

# KNOWSLEY METROPOLITAN BOROUGH COUNCIL

## Policy on the use of Computer Equipment & Systems (including Email and Internet Facilities) by elected Members

Version 1.4 (April 2007)

### 1. Introduction

- 1.1 New technology offers major opportunities to improve the way we work and communicate. Email, internet, intranet and mobile technologies (including mobile telephones) facilitate the means both to provide information and services to the community and gain access to a wide range of information and services in an increasingly flexible manner. Knowsley Council has developed as an innovative user of Information Technology (IT) in service delivery, and is committed to continuing to explore the potential benefits of IT.
- 1.2 The Council believes that IT facilities will increasingly benefit both the organisation and the Borough as a whole and that mobile technologies and email will improve the Council's communications systems. The use of these facilities is therefore to be encouraged, although it is recognised that the Council's IT facilities are predominantly for business use.
- 1.3 **All elected Members are provided by the Council with the loan of IT equipment to assist and support them in undertaking their roles and responsibilities as Members during their period of office. The use of these facilities carries with it a significant personal responsibility for Members, who must ensure that the equipment and facilities provided are always used within appropriate guidelines. This Policy is designed to protect the Council, its data and security by giving guidance to Members on the appropriate use of the Council's IT facilities, and to providing information on the types of use that may be considered inappropriate.**
- 1.4 **This Policy is intended for all elected Members of Knowsley Council. Members should be aware that non compliance with this policy may place the Council's IT infrastructure and the data contained within it at serious risk and may result in the matter being referred to the Council's Standards Committee or action being taken by the Monitoring Officer.**

### 2. Council Email Facilities

- 2.1 The Council encourages the use of email as an efficient form of communication. In common with other forms of communication, Members may utilise email facilities for their own personal use. Members must however note the requirements in paragraphs 2.2(b) below regarding the use of a disclaimer and paragraph 6.10, which prohibits the use of the Council's IT facilities for personal business use.

2.2 It is important to note that the legal status of an email message is similar to any other form of written communication (see paragraph 6.5 below). Consequently, any email message sent from a facility provided for business use could be considered to be an official communication from the Council and could be subject to disclosure to third parties under the Data Protection Act 1998 or the Freedom of Information Act 2000. Given the availability of personal use, and in order to ensure that the Council is protected adequately from misuse of email, the following controls will therefore be exercised:

(a) in accordance with the Council's policies and values under no circumstances should Members communicate material (either internally or externally), which is, for example, defamatory, obscene (see paragraph 6.9 below), racist, or which could reasonably be anticipated to be considered inappropriate. A Member who is unclear about the appropriateness of any material should consult the Monitoring Officer.

(b) Members choosing to make personal use of email facilities must use the disclaimer set out below.

*"This email is personal. It is not authorised by, or sent on behalf of, Knowsley MBC. This email is the personal responsibility of the sender."*

(c) Members must take steps to ensure that due care is taken with regard to the transmission of confidential material via email (see paragraph 6.3 and 6.4 below). In cases where material is sensitive, it is suggested that email is not an appropriate form of communication. If a Member is uncertain or unclear as to the appropriateness of sending certain information by email, they should discuss this with the Monitoring Officer.

2.3 In order to ensure that the systems enabling email are available and perform to their optimum, Members must avoid sending unnecessary messages. In particular, the use of the "global list" of email addresses, or sending emails with large attachments, is discouraged, and should be replaced by use of the intranet, Sharepoint portal work areas, or appropriate addressee groups. Similarly, email users must manage their email accounts to ensure that items are regularly filed, archived, or deleted. Members should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the Council's IT systems.

2.4 Email users should take steps to utilise the available automated reply facilities during periods of absence to ensure that communications (and the absence of replies) are not misunderstood.

2.5 Whilst respecting Members' privacy, the Council maintains its legal right, in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, to monitor and audit the use of email by Members to ensure adherence to

this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of these regulations and in such a way as to comply with the provisions of the Data Protection Act. Members should therefore be aware that they can have no expectation of privacy in relation to their use of the Council's email facilities.

### 3. Internet

- 3.1 The Council encourages the use of the internet as an efficient form of communication and research. Members may utilise internet facilities for their own personal use. However, Members wishing to place orders for personal goods or services via the Council's IT facilities must always make full use of the standard email disclaimer set out in paragraph 2.2 (b) above. Members must also take note of the comments set out in paragraph 6.10 below regarding personal business use.
- 3.2 Members who access to internet email services such as 'Hotmail' and 'Yahoo Mail', using Council IT equipment, must use the email provider's standard internet interface to the email service (i.e. Hotmail email accounts should only be accessed via hotmail.co.uk and Yahoo email accounts via yahoo.co.uk etc. via the council's standard internet access route, which is a protected environment). Members must not use third party software, such as 'Outlook Express', to access personal email accounts on Council equipment as this may interfere with the filtering and virus protection software and place the Council's network and data at risk.
- 3.3 Access to the internet from Council IT equipment must be undertaken through the Council's Internet Service Providers (ISP). Under no circumstances should software from other ISPs (such as Yahoo, BT, Wanadoo, Tiscali, Tesco.net etc) be loaded or downloaded onto Council IT equipment. Such action will reduce the effectiveness of the Council's security procedures and could place the Council's network and data at risk.
- 3.4 The Council's internet facilities are provided via a filtering system, which is designed to ensure that inappropriate use is avoided. The Council receives and monitors regular reports of attempts to access information which are prevented by the filtering system. Any Member wishing to add a site to the list of those barred from access should contact the Information Technology Division's Service Desk or email "ITD Service Desk", and report an "Internet Access" call, providing the full internet address of the site in question. Confirmation of the action taken will be provided. The Council maintains its legal right, in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, to monitor and audit the use of internet facilities by Members to ensure adherence to this Policy and Members should therefore be aware that they can have no expectation of privacy in relation to their use of the Council's internet facilities. Any such interception or monitoring will be carried out in accordance with the provisions of that Act.

- 3.5 Misuse of internet facilities by Members will be deemed to be a breach of this policy. Misuse would include visiting, viewing, or downloading any material from any web site containing sexual, racist, or illegal material, or material which could reasonably be anticipated to be classed as offensive or obscene. Any Member who accidentally accesses such a site or receives a “red hand” or other form of warning from the Council’s filtering system, must inform the Monitoring Officer immediately.

#### 4. Security

- 4.1 As the use of IT facilities is fundamental to the business of the Council, it is imperative that all Members take personal responsibility for the security of the facilities and physical assets (particularly portable items) available to them. It is every Member’s responsibility to comply fully with the Council’s IT Security Policy.
- 4.2 Access rights and privileges are based on business requirements and are subject to individual log-in user names and passwords. The integrity of electronic systems depends on password protection. Members must ensure that passwords are not communicated or shared, are suitably obscure, and are changed regularly. Members must ensure that unattended equipment is appropriately protected. If Members need to leave their IT equipment unattended, the use of the password protected screen saver, that is supplied with every PC/laptop, is mandatory. Advice on such security procedures is available on the Council’s intranet. Where failure to secure an IT system results in data being compromised, or if evidence of fraud or error is identified, the Member to whom the password relates will be required to demonstrate that they have followed the requirements of this policy. The failure to secure passwords or access may, therefore, lead to the matter being referred to the Council’s Standards Committee or action being taken by the Monitoring Officer.
- 4.3 The potential for contamination of software and data files through computer viruses is significant. Consequently, full use must be made of the Council’s anti-virus software, and any suspicious material (e.g. emails from unknown origins) must not be accessed without advice from the Information Technology Division (see paragraph 6.6 below). Any material to be accessed from external sources, e.g. floppy disks, CDs, etc., must be subjected to a full virus check beforehand in accordance with the Council’s IT Security Policy.
- 4.4 Members are reminded that the use of unauthorised software on Council facilities is strictly forbidden. In particular, there must be no downloading of software including, but not exclusive to, updates, patches and screen savers, as these can be a prime source of virus contamination. Any queries or requests for authorisation should be directed to the Head of Democratic Services. Requests will be considered on the basis of business need and in consultation with the Head of the Information Technology Division. Members should note that failure to comply with this requirement presents a considerable risk

to the Council's communications network and its data and will be considered to be a breach of this policy.

- 4.5 The use of web "pop up" blockers must be limited to those approved by the Information Technology Division. Utilisation of other pop up blocking facilities has been shown to interfere with Council web based computer applications, and such use can adversely affect business continuity.
- 4.6 Non-Council equipment must only be connected to the Council's IT equipment or to its communications network with the prior written approval of the Head of Democratic Services in consultation with the Head of the Information Technology Division. This includes, but is not exclusive to, personal laptops, personal digital assistants (PDAs) and mobile phones. Failure to comply with this requirement would present a considerable risk to the Council's communications network and its data and will be considered to be a breach of this policy.
- 4.7 Members provided with Council equipment (including, but not exclusive to, laptops, tablet PCs, PDAs and mobile phones, etc) for use away from the Council's offices must obtain authorisation from the Head of Information Technology prior to connecting such equipment to any other computer network, including wireless connections and the internet, as such action can result in virus contamination.
- 4.8 Members are reminded of the requirement to take adequate precautions to secure portable equipment at all times. Equipment should not be left unattended and should be kept locked away and out of sight when not in use; do not leave any equipment on display, especially in vehicles. Hardware security keys must not be stored with laptops.

## 5. Training

- 5.1 As an accredited Investor in People employer, the Council is committed to providing training and development for its Members.
- 5.2 Email and internet training opportunities will be made available to all Members who have access to these facilities. For further information on IT training, Members should contact the Members' Services Unit.
- 5.3 All new Members will be made aware of this Policy as part of their induction.

## 6. Other Matters

### Copyright

- 6.1 Although the internet was designed to be a free provider of information, it is possible to download computer software, magazine articles, reports, music and photographs, which may be protected by copyright or related rights. If such material is copied by being downloaded where there is no express or implied permission to do so, copyright may be

infringed. Members must therefore take appropriate steps to ensure that any material downloaded is done so legally. Members are reminded of the restrictions regarding the downloading of software as set out in 4.4 above.

- 6.2 Copyright exists in all recordings and it is illegal to copy them in whole or in part for any purpose without the permission of the copyright holder. Accordingly the Council's IT facilities must not be used for unauthorised copying of recordings from whatever media [including CD and DVD] that will infringe copyright.

#### Breach of Confidence

- 6.3 As material can be easily forwarded and copied by the use of IT facilities, a breach of confidence may be more likely to arise. If confidential information is provided to the Council and is used by a third party without authorisation, the Council could become liable in respect of a breach of confidence. Members may therefore seek advice on confidentiality and the use of confidential information from the Monitoring Officer in the first instance and should have in mind the Council's Code of Conduct for Members when using confidential information.

- 6.4 The Council's banking details must not be supplied to any person or organisation without prior authorisation by the Borough Treasurer. This includes all aspects of e-commerce.

#### Contractual Relations

- 6.5 Provided that an external party reasonably believes that a Member has the authority to negotiate, or enter into, an agreement, then the Council will be bound by the Member's actions. Emails sent by Members are usually acknowledged as originating from the Council, so recipients will in most cases be acting reasonably if they assume that they are sent with the Council's authority. Members must consequently exercise particular care in sending emails to external parties.

#### Negligent Virus Transmission

- 6.6 If a computer virus is transmitted to another organisation, the Council could be liable if there has been negligence in allowing the virus to be transmitted. Members must therefore comply with the requirements for virus checking. If any Member has concerns about possible virus transmission, he/she must report these concerns to the Information Technology Division.

#### Data Protection

- 6.7 All Members must comply with the data protection principles, which include a requirement that computer systems are secure. Information on data protection issues is available from the Council's Information Officer at [information.officer@knowsley.gov.uk](mailto:information.officer@knowsley.gov.uk). Members must maintain the same standards of confidentiality when working on

material or documents either at the Council's offices or elsewhere (including at home).

#### Obscene Material

- 6.8 The publication of obscene material is a criminal offence. The definition of "publication" includes electronic storage or transmission of obscene material.

#### Personal Use

- 6.9 Consideration must be given to the volume of personal files stored on PC/laptop drives; in particular images, music and video files are by their nature large and will occupy considerable amounts of disk space. One Gigabyte of disk space is deemed an appropriate limit for personal files.

#### Personal Business Use

- 6.10 Members must not under any circumstances use the Council's IT facilities for the conduct of personal businesses. The use of any IT facilities in this manner may be referred to the Standards Committee or be subject to action by the Monitoring Officer, as the conduct of such personal business may be viewed in legal terms as having been approved by the Council. For clarification, the definition of "personal businesses" for the purposes of this Policy relates to the carrying out of a commercial concern, rather than individual transactions. For example, the use of IT facilities to book personal travel arrangements is permissible, whereas the use of facilities to buy and sell goods on a wider commercial basis is not.

Knowsley Council

November 2001

Updated: June 2004, April 2006, April 2007

Date of Next Review: April 2008