Section 9 - Guidance for Members in Relation to the Use of Council ICT Facilities

1.0 Introduction

1.1   Increasingly people expect to be able to deal with local authorities and those elected to represent them by use of e-mail and the Internet. To meet these expectations the Council has decided to provide its members with the necessary basic IT facilities.

1.2   This document outlines the basis on which these facilities are provided. It is also designed to help protect the Council and Members from accusations of misuse and/or malpractice and all Members will, therefore, be asked to sign up to the Council's Protocol for Members and Co-opted Members – Use of Council Resources and Equipment.

1.3   This guidance should be read in conjunction with the Council's other ICT and Security related policy and guidance documents which complement this document. Copies of the 'Information Security Policy' and IT Security Advice Notes are available from Sunderland City Council ICT Unit and via the Council's Intranet site at Security

2.0 Ownership

2.1   All equipment and software provided by the Council will at all times belong to the Council and equipment must be brought into the Civic Centre for repair.

2.2   All equipment should be returned to the ICT Unit at the end of a Councillor's 'term of office'.

2.3   Members should be aware that any information created on Council systems remains Council property. E-mail documents form part of the administrative records of the City Council and Sunderland City Council has the right of access to all e-mail sent or received, on the same basis as written documentation. For this reason, and to protect the network, members should not expect any information, whether it is related to the business or personal, to be private.

2.4   For security purposes and to maintain the network, Sunderland City Council may authorise certain people to monitor equipment, computer systems and use of the Council's network at any time.

2.5   Periodically audits of equipment may require that the equipment is brought to Council premises for verification purposes.

2.6   The equipment is provided primarily to assist with Council business and the majority of use should be for Council business. Members are reminded that they are responsible for ALL use of equipment that has been provided to them.

3.0   Security of the hardware

3.1   Members are required to take all reasonable care in respect of the security of the hardware. Laptops are particularly vulnerable to theft and the following recommendations must be observed:-

- When it is in your home you should make sure that it is stored safely and out of public view,

- Ensure the laptop is kept secure at all times. Do not leave a Laptop in an unattended vehicle (including a locked boot),

- Never leave a laptop logged in and unattended,

- When using a laptop in a public place ensure that a third party cannot see the screen contents,

- Regularly back up any files you keep on a laptop,

- The data on the laptop is your responsibility. Ensure that the information you record is not in contravention of the Data Protection Act 1984 & 1998. If you are unsure on this issue please check your compliancy with the Data Protection Officer, and

- Tape a business card/identification to the laptop or mobile equipment.

4.0   Security of the network and its systems

4.1   Members will be given a user name and password, which they should keep private and change it if they suspect that someone else knows it.

DON'T:

- Divulge your password to anyone else,

- Use passwords easily associated with you e.g. middle name,

- Leave confidential information on an unattended screen,

- Turn off or bypass the virus scanning software,

- Allow unauthorised people to use your computer,

- Use any disk, CD, DVD or other media unless this has been checked for viruses by using the anti-virus software provided, and

- Download or install any software without prior agreement with the ICT Unit.

DO:

- Be extremely careful when opening email attachments received from unknown senders. These may contain viruses, email bombs or Trojan horses (for information on what these are, please see the Anti-Virus Advice Note on the Council's Intranet site). Members should report any incidence to the ICT Help Desk,

- Keep your password secure Treat it in the same way as you would the PIN number for your personal bank account,

- Use your Smart Card Security where issued, and

- Understand the risks of using memory sticks and other USB disk equivalents (see USB and FireWire Devices Advice Note on the Council's Intranet site).

4.2   If you discover or suspect a virus, immediately stop what you are doing. Retain all disks etc used on the machine for analysis and recovery. Contact the Council's ICT Help Desk ((0191) 561 5000) as soon as possible. For more information on viruses, please see the Anti-Virus Advice Note on the Council's Intranet site.

5.0   E-Mail

5.1   This facility is a very valuable tool but it can be misused. Members should observe the following guidelines:-

DON'T:

- use the e-mail service excessively for personal messages,

- send messages in anger – cool down first!

- send messages that could be perceived as aggressive, abusive, sexually offensive, racially biased or discriminatory,

- send an e-mail for the sake of it,

- open an attachment from an unknown source without consulting the ICT Help Desk, and

- use your Council e-mail address to express a personal opinion that may be interpreted as Council policy.

DO:

- be as careful of the wording of an email as you would with a letter. It is just as legally binding,

- include a meaningful subject line,

- try and ensure your message is clear and not open to interpretation,

- remember that both the civil and criminal law recognizes e-mail as evidence of libel, copyright infringement, software theft, discrimination and harassment, and

- be aware that an e-mail is not secure once it leaves the Council's network – take advice before sending confidential information.

5.2 Remember; your e-mail is NOT private. E-mail documents form part of the administrative records of Sunderland City Council and the Council has the right of access to all email sent or received, on the same basis as written documentation. In addition, there is no guarantee that electronic communications, either internally or outside the Council, are private. So you should not email confidential, personal or other sensitive information.

6.0   Internet

6.1 The 'Web' contains a significant volume of information from numerous sources. It is entirely unregulated, insecure and open to exploitation. You are advised to exercise extreme caution, particularly in terms of the type of information accessed.

6.2 As a general principle, remember that you are acting as an elected representative of Sunderland City Council, using Council equipment and are accessing a non-private network. At all times have regard for Sunderland City Council policies and legal requirements when using the Internet. Where appropriate, have equal regard for specified rules and policies of the owners of services you access via the internet.

6.3 The equipment should be used primarily for Council business and private use shall be ancillary and not significant otherwise tax liabilities may be incurred. It is considered acceptable for elected Members to use the equipment provided for the following:

- personal purposes, for example purchasing holidays, goods and services, and

- general surfing of the internet for non-Council work related purposes.

This includes only true personal use and nothing related to a Councillor's other business interests.

6.4 Members should observe the following guidelines:-

DON'T:

- download software from the Internet without first seeking approval from the ICT Unit via the ICT Help Desk

- access websites which contain material which is pornographic, obscene or otherwise offensive

- use 'chat rooms' (A chat room or chatroom is an online site in which people can chat online (talk by broadcasting messages to people on the same site in real time). Sometimes these venues are moderated either by limiting who is allowed to speak (not common), or by having moderation volunteers patrol the venue watching for disruptive or otherwise undesirable behaviour. Chat systems come in a variety of styles ranging from text only messaging systems to fully immersive 3D environments Note that chat rooms are not the same as discussion groups or online forums, which do not take place in "real time")

- use it for your own commercial activities or personal financial gain

- visit Web sites that promote threatening or violent behaviour

- use the Internet for Illegal activities - in general terms, any use of the internet which contravenes any legislation (for example, The Data Protection Act 1998; The Computer Misuse Act 1990; The Copyrights, Designs and Patents Act 1988; The Obscene Publications Act 1959 and 1964); or any internal City Council policy (in particular, Council policies on Information and Internet Security; Equal Opportunities and Harassment)

- access gambling or games websites

- promote discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability

DO:

- be aware of copyright infringement

- exercise caution when using search tools (see below)

- remember that possession of certain material is a criminal offence – think before you download or print

- remember that the Council reserves the right to, and from time to time will, audit your computer to monitor the sites accessed by you

6.5   The above is not an exhaustive list. If in doubt contact the ICT Help Desk on (0191) 561 5000

6.6   It is possible to do a legitimate search using search engines and end up with inappropriate results. If you see anything that looks doubtful, do not click on it. If you do click on something that looks innocent but turns out to be inappropriate, please immediately report the matter to the ICT Help Desk, so that this can be taken into account as part of the auditing procedure. This will help protect both you and the Council.

7.0   Conditions of Use

7.1   The equipment and other facilities are provided primarily in relation to the official work of Sunderland City Council. Reasonable personal use is, however permitted subject to observance of the guidelines set out in this Policy.

When using Sunderland City Council computer facilities, Council business use takes priority over personal use at all times.

7.2   Members are reminded that Internet access and e-mail is monitored by Internal Audit and users must abide by the policy guidance.

7.3   A Member's failure to comply with this Policy will be regarded as a breach of the general Code of Conduct for Members, which has been circulated to all Members.

7.4   The Chief Executive may, at his/her discretion, authorise the return of ICT equipment where there has been a breach of this Policy and require the reimbursement of any costs incurred by the Council in respect of inappropriate use.

7.5   Where any criminal activity is suspected the Council will refer the matter for police investigation.

I acknowledge receipt of the above guidance and have read and understand the conditions of use set out above and I undertake to observe the Policy in relation to the IT facilities provided to me by Sunderland City Council.

Signed: ....

Name of Councillor: ....

Date: ....