

Protocol on the Use of Council-supplied Computer Facilities by Members

1 Introduction

The Council provides Members with computer equipment to use to facilitate the performance of their duties as Members. This protocol sets out the conditions on which such facilities are provided.

2 Security for the equipment

- (a) The Member will not be held responsible for theft of loss or accidental damage to the computer equipment, provided s/he takes reasonable care of it. The Member agrees to make reasonable arrangements for the safe-keeping of the equipment while the equipment is in the Member's possession
- (b) Access to the Council's information systems via the equipment will be available, but subject to password or other security. The Member shall ensure that no-one other than the Member is given access to those systems and shall not reveal any such password to any other person.

3 Use for Council Business

- (a) The equipment is provided to the Member specifically to facilitate the discharge of the Member's functions as a Member. The Member must therefore not use the equipment in any manner which will prevent or interfere with its use for that purpose.
- (b) Accordingly, the Member must not knowingly:
 - (i) misuse the equipment
 - (ii) install or use any other equipment or software
 - (iii) use any device as a telephone or for any purpose whereby a charge may be incurred by the Council
- (c) The Member must:
 - (i) Ensure that the equipment is maintained in a working condition;
 - (ii) Report any faults promptly to the IT service desk (tel: 01799 510412);

- (iii) Provide reasonable access to Council officers to service, maintain and repair the equipment.
- (d) The Council provides the equipment together with ancillary materials required for the Member's functions as a Member. Accordingly, the Council may decline to provide further equipment or material beyond a certain allowance where the use of such equipment or material appears to the Council to be required for private (non-Council) use.

4 Use for Private Purposes

- (a) The Member may use the equipment for private and family purposes;
- (b) The Code of Conduct restricts Members from improperly using Council resources for political (including party political) purposes. For this purpose improperly using Council resources for political purposes shall mean:-
 - (i) communications sent on Council headed notepaper or by way of electronic transmission on Council owned equipment which constitutes an attack on any individual Member, on a political group or the adopted policy of the Council;
 - (ii) communications sent on Council headed notepaper or by way of electronic transmission on Council owned equipment which promote the views or policy of a political group which has not been adopted as the policy of the Council
 - (iii) canvassing support or opposition for a candidate or political group for any election

provided that this shall not in any way restrict the use of Council resources for communications between Members or Council officers or restrict a Member from responding to individual constituents using Council resources

- (c) The Council accepts no responsibility for private use of the equipment or any loss, costs or liability which the Member or any other person may suffer as a result of the use of Council supplied computer equipment.

5 Inspection and Audit

The Council reserves the right to inspect or audit the equipment at any time. The Member is required to give Council officers access at any reasonable time for such inspection and audit. Members are advised that

the equipment includes a history file which records its use, and particularly any websites which it has accessed.

6 Costs

- (a) The Council will meet the cost of providing the computer equipment, together with a limited supply of paper and printer cartridges.
- (b) Each Member is responsible for his/her own electricity bill in using the Council supplied computer equipment.

7 Return and Recovery of the equipment

- (a) The equipment remains the property of the Council.
- (b) The Council reserves the right to require the Member to return the equipment at any time and the right to recover the equipment from the Member.
- (c) The Member is required to return the equipment to the Council upon ceasing to be a Member.
- (d) The Member is required to return the equipment to the Council in the event that the Member's use of IT equipment is suspended by the Standards Committee of the Council or by the Adjudication Panel for England unless such suspension is stayed by the Adjudication Panel pending an appeal

8 Data Protection/Freedom of Information

- (a) Members are covered by the Council's registration under the Data Protection Act 1998. As such the subject access provisions of that Act apply. This means that a person about whom a Member holds information electronically on Council owned equipment may require all such information to be disclosed to them unless a statutory exemption applies. A Member not wishing a disclosure to be made in response to a request should consult with Legal Services to ascertain if such an exemption may apply.
- (b) Where a Member stores information other than as representative of the Council on the Council's systems the Council generally holds this information on behalf of the Member, not on its own account. Accordingly the Council will not "hold" the information for the purposes of the Freedom of Information Act 2000 and would not normally be required to disclose it in response to a request for information made under that Act. Information stored by Members as representatives of the Council is disclosable under the Act however unless a statutory exemption applies. Members will be consulted

regarding any request for information stored by them and if a Member objects to the information being disclosed Legal Services will advise as to whether an exemption exists which may be applied.

9 Restriction of Use

The Council reserves the right to restrict the use of the equipment if it has reason to believe that the use of the equipment is likely to offend any provision of the Protocol. In particular, the Council reserves the right to:

- (a) remove or disable any software or equipment not installed by the Council;
- (b) remove any information not relating to the business of the Council of the office of Member.
- (c) disable remote access

10 Additional advice

Attached to this Protocol are Annex A, which gives advice on the health & Safety aspects of using Council-provided Council supplied computer equipment at home, and Annex B, which is the Policy applicable to **employees** on use of e-mail and the internet. Clearly, not all of this Policy will apply to Members, but they should comply with it where it is relevant .

**ANNEX A: ADVISORY HEALTH AND SAFETY GUIDELINES FOR MEMBERS
WHEN USING CITY COUNCIL IT equipment AT HOME**

1. The Council needs to consider the health and safety requirements regarding home working as they relate to Members using Council-provided IT equipment in their homes.
2. A copy of the Health and Safety Executive leaflet on home working is enclosed. **Please read it carefully.**
3. It is important that the electrical system in Members' homes is properly constructed and maintained. Anyone with a modern home (built in the last 20 years) should be alright; however older properties, or a property that has not been rewired within the last 25 years, should advise the IT section of this. They will then contact the Central Safety Advisory Service for advice on the suitability of the electrical system in the Member's home. **However, the cost of any remedial work is the responsibility of the homeowner.**
4. Members who work from home will have their workstation assessed to comply with the Display Screen Equipment Regulations.
5. Please remember never to eat and/or drink close to electrical/IT equipment .

ANNEX B: INTERNET AND E-MAIL ACCEPTABLE USE POLICY FOR COUNCIL EMPLOYEES

The following outlines the Council's Acceptable Use Policy regarding e-mail and the Internet. Please ensure that you understand the policy and that you abide by it. Any misuse may result in disciplinary action.

E-mail and the Internet are provided by the Council to assist employees in carrying out their work. Use of these services should support Council policies and objectives and reflect the Council's high standards of service.

Although it is not the policy of the Council to monitor e-mail and Internet use in general, the Council reserves the right to monitor usage for operational, maintenance, security or investigative reasons. Full co-operation will be given if law enforcement or regulatory agencies request information about e-mail or Internet use by an employee. If necessary for operational purposes, the Council reserves the right to access an employee's e-mail, for example, during prolonged absence of the employee. Proxy access should be used where it is important to ensure regular access to an employee's mailbox.

If you are aware of any abuses of this policy they should be reported to your line manager, or reported in accordance with the Council's Confidential Reporting ("Whistleblowing") Policy.

Separate good practice guidelines will be issued covering use of Groupwise or any replacement e-mail system, including archiving, out-of-office notification, use of service e-mail accounts etc.

Internet

General

- Do not download any material that you suspect may contain a virus. All files should be downloaded using a equipment with virus checking software installed. No software should be downloaded (including screen savers). If there is software on the Internet that you feel you need, a request should be made via the Helpdesk.
- Do not use material from the Internet without checking whether it is restricted by copyright or licensing laws.
- Goods should not be purchased via the Internet unless you are authorised to approve purchase orders, or have an approved purchase order. If in doubt about the organisation or the process for ordering check with Audit or Finance.

Personal use

- The Internet may be used for personal purposes but only outside peak working hours (i.e. before 9:00, after 5:00 or at lunchtimes). *NB network problems mean this is currently limited to before 8:30 or after 5:30 until further notice.*
- Sites should not be accessed if they are likely to contain illegal or offensive material, for example, pornography, or material that may be considered obscene or abusive. A filtering mechanism is in place that will block many of these sites.
- Systematic attempts to log onto sites containing illegal or offensive material or to blocked sites may amount to gross misconduct and result in disciplinary action, up to and including dismissal.
- The Council Internet service must not be used to access “chat rooms”.
- The Council Internet service must not be used to purchase goods and services for non-Council purposes.
- The general restrictions listed above also apply to personal use.

E-mail

General

- E-mail messages cannot be guaranteed to be private and secure: do not send confidential, sensitive or personal data via e-mail. Remember that any message you send could potentially be forwarded to others by the recipient.
- No message should be sent, either internally or externally, which contains illegal, offensive, obscene or abusive material (for example, pornography) or libelous, defamatory or discriminatory material, or material which may bring the Council into disrepute. **You** are responsible for e-mails you send. E-mails could be used as evidence in a tribunal or other court proceedings.
- Respect the rights of others when sending e-mails. E-mail should not be used to harass or discriminate against others. If you receive such an e-mail bring it to the attention of your line manager or report it in accordance with the Council’s Confidential Reporting (“Whistleblowing”) Policy.
- Use the same level of professional language, spelling and grammar for external e-mail that you would use for letters and other business correspondence.

- E-mails are subject to the same maximum response times as letters. Please ensure that e-mail messages sent to individuals or service addresses are properly dealt with if someone is on leave, off sick or otherwise out of the office for an extended period
- Be aware that agreements made by e-mail may have the same status as letters or formal contracts. Seek guidance from Legal Services or Internal Audit before making any agreement by e-mail.
- If you receive e-mails from unknown sources and they contain attachments, they should not be opened as they may contain viruses. Any suspicious e-mails should be reported to the Helpdesk (ext 7600).
- If you receive a virus warning this should be forwarded to the Helpdesk, but not to other e-mail users.
- You may subscribe to newsgroups and mailing lists for business purposes only, after obtaining permission from your line manager. Ensure that such subscriptions do not produce high numbers of e-mails (i.e. more than 10 per day).
- Do not disclose your e-mail address unnecessarily as to do so may result in unsolicited e-mails (sometimes known as junk or spam).
- Ensure that you delete messages that are no longer needed. E-mails will be deleted automatically after 3 months.
- Ensure that your e-mail is password protected (this facility is available in GroupWise) and that you do not disclose your password to others. Ensure that your screen saver is also password protected.
- Do not access e-mail messages that you are not authorised to view i.e. e-mails where you are not the recipient or have not been granted proxy rights.
- Do not send large files (over 1mb) via e-mail without checking with the Helpdesk first.
- Do not use e-mail to transmit material that may infringe copyright or licensing laws.

Personal use

- Personal use of e-mail is permitted, with permission of your line manager. However, e-mails should be short and not excessively frequent (i.e. no more than 3-4 per day). Any personal use of email should not adversely affect your work.
- Do not forward chain letters, jokes or other multiple mailings that are not business related.