Metropolitan
Borough of Wirral

USE OF COUNCIL ICT FACILITIES

CODE OF PRACTICE - MEMBERS

1. In order to assist Members carry out and discharge their role effectively, the Council provides personal computers with necessary software, peripheral hardware, telecommunications services and consumables ("ICT Facilities") to all Members. When using the IT Facilities provided, Members are required to adhere to this policy.

2. This policy outlines the manner in which ICT Facilities, should be used by Council Members and should be considered in conjunction with any guidance issued in relation to the use of ICT Facilities, in particular in relation to email and internet use.

3. In the course of their duties Councillors may store and process personal data on the computer equipment supplied by the Council. They will therefore be registered with the Information Commissioner's Office as data controllers as required by the Data Protection Act 1998.

4. This policy must be signed by all newly elected and re-elected Members.

5. All ICT Facilities provided by the Council shall remain the property of the Council and must be surrendered to the Council in the event that a Member ceases to be a Wirral Councillor. In this event access to Council electronic systems will be suspended and terminated within ten working days.

6. ICT Facilities are provided for the sole use and benefit of Council Members and must be used primarily for Council business. Use by family / friends and the like is not permitted however family members can provide assistance to Members in the use of the system as long as the Member remains in overall control of the PC and does not divulge their user name or password.

7. Members are expected to demonstrate a responsible approach to the use of the ICT Facilities provided and are expected to behave in a legal, moral and ethical fashion that is consistent with Council policies and standards.

8. All access to the Internet using computer systems (including portable computers) provided by the Council should be via the Council's network and established filtering system. This means that inappropriate sites will be blocked and a log of visited sites will be kept. These logs will be routinely monitored and will be used to assist in the investigation of inappropriate use.

9. It must be recognised that any view communicated over the Internet will be deemed to be the view of the Council, and will in most cases be treated as equivalent to correspondence sent by traditional formal routes. Any personal view expressed via a Council e-mail address should be endorsed "The contents of this e-mail are the personal view of the author and should in no way be considered the official view of Wirral Metropolitan Borough Council".

10. Members must use a password to log on to the computer provided as part of the ICT Facilities. Members must not disclose their password to another person. In the event that the password becomes known by anyone (or a Member suspects it has become known) then the password must be changed immediately.

11. Members ICT Facilities are configured to comply with the Council's ICT Security Policy and to meet the requirements of the Governments Code of Connection to the Public Services Network. Any unauthorised changes may contravene these policies therefore configurations must not be changed and Members must not attempt to add additional hardware, load software or connect personal devices to the equipment provided. Members will be able to connect approved personal devices to Council applications using the infrastructure installed for that purpose. Use of a personal e-mail account is permitted and will be configured on request by the Council's corporate ICT section.

12. All software provided by the Council with the computer, or subsequently, remains the property of the Council, or the licensing organisation as appropriate, and may not be shared or copied to another computer/device without written authorisation from the Head of Legal Services.

13. The security of any personal data held on a Council provided computer is the responsibility of the Member and recovery of such data cannot be guaranteed should the computer need repair. Members are responsible for the backing up of data held on the computer in accordance with any guidelines issued.

14. Members should print only essential material, and should check the length of a document before printing. For example Members should give consideration to only printing salient pages for reference purposes; and consider accessing material electronical that is available through Modern.gov e.g. Members Library. Consumables, e.g. printing ink and paper provided by the Council should only be used for Council business.

15. Members in using their ICT facilities must have regard to the Local Authority Code of Practice on Publicity and any guidance issued by the Council concerning the use of ICT facilities.

16. Members may use their Council provided ICT facilities 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. Fire Authority.

17. Members should not use their 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.

18. In the interest of national security, Members using Government Connect Secure Extranet (GCSx) or Government Secure Intranet (GSi) e-mail addresses may have their communications monitored by Government agencies. The contents of a Members e-mail folders may be accessed by officers of the Council, or Police Officers, as part of any investigation into inappropriate use of e-mail, or complaint against the conduct of a Member.

19. Members must not automatically or manually forward electronic mail from a Wirral Council email account to a web mail account hosted on the Internet by a third party, for example Google, Yahoo, Hotmail etc. This is because they are lower classification domains and not considered secure by Government security advisors.

20. The Information Commissioner has the power to fine public sector organisations up to £500,000 in the event that unencrypted personal or sensitive data is lost or stolen. Members should therefore avoid downloading or storing such data on their computer's internal disk. Council provided computers will be encrypted but in the event that any equipment is lost or stolen then this must be reported to the Council's corporate ICT unit as soon as possible following discovery of the of the loss or theft.

21. <u>Unacceptable Deliberate Use</u>

The following activities, whilst not an exhaustive list, are considered unacceptable:

a. The access to or creation, transmission or publication of any illegal or indecent images, sounds, data or other material.

b. The access to or creation, transmission or publication of any data capable of being displayed or converted to such illegal or indecent sounds, data or other material

c. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience, discrimination or needless anxiety, or which may intimidate or create an atmosphere of harassment.

d. The creation, transmission or publication of defamatory material.

e. The storing or transmission of material that infringes the copyright of another person.

f. The creation, transmission or publication of any material in violation of Data Protection legislation or of any UK or International laws or regulations. Such activity may constitute a criminal offence.

g. The transmission of unsolicited commercial or advertising material to other users of the Council's network or users of the Internet.

h. The deliberate unauthorised access to facilities, services, data or resources within the Council or any other network or service accessible via the Internet, or attempts to gain such access.

i. Unauthorised access to the electronic mail of another individual.

j. Deliberate activities with any of the following characteristics or that by their nature could result in:

   i. wasting staff or other users' efforts or network resources;
   ii. corrupting or destroying other users' data;
   iii. violating the privacy of other users;
   iv. disrupting the work of other users;
   v. using the Internet in a way that denies service to other users (for example by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files);
   vi. continuing to use any item of software or to access any material after being requested to cease its use because of disruption caused to the functioning of the Council's network or the Internet (for example utilities designed to broadcast network-wide messages); and/or
   vii. the introduction or propagation of viruses.

k. Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network.

l. Any use of the Internet or other facilities that could damage the reputation of the Council.

22. Any breach of this policy could result in the withdrawal of ICT Facilities from the relevant Member or in some cases result in further action being taken. (See below).

23. Any alleged breach of this policy will be subject to an investigation by the Council's Monitoring Officer in consultation with the Council's Internal Audit Section. Upon

conclusion of any investigation undertaken where in the opinion of the Monitoring Officer a breach(es) has been found, the Monitoring Officer may take one or more of the following actions,:

a. Notify the Member's Party Group Leader of the breach;
b. By complaint refer the breach(es) to the to the Council's Standards Committee Initial Assessment Panel;
c. Notify the breach(es) to the Police if the Council suspects a criminal act has been committed.

Issued to: Councillor . . . . . Date

I agree to abide by terms defined above

Signed _____ Date

_____

A signed copy of this document should be returned to the Monitoring Officer with a copy held by the individual Member.

……..……..