Ealing Council

Acceptable Use of Electronic Communications Policy

Classification:	Internal Use
Date Created:	18.01.08
Doc Ref:	IS.A11.2
Release Date:	
Author:	Marlene Whyte
Job Title:	Information & Data Compliance Manager
Owner:	Business Services Group/Information and Data Management

Document Change Control			
Date	**Change Description**	**Release**	**Version**
18.01.08	Initial document creation	Draft – For Discussion	0.1
21/08/08	Revision incorporating comments	Final Draft	1.0

Distribution This document has been distributed to:

Name	Title / Role	Date of Issue	Version
Diane Malpass	Head of Information & Data Management	24/01/08	Draft – For Discussion
Catherine Taylor	Head of Litigation	24/01/08	Draft – For Discussion
Teresa Bengey	Head of Audit & Investigation	24/01/08	Draft – For Discussion
Jacqueline Wiltshire	Director of Human Resources	29/07/08	Draft – For Discussion
Clementine Adewunmi	Knowledge Manager	24/01/08	Draft – For Discussion
Anthony Kemp	Director Business Services	16/09/08	Draft - For Approval

Policy Approved By			
Title/Role	**Name**	**Date approved**	**Version**
Director of Business Services	Anthony Kemp	16/09/08	1.0

Contents

Introduction

Electronic communication plays an essential role in the conduct of the Council's business, with the Council's workforce making extensive use of the electronic communication systems and facilities both within the organisation and externally with other organisations and customers.

The Council values every authorised user's ability to communicate with colleagues, clients, customers and business partners and has invested substantially in information and communications technology (ICT) that will enable them to work more efficiently and effectively.

An electronic address, number or account identifies, not only the user but also the Council as a business organisation and as such, any activity engaged in by the user will also reflect on the Council.

Purpose

This policy defines the conditions under which these systems and facilities may be used and the standards of behaviour expected of all users. It will also:

- Ensure that the Council's electronic communication systems and facilities are used for purposes appropriate to the Council's business;
- Inform users of the applicable laws and policies and ensure compliance with those laws and policies;
- Avert disruption to and misuse of the Council's electronic communications systems and facilities; and
- Establish rules on privacy, confidentiality, and security in electronic communications;

Scope

This policy applies to all:

- Electronic communication systems and services owned, leased or managed by the Council or provided by the Council via contracts and other agreements. This includes but is not limited to:
    - Internet/Intranet;
    - Email;
    - Telephones (landline and mobiles (including WAP enabled);
    - Laptops and Personal Digital Assistants (PDAs),
    - Voicemails;
    - Videophone/video conferencing
    - Faxes, scanners, printers & photocopiers (including Multi-function Devices)
- Users granted authorised access to and any uses made of the Council's electronic communication systems and facilities whether the user is office based or working remotely (Mobile and home working);
- Electronic communication records created or received by users of those systems and services including the content of attachments and transactional information.

To support this policy and to assist users in their use of the electronic communication systems and facilities stated above, good practice guidelines have been produced.

Provision and Use

All users granted access to the Council's communication systems and facilities are reminded that these services are provided primarily to support the provision of the Council's business and services.

The Council is a legal entity and as such, all correspondence including emails is considered to be legally binding. Users are responsible for the content of all text, audio and images that they transmit

using any of the Council's communication systems. The Council reserves the right to withdraw the use of these facilities at any time.

Confidentiality and Security

All users of the Council's communication systems and services will inadvertently be involved in the processing of confidential business information and personal data as part of the service function. Breaches of confidentiality and privacy can occur as a result of inappropriate handling of data, the unintentional transmission to an external sources or its unauthorised interception by unknown entities. In order to protect the confidentiality and privacy of data during transmission all users must comply with the law of confidentiality, the Data Protection Act 1998 and the Council Information Security and Data Protection policies (see Appendix1).

Confidential and personal information should never be transmitted without the appropriate level protection; consideration should be given to the nature of the content or the method of communication prior to transmission.

Statement of principles

Acceptable Use

Use of the Council's electronic communications systems and services are subject to the following conditions:

- Electronic communications systems, services and facilities are provided to support the legitimate business needs and administrative requirements of the Council;
- Electronic communications pertaining to the administrative business of the Council are considered public records whether or not the Council owns the electronic communication systems, services or facilities used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print, or record them, and are subject to the Council's Records Management policy;
- Information relating to our customers and some of our business operations are confidential. All such information must only be used for the purpose(s) intended and not disclosed to any unauthorised third party (this may sometimes include other employees of the Council). Confidential information should never be transmitted without appropriate protection; **Consideration must be given to the nature of the content or the method of communication used and the appropriate standards of security must be is exercised, such as encryption or a secure connection;**
- Reasonable use may be made of electronic communication systems and services for **incidental personal purposes** provided that:
    - The systems are not used for private business or other commercial purposes, including the private sale or purchase of goods and services;
    - Use of the systems do not interfere with the normal performance of your duties and there is no breach of the prohibitions identified in this policy;
- Any abuse of the systems, services and facilities is reported immediately once users become aware of any taking place;
- Any uses that violate other Council policies, procedures or guidelines.

Unacceptable Use

Electronic communication systems and services **will not** be used to:

- Take part in or aid and abet any criminal action including (but not limited to) offences under the following acts:
    - The Data Protection Act 1998,

  - Human Rights Act 1998,
  - Computer Misuse Act 1990,
  - Copyright, Design and Patents Act 1998,
  - the Obscene Publications Acts1959,
  - Equal Opportunities law,
  - Protection from Harassment Act 1997.

- Transmit, download, retrieve or store any messages, attachments, images or pages that contain offensive, libellous, defamatory or obscene material including but not limited to, pornographic, racist, terrorist, anarchic, insulting and sexist material;
- Download store or transmit messages, images or pages that are intended to harass, intimidate, persecute, terrorise or bully other users relating to but not limited to gender, age, race, sexual orientation, religion, disability or other similar issues (including 'jokes');
- Introduce or transmit pirated or unauthorised commercial software or deliberately spread computer viruses, worms or Trojan horses or programmes that create trap doors or sustain high volume network traffic that substantially hinders others in their use of the network, deliberately corrupt, modify or erase data or programmes intentionally interfering with the normal operation of the council's network; use the facilities in such a manner that would inhibit, distract or have a detrimental affect on Council services;
- Introduce copyright material without the owner's permission onto the Council's network;
- Transmit or upload personal, sensitive personal or confidential information without the appropriate safeguards, such as encryption;
- Overload or disable the system, services or facilities or attempt to disable or circumvent any security mechanisms intended to protect the privacy or security of the system, service or facility or any associated information, records or messages;
- Employ a *false identity or hide* the identity of the sender or tampering with the communications of others;
- Abuse the services and computer facilities in such a way that wastes resources (including employee time), denial of service, global mailings etc. not taking appropriate care in terms of limiting file sizes and maintaining archives of messages sent and received, this refers to the size that will have a detrimental impact on the performance of the network
- Access, receive or transmit electronic communications to participate in or circulate inappropriate or non-business related material to others including (but not limited to) chain letters, business opportunities, jokes, electronic greeting cards, executable files, Items for sale, entertainment software, gambling or betting, financial markets, sport scores, social networking or any other bulletins that are not business related;
- Operate a business or participate in any pursuit geared to personal gain for themselves or an acquaintance or enter into any contractual arrangement using a Council electronic identity and/or address as any part of a personal contract with a third party;
- Promote personal views that are detrimental to the Council or commonly regarded public decency or participate in discussions that are politically sensitive or controversial or give advice of information that they know to be contrary to the Council's policies and interests;

Exceptions to the above will apply to employees who, as part of their job function, have to access material that may contravene the prohibited uses listed in this policy. All such employees will need authorisation from their line managers in order to access such material.

Monitoring

The Council may monitor its business communications to:

  - Provide evidence of business transactions;
  - Ensure the accessibility of business records

- Ensure that the Council's business procedures, policies and contracts with staff are adhered to;
- Comply with legal obligations
- Observe standards of service, staff performance and for staff training;
- Prevent and/or detect unauthorised use, abuse or any criminal activities taking place using the Council's communication systems and services; and
- Maintain the effective operation of the Council communication systems

The Council does not monitor the content of electronic communications as a matter of course, because it is recognised that it may constitute a breach of an individuals human rights. **However, if misuse is suspected which contravenes this policy or the Council deems it to represent a threat to the security of Council systems, the Council reserves the right to inspect the content of any messages without authorisation from or notification to the sender and/or the recipient, in line with the Lawful Business Practice Regulations and the Information Commissioner's Employment Practices Code Part 3.**

Responsibilities

Users – have a responsibility to:

- Read and comply with the requirements of this policy
- Keep up-to-date with the latest requirements of the policy

Line Managers - must ensure that all users within their area of responsibility are aware of and adhere to this policy at all times.

Business Services Group – is responsible for

- The maintenance and review of this policy
- The provision of guidance in support of this policy
- Undertaking adhoc compliance reviews

Policy breach

Failure to adhere to this policy would constitute a breach of the Council's code of conduct and will be considered a serious disciplinary offence, dealt with in accordance with the Council's disciplinary procedure. This could lead to a termination of employment for employees, termination of a contract in the case of service providers or consultants, and expulsion in the case of student placements.

Additionally, individuals may be subject to civil or criminal prosecution if illegal material is involved or legislation is contravened. The Council will not hesitate to bring to the attention of the appropriate authorities any use of its communication systems and facilities that it believes might be illegal.

Policy compliance

To ensure compliance with this policy adhoc reviews will be undertaken periodically

Policy review

This policy will be reviewed annually. It will be amended in response to changes in operational and legal requirements. Every effort will be made to ensure individual users are made aware of changes when they occur.

The most current version of the policy will always be available on the Intranet and on request from the HR Shared Service Centre.

If you have any queries or questions about this policy contact the Information and Data Compliance Team on ext: 9606 or 5354 or 6034.

Related policies, procedures and guidelines

The following policies and guidance should be read in conjunction with this policy:

- Code of Conduct
- Acceptable Use of Information Resources policy
- Data Protection Policy
- Information Security Policy
- Records Management Policy
- Disciplinary Policy and procedure
- Electronic Communications guidance

Appendix 1

DEFINITIONS

Knowledge of these definitions is important to an understanding of this policy.

Electronic communications
Any transfer of signals, writings, images, sounds, data or intelligence that is, created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems.

Electronic communication systems and facilities
Telecommunications equipment/systems used as a means of sending, receiving and displaying communications electronically through connected computer systems.

Electronic communication records
The content of electronic communications

Encryption
To convert data from its original form to a form that can only be read by someone that can reverse the encryption. The purpose of encryption is to prevent unauthorized reading of the data.

WAP
The open international standard for applications that use wireless communication. Its principal application is to enable access to the Internet from a mobile phone or PDA.

Relevant Legislation

Computer Misuse Act 1990
This Act makes it an offence for an unauthorised person to access knowingly a program or data or for such a person to modify knowingly the contents of a computer. The Police and Justice Act 2006 have increased the penalties under this act.

Data Protection Act 1998 (DPA)
This Act regulates the processing of personal data by organisations employers.

Human Rights Act 1998
There may be human rights implications to consider when investigating misuse. Inspecting or monitoring electronic communications may infringe the employee's right to respect for his or her private life (Article 8), particularly if s/he has a reasonable expectation of privacy, if the employer has given no warning that it may undertake monitoring.

Protection of Children Act 1978; Criminal Justice Act 1988
These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Sex Discrimination Act 1975, Race Relations Act 1976 and Harassment Act 1997
These Acts outlaw sex and race-based discrimination. Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities has played a role. The employer could be liable, unless it has taken steps to reduce the risk of such e-mails being distributed.

Obscene Publications Act 1959
This Act makes it a criminal offence to send material to another person which is likely to 'deprave or corrupt' the recipient (those likely to read, see or hear it). There are tighter provisions relating to the

handling of child pornography, under the Criminal Justice Act 1988 and the Protection of Children Act 1978.

Copyright, Design and Patents Act 1988
This Act applies to digital and electronic publications as much as it does to books and other forms of writing. Where permission has not been granted, individuals and the Council could be liable to civil proceedings by the author.

Regulation of Investigatory Powers Act 2000 (RIPA)
This Act regulates the interception of communications by public or private telecommunication systems. The **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** - these regulations temper the requirements of RIPA and allow certain monitoring in the course of legitimate business practice. Therefore e-mail (and telephone) monitoring is allowed without consent for the following reasons:

- Quality control monitoring
- Combating crime
- Combating unauthorised use of the system (for instance, investigating suspected misuse of e-mail or internet)
- Determining whether the communication is business-related (this allows an employer to inspect the inbox of an employee who is absent from work, in order to check whether any business-related e-mails have come in).

Defamation Act 1996
This Act exists to protect the reputation and good standing of an individual. Defamation is a false statement made by one individual about another. This statement attempts to discredit that person's character, reputation or credit worthiness. In order to be defamatory, such a statement must be communicated to at least one other person. If such a statement is spoken then it is described as slander. However, if it is written, broadcast or shown in a film it is described as libel.