STANDING ORDERS
RELATING TO INFORMATION and COMMUNICATIONS TECHNOLOGY

INDEX

STANDING ORDERS RELATING TO INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

1 PURPOSES

1.1 The purposes of these Standing Orders are: -

To ensure that all of the Council's ICT-related assets (including hardware, systems, programmes, data, information, and standards) are correctly used and adequately protected against accidental or deliberate damage, destruction, or loss.

To ensure that Council Members and employees are aware of and comply with ICT security and confidentiality issues and relevant legal requirements.

To identify individual responsibilities in maintaining appropriate levels of ICT security and ensuring that the confidentiality, accuracy and integrity of Council information is protected from unauthorised access.

1.2 All users of the Council's ICT facilities shall comply with all legal requirements including those in the Data Protection Act 1998, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, Copyright, Designs and Patents Act 1988 and the Computer Misuse Act 1990. The law on written communications applies equally to e-mail messages, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information and wrongful discrimination.

1.3 Breaches of these Standing Orders and of the instructions will be treated very seriously and appropriate action will be taken which may involve individuals in disciplinary proceedings and/or criminal proceedings and removal of access rights.

2 RESPONSIBILITIES

2.1 **The Operational Director – ICT and Support Services:-**

- is the ICT adviser to the Council and the Management Team and will advise on ICT strategy, policy, technical infrastructure and best practice.
- shall approve and procure all ICT assets and services for the Council and maintain an inventory of such purchases.
- will regularly monitor the usage of software on Council PCs to ensure that it is duly licensed.
- in conjunction with Operational Directors or equivalent ensure that emergency procedures and contingency plans, including the restoration of systems from back-up copies, are fully documented and regularly tested.

- advise on the acquisition and usage of ICT within the Council.

- advise on the prioritisation of ICT projects and the levels of ICT support services required

- advise and make recommendations to the Management Team on the suitability and cost effectiveness of ICT projects having a total cost exceeding £25,000 or that are considered as having a high strategic impact on the ICT Infrastructure and Services of the Council.

2.2 **All Operational Directors** shall:-

- Ensure that staff are aware of and comply with these Standing Orders and associated guidelines both generally and specifically in relation to security and access.
- Ensure that staff are adequately trained in the use of ICT facilities assigned to them.
- Ensure that all electronic data is accurately maintained and kept up to date.
- Ensure that documented procedures are available for staff involved in the access, use or the operational running of ICT systems within their service area.
- Ensure that appropriate levels of access are assigned to staff to enable them to perform their work function and ensure that these access rights are regularly reviewed, and if appropriate, revoked for staff under suspension, moving from a Directorate or leaving the employ of the Council.
- Ensure the optimum use of ICT systems and facilities within their service through the monitoring of usage.
- Ensure that staff are aware of and comply with all Council health and safety requirements associated with the usage and deployment of ICT facilities.
- Ensure, so far as practicable, that organisations with whom the Council is working in partnership are required by contract to comply with these Standing Orders.
- Ensure that there are documented procedures for the regular back-up of locally stored data and that these procedures comply with the Back Up and Recovery Guidelines on the HBCNet and that back up copies are stored away from the source computers, preferably in a different building.
- Ensure that staff are aware of and comply with the documented back up procedures in place.
- Ensure that, where appropriate, employees are asked to sign confidentiality (non-disclosure) agreements.
- Ensure that formal reporting procedures are established in respect of security incidents and software malfunction and staff are made aware of them.
- Periodically monitor use of the Internet by staff.

2.3 **All Individuals (staff and Members)** shall: -

- Be aware of and comply with these Standing Orders and the associated policies, guidelines and departmental instructions.
- Be responsible for their own actions and the use of the Council ICT hardware and software assigned to them.
- Ensure that they are adequately trained.
- Not divulge passwords to others except with management approval.
- Log-off their PCs if they are leaving their PC unattended for any period unless a screen-saver has been enabled with a suitable time delay and password.
- Not use Council ICT facilities for personal use except with prior written management approval.
- Not add any software or hardware to their equipment without prior approval of ICT Services. (This includes “Free-ware”, “Share-ware” and Screen Savers – any of which may contain viruses or may adversely affect the operation of the software and equipment provided.)
- Not remove any pre-installed software or hardware without prior approval of ICT Services.
- Comply with the Back Up and Recovery Guidelines on the HBCNet.
- Be aware that deleted emails remain accessible to management through the Journal.

3. ACQUISITION POLICY

3.1 All projects with a total value of £25,000, or projects that are considered as having a high strategic impact on the ICT Infrastructure and Services, must be submitted to the E-government Steering Group for approval, prior to entering into any contractual obligation for the acquisition of any ICT software or hardware.

3.2 The prior approval of the Operational Director – ICT and Support Services shall be obtained for all ICT purchases prior to entering into any form of contractual obligation for the supply or installation of ICT hardware or software and all ICT acquisitions shall be conducted or managed by ICT Services.

3.3 Operational Directors shall obtain approval from ICT and Support Services for the installation and relocation of ICT equipment and assets.

3.4 All disposals of ICT hardware or software shall be undertaken by ICT and Support Services subject to compliance with Standing Orders Relating to Finance 7.9 (Disposal of Assets).

4. ACCEPTABLE USE

4.1 Access to ICT systems and data shall be controlled on the basis of each user’s business needs and responsibilities.

4.2 ICT equipment and systems shall only be used for their permitted purpose and in the permitted manner by those who have been duly authorised.

4.3 ICT equipment and systems shall only be used for Council purposes unless permitted under the Acceptable Use Policy.

4.4 Where permission is given the manager shall monitor the situation and may withdraw the permission at any time if satisfied that the permitted use is adverse to the interests of the Council.

4.5 ICT equipment and systems shall not be misused nor shall anyone induce or allow others to misuse such equipment and systems.

4.6 Staff shall be aware of and shall comply with documented procedures relating to the usage and operational running of specific ICT systems.

4.7 Staff shall familiarise themselves with and shall comply with any Council Health and Safety regulations relating to the use of ICT equipment.

4.8 In the event of any conflict between the Acceptable Use Policy and the Standing Orders relating to Information and Communications Technology the Standing Orders shall prevail.

Passwords

4.9 All systems shall be password protected.

4.10 Passwords shall not be disclosed nor shall individuals be permitted access to others' ICT equipment and systems except with the prior approval of the manager. Disclosed passwords must be changed as soon as operationally possible.

4.11 Temporary passwords must be changed at first log-on to an application.

4.12 Passwords shall be changed at least every 90 days.

E-mail and Internet

General Principles

4.13 Use of the Internet by staff and members is permitted and encouraged where such use is for Council purposes and supports the goals and objectives of the Council or otherwise is permitted under the Acceptable Use Policy. The Internet

is to be used in a manner that is consistent with the Council's standards of business conduct and as part of the normal execution of an employee's job responsibility.

4.14 Corporate "generic" email accounts, Internet IDs and web pages should not be used for anything other than corporate-sanctioned communications.

4.15 Use of the Internet/Intranet and E-mail is subject to monitoring for proper use (in accordance with the notice given under the Regulation of Investigatory Powers Act 2000), security and/or network management reasons.

4.16 The distribution of any information through the Internet, computer based services, email, and messaging systems is subject to the scrutiny of the Council. The Council reserves the right to determine the suitability of this information.

4.17 Users should be aware that the medium of e-mail and the Internet is not a secure environment unless formal encryption methods are employed.

4.18 The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately.

4.19 Access to e-mail facilities and Internet facilities for a member of staff or Member shall be subject to the divisional manager or equivalent authorised budget holder completing the relevant form authorising access to the facilities. (Available from the ICT Help Desk).

4.20 The viewing, sending or storage of any discriminatory, defamatory, offensive, oppressive, obscene or pornographic messages, information or other material is prohibited.

Internet

4.21 All access to the Internet shall be through the Council's approved Internet Service Provider (ISP) via the Council's network and 'firewall'. Access to any other ISP through a PC not connected to the Council's network is subject to prior written approval by the Operational Director - ICT and Support Services.

4.22 Fees can be incurred as a result of the unauthorised downloading of files from the Internet. These will be charged directly to the individual employee or section who downloaded the file.

4.23 Managers shall keep records of Internet data access and download fees.

E-mail

4.24 Users shall not solicit e-mails that are unrelated to business activities (except as permitted under the Acceptable Use Policy) or for personal gain.

4.25 Users shall not send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.

4.26 Users shall not represent personal opinions as those of the council.

4.27 Users shall ensure they do not form a “binding legal contract” by inappropriately wording an email to a third party.

Confidentiality

4.28 Users shall not knowingly up-load, access, download, or otherwise transmit unauthorised or pirated material, commercial software or any copyrighted materials belonging to parties outside the Council, or to the Council itself.

4.29 Users shall not reveal or publicise confidential or proprietary information, which includes, but is not limited to:- financial information, new business ideas, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/network access codes, and business relationships.

Security

4.30 Users shall not download any software or electronic files without implementing virus protection measures that have been approved by the Council.

4.31 Users shall not intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

4.32 Users shall not examine, change or use another person’s files, output, or user name for which they do not have explicit authorisation.

4.33 Employees shall comply with the security rules of the Government Secure Intranet (GSI) Code of Connection relating to secure email and IT systems usage as set out in the Personal Commitment Statement published on the Halton Borough Council Intranet.

Data and Back up

4.34 Individuals and managers shall back up data on a regular basis and comply with the documented back up and recovery process and test these processes on a regular basis.

4.35 Individuals and managers shall ensure that back up copy data is stored separately and ideally in a different building.

4.36 Individuals shall regularly review their data at least every 90 days and shall either archive the data or, if the data is no longer required, shall delete the data.

4.37 Individuals shall keep their data accurate and timely.

4.38 Individuals shall only keep personal data on their PCs if and to the extent approved by their divisional manager or equivalent.

5. SECURITY

Disaster Recovery

5.1 Operational Director – ICT and Support Services in conjunction with other Operational Directors shall have in place plans for disaster recovery for all the Council's systems.

Unauthorised Software

5.2 Unauthorised and or unlicensed software shall not be installed on the Council's PCs.

5.3 No individual shall make unauthorised copies of software.

Intellectual Property

5.4 All intellectual property rights created in connection with Council work whether by employees or contractors are unless otherwise provided by contract the property of the Council and not of the individual employee or contractor.

5.5 All information created on or transported over the Council's system is private and confidential to the Council.

Monitoring

5.6 All e-mail and internet usage on Council PCs is monitored for, amongst other things, the investigation or detection of unauthorised use and to determine whether messages are business or personal communications.

5.7 All material transferred from the Internet to the Council's computers is screened and virus checked by ICT using the Council's dedicated security software.

5.8 All e-mail traffic is screened by ICT using the Council's dedicated security software.

5.9 Those staff permitted by their managers to use e-mail or the Internet for non-Council purposes should be aware that monitoring takes place to secure the interests of the Council as a publicly accountable body and for the purposes of the Regulation of Investigatory Powers Act 2000 and related legislation and that deleted emails remain on the system and can be inspected by authorised Officers.

Computer Viruses

5.10 All incoming media and software arriving via the internet is virus-checked by ICT.

5.11 Any electronic information brought into the Council must be suitably virus checked.

5.12 The use of diskettes or other media of uncertain or unauthorised origin should be avoided.

5.13 Incidents of suspected or actual virus infection must immediately be notified to the ICT Services helpdesk.

Security of Council Property

5.14 Individuals may only use Council equipment away from Council premises for Council or private purposes with the prior written permission of their manager.

5.15 Individuals who have been permitted to use Council ICT equipment away from Council premises shall exercise due care and attention to ensure the safety and security of such equipment.

5.16 Individuals shall not leave Council ICT equipment unattended in any vehicle.

System Security

5.17 All connections to the Council network and access to systems are monitored and any additions to these must be authorised in writing by the Operational Director – ICT and Support Services.

5.18 “File Sharing” on PCs is not an acceptable practice due to the risk of propagating viruses. If you require such “File Sharing” facilities please contact the ICT Help Desk, who may be able to offer alternative solutions.

5.19 No person shall, without prior written approval from the Operational Director – ICT and Support Services, divulge technical details of the Council’s systems and infrastructure.

5.20 Staff shall make themselves aware of and shall comply with the disclaimers automatically attached to all Internet e-mails.