of the Council.
- All corporate laptops must be encrypted. This should be arranged via the ICT Service Desk.
- Only corporate encrypted memory sticks must be used.
- Always ensure that equipment and media are powered off when left unattended and preferably locked away.

- Good security measures should be used to protect a laptop i.e. not left unattended when in use or when in sleep or standby saving states. The laptop must be kept in a secure location (i.e. out of sight) when not in use and not be an easy target for thieves.
- Ensure that only equipment belonging to the Council is connected to a Council PC or the network.

3.2 *The Council's Internet*

- The Council's Internet and email service may not be used for transmitting, accessing, retrieving or storing any communications of a discriminatory or harassing nature or materials that are racist, offensive, obscene, pornographic, sexually explicit, or used for the purposes of gambling.
- The Council does not accept liability for any loss or damage arising from use of the Internet to make personal financial transactions.
- Software must not be downloaded from the internet without approval from the ICT Service Desk.
- Internet use is monitored in line with the ICT Security Policies.

3.3 *Software and Virus Protection*

The Council adheres strictly to software licence agreements.

- Members should ensure that all software is purchased through ICT Strategy and that the suppliers' conditions of use are followed.
- Software should not be copied and unlicensed software should not be used.
- Care should be taken to prevent and detect the introduction of viruses and other malicious software. For example:

  - Do not use removable media of an unknown origin e.g.: USB keys, CDs etc:
  - Do not share removable media with personally owned PCs to avoid spreading a virus.
  - Do not download game/joke software or screen savers as they are a common method for spreading viruses.

4 Guidance when using own equipment

- Non Council equipment or privately owned equipment should only access systems through ICT approved remote access solutions.
- Members must 'log out' of systems fully or lock the computer when leaving a workstation unattended.
- All information and files created, received, stored or sent while on Council business or using Council facilities form part of the Council's corporate records and remain property of the Council.
- Members should clearly state in any email whether it is being sent on official Council business.
- The content of every email sent on official Council business must not be such that it brings the Council into disrepute. Emails whether including text, audio and/or images must not contain derogatory statements, potentially libellous or defamatory comments or anything likely to cause offence, to others either inside or outside the Council. Note that gossip, hoaxes, or jokes fall within this category.
- The Internet is an insecure medium, confidential or sensitive information should not be sent by personal email.
- Members are reminded that the Council's indemnity and insurance arrangements are limited to official business.