

MEMBERS' E-MAIL AND INTERNET USAGE POLICY

1. Introduction

- 1.1 **It is vital that you read this Policy carefully.** If there is anything that you do not understand, please ask HLDS to explain. Once you have read and understood this Policy, you must sign it and return the signed copy to Democratic Services. If you wish to refer to the Policy in the future it is in the Council's Constitution, on the website. If the signed agreement is not returned within a reasonable time your use of e-mail and internet facilities may be withdrawn.
- 1.2 This Policy contains important rules covering e-mail, internal and external, and access to the Internet. Many of the rules apply equally to the Council's other methods of communicating with the outside world such as letter, fax and telephone.
- 1.3 This Policy explains how e-mail and Internet access should be used. It explains what you are allowed to do and what you are not allowed to do. If you have any general problems with this Policy please contact the Assistant Director (HR, Legal and Democratic Services).
- 1.4 This Introduction of the Policy describes some of the controls operated by the Council. Next are General Rules for the use of the Council's Internet and e-mail services and some advice on the sensible use of internet services. We have then identified six areas where legal problems might arise for you and for the Council. These are harassment, defamation, copyright, entering contracts, pornography and confidential information.
- 1.5 Failure to comply with this Policy:
 - (a) may result in legal claims against you and the Council; and
 - (b) you may breach the Council's Code of Conduct; *leading to your being reported for a breach of the Code of Conduct*
- 1.6 The Council routinely monitors the level and route of e-mail and Internet traffic. Logs are kept on the system. These may be inspected at any time without notice where there is just cause for suspicion of misuse. If through routine monitoring the Council has grounds for suspecting a councillor of illegal or inappropriate e-mail or internet use, further investigations, including the examination of relevant computer files, records and personal e-mails, may be carried out. This will be conducted by Information and Communication Technology (ICT) staff but always subject to the individual member being advised that this action is to be taken.

- 1.7 The Council automatically monitors internet sites visited from the Council's network for inappropriate content. 'Inappropriate' includes, but is not limited to, material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, describes techniques for criminal or terrorist acts and any other categories as determined from time to time by the HLDS. If it is found that such sites have been visited, the procedure described in 1.6 above will be followed.
- 1.8 The Council's systems are set up so that all external e-mail and files exchanged over the internet pass through the Council's 'firewall' and filtering software to prevent the spread of viruses and malicious software.
- 1.9 All e-mail and attachments are scanned for viruses and inappropriate content. If any are found the e-mail is withheld. A message to that effect is returned to the sender and, for incoming mail only, to the recipient. The e-mail Administrator in the ICT Unit is informed of any virus or inappropriate content.
- 1.10 It must be understood that e-mail is not secure and that no personal, confidential or sensitive material should be sent by e-mail without careful consideration. For example it is possible that technical staff may see isolated messages just as telephone engineers may overhear telephone calls, or a hacker may intercept an e-mail. Council staff are required to maintain the privacy and confidentiality of any message inadvertently viewed.

2. General rules

- 2.1 The Council Internet and e-mail system is primarily for business use, but occasional and reasonable personal use is permitted. **However, you must not allow third parties to use the system.** Remember that misuse of council resources is a breach of the Code of Conduct.
- 2.2 Council-owned equipment, such as a laptop computer, or facilities, such as a St Edmundsbury email address, cannot be used for any party political purposes. If you do so, you could be breaching the Code of Conduct and could also cause the Council to breach the rules about not using resources to support political parties.
- 2.3 The use of web based e-mail services such as Microsoft Hotmail is prohibited, as this bypasses the Council's full security system. All e-mail should be sent/received using the corporate e-mail system.
- 2.4 For external e-mails, the Council System will automatically add a Council disclaimer. However, if you send a personal e-mail sign off the e-mail with the following statement:

PERSONAL E-MAIL: *This e-mail is personal. It is not authorised by or sent on behalf of St Edmundsbury Borough Council. This e-mail is the personal responsibility of the sender.*

- 2.5 E-mails are not to be sent nor Internet pages accessed if the contents are likely to be illegal, could bring the Council into disrepute or could make the Council liable to action against it. Examples include but are not limited to material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, describes techniques for criminal or terrorist acts, or otherwise represents values which are in the opinion of the Chief Executive Officer inappropriate to the Council's activities or could bring the Council into disrepute. **If it is justifiable in terms of legitimate Council business to access a website which could fall into any of the above categories, a member may do so, but is advised to notify their group leader or Assistant Director (HR, Legal and Democratic Services) of the reason for doing so.**
- 2.6 Sending viruses and hacking into any e-mails or computer systems of the Council or outside the Council are strictly prohibited and is illegal.
- 2.7 The Council's Internet or e-mail facilities must not be used for personal gain.
- 2.8 Take advice from ICT before using your council equipment to sign up to social media, such as Facebook or YouTube.
- 2.9 Keep all passwords secure and never write them down.
- 2.10 Access to another person's e-mail is only allowed with the authorisation of the owner or the ICT & eServices Manager.
- 2.11 Remember the Freedom of Information Act (FOI). All emails sent from or received by your council equipment are subject to FOI and will be provided to anyone making a relevant request for information under the Act. Ask yourself, before sending an e-mail, how you would feel if your message were read out in court. E-mail messages may have to be disclosed in litigation.
- 2.12 If your email contains information which could identify a living person, such as a name or address, this must not be disclosed without their prior consent, otherwise you will be **breaking the Data Protection Act**. Contact Legal Services if you need further advice.
- 2.13 Take care about the style you use, be friendly, businesslike and brief but not curt.
- 2.14 **Do not:**
- (a) impersonate any other person (such as using another's password) when using e-mail and do not alter messages received;
 - (b) attempt to bypass the Council's security controls;
 - (c) introduce software or any electronic media onto the Council's system without the prior permission of the ICT Unit. This includes software, shareware and freeware available on the Internet;

- (d) use **bold** or UPPERCASE lettering unnecessarily. This is known in e-mail terms as shouting;
- (e) create e-mail congestion by sending trivial messages or personal messages or by copying e-mails to those who do not need to see them. Do not engage in trivial banter;
- (f) misuse the 'Reply to all' button, or comprehensive distribution lists. The system becomes clogged with unnecessary items. Make sure only those who need to see them receive your messages;
- (g) send or forward chain letters of unsolicited mail (SPAM).

2.15 **Do:**

- (a) use appropriate language. Emails tend to be more informal than printed letters but always have the reader in mind – sometimes a level of formality may be more appropriate;
- (b) obtain confirmation of receipt (e.g. asking the recipient to send an e-mail reply) for important e-mails sent. Don't rely on "view acknowledgements" as this is not supported on all e-mail systems;
- (c) keep copies of important e-mails received and delete unwanted e-mails regularly including emptying your deleted items folder;
- (d) check your e-mail regularly, at least once each working day;
- (e) make arrangements for your e-mail to be forwarded to, or accessed by, someone else in your absence. Use the 'Out of Office Assistant' under Tools in Outlook to inform senders and use it to make arrangements for your e-mail to be forwarded as appropriate;
- (f) reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will/should be sent;
- (g) acknowledge internet derived material in Council documents. See also Copyright below;
- (h) if you accidentally visit a site with inappropriate content or receive such e-mails, immediately inform the ICT Help Desk.

3. Problem areas

3.1 Harassment

You could be held liable for harassment of fellow members, officers or the public if you send e-mails of a bullying or offensive nature. Such behaviour could also be a breach of the Code of Conduct.

3.2 Defamation

Inflammatory or derogatory messages sent through the internet can be held to be defamatory if the message is likely to be available to readers other than the person referred to and the recipient. A defamed party could personally sue the sender for large sums in damages.

3.3 Copyright

Copyright laws protect most material appearing on the internet and some attachments to e-mails. Both the employer and the employee could be liable under civil and criminal law for any unauthorised copying of those materials by the employee.

3.4 Pornography

Displaying on screen, printing or transmitting material with a sexual content could constitute criminal offences.

3.5 Confidential information

E-mails are not necessarily a secure way of sending information. Not only could it be embarrassing for the organisation if sensitive or confidential information of its own is publicly disclosed, but disclosure of a third party's confidential information, for example that of a client, could expose it to negligence actions and commercial risk. Members are reminded that disclosure of confidential information is a breach of the Code of Conduct.

3.6 Freedom of Information

Members will receive guidance on the Freedom of Information Act, including the recommended time limits for keeping e-mails before deletion.

3.7 Amendments

The Council may amend this Policy at any time and users will be notified of any changes made.