APPENDIX 11

HILLINGDON
LONDON

ICT Acceptable Usage Policy

May 2018

Contents

1. Scope

1.1. This Policy applies to all those who use Council IT systems (referred to as 'users'):

1.1.1 All Employees of the Council;
1.1.2 Suppliers and Contractors of the Council;
1.1.3 Temporary and Agency Staff engaged by the Council;
1.1.4 Volunteers at the Council;
1.1.5 Others using the Council's information or systems.

1.2. It does not apply to staff employed in schools. Members are governed by the Information and Communications Technology Usage Policy which can be found in the Councils Constitution.

1.3. This Policy covers the use of the Council's network, Council computer facilities, (including telephony, hardware, software, e-mail, internet, etc) used anywhere, for professional or personal purposes whether in working time or in the user's own time.

2 Purpose

2.1 The purpose of this Policy is to:

2.1.1 protect users by making clear what is an acceptable use of the Council's computer facilities;
2.1.2 Protect the security and integrity of the Council and its computer facilities.

2.2 This Policy encompasses the core values from the London Borough of Hillingdon Information Governance Policy; confidentiality, integrity, quality, availability, authentication, access control and auditing.

2.3 High standards of conduct and probity are as relevant to the use of the Council computer facilities as they are to all other aspects of work, and users must conduct themselves in line with the Councils Code of Conduct and Disciplinary Code.

3 **Policy and Guidance**

Access to ICT Systems and Equipment

3.1 The Council provides access to ICT to enable users to undertake their duties. It is important that access to ICT systems is restricted to those staff members and others who are authorised to have access.

3.2 Users must not:

3.2.1 write down their user name and password;
3.2.2 share their username and password with anyone else;
3.2.3 allow other users to log in with their username and password;
3.2.4 leave their PC, laptop or other device unattended at any time without locking the PC keyboard or logging out completely.

3.3 There may be occasions when it is necessary to gain access to files and documents created by a member of staff when the staff member is not available or unable to provide access to the required documents.
Service Managers have authority to obtain access to user's data and documents following a written request to their Deputy Director which should then be forwarded to the ICT Service desk

Personal Use of ICT Equipment

3.4 Users can use the Council's computer facilities for reasonable personal use provided it;
3.4.1 does not interfere with the performance of their duties;

3.4.2 is appropriate;
3.4.3 is on an occasional, rather than a regular or substantial basis;
3.4.4 does not compromise the security of the Council's systems or reputation.

3.5 Users must not charge their personal mobile device (such as a personal mobile phone) by connecting it to Council-owned ICT equipment as this could inadvertently introduce a computer virus into the network.

Inappropriate Use

3.6 Users of the Council are expected to maintain high standards of conduct at all times as set out in the Council's Staff Code of Conduct. Failure to follow the Code of Conduct could lead to disciplinary action being taken against an individual staff member.

3.7 Users must therefore not use the Council's computer facilities to:

3.7.1 send or access messages that are, or perceived to be libellous, harassing or defamatory, or cause offence to the dignity of an individual or group;
3.7.2 access inappropriate internet sites or material. These may include pornographic, racist or any other sites not appropriate for a public authority. In the case of accidental access the user must immediately disconnect and inform their Manager;
3.7.3 store, view, print or redistribute any inappropriate material or data;
3.7.4 access chat rooms, social networking sites or newsgroups for personal use;
3.7.5 advertise or send personal messages to large groups internally or externally unless through the Noticeboard on Horizon;
3.7.6 spread harmful programmes (Malware) that may damage the Council's computer facilities;
3.7.7 download, use or distribute software including entertainment software or games;
3.7.8 download video and audio streaming for personal purposes;
3.7.9 use their Council email address to log into any website (or other on-line system) that is not related to work. This includes gambling, dating, recruitment and social media sites.

Authority to Express Views

3.8 When using Council computer facilities, it is important to remember that employees are representing the Council. Users of Council computer facilities must

communicate the Council's, and not their personal, views. Users must state when they have expressed a professional view rather than the Council's.

3.9 Users must not:

3.9.1 participate in newsgroups / chat rooms / social networking sites to express views, unless in a professional capacity relevant to their duties and with prior agreement from their Service Manager and their Deputy Director, who should then inform the ICT Service desk of their requirement

3.9.2 use the Council or its name to endorse any non-Council commercial product or service.

Confidentiality and Security of Data

3.10 The Council is legally responsible for all information stored or transmitted by its computer systems and for any improper disclosure. Under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), all staff have a duty to protect the information held about the public.

3.11 Residents have a right to know that information about them is kept secure. Breaches of the DPA, through loss or mishandling of personal data, can result in both large fines for the Council and disciplinary action against individual members of staff which may lead to dismissal. All staff have a responsibility at work to look after personal data properly and appropriately.

3.12 Failure to comply with the Council's Data Protection Policy and other Data Protection Policies and Procedures may lead to action under the Council's disciplinary procedure.

3.13 To ensure the Council keeps data safe and secure, users must:

3.13.1 keep User IDs and passwords secure and confidential, and passwords must be changed if an anyone else becomes aware of your password;

3.13.2 carefully address e-mails to avoid sending sensitive information to the wrong recipient;

3.13.3 ensure that data they are storing, updating or transmitting is accurate, and must not amend or alter emails they receive;

3.13.4 use the password-protected screen saver if leaving their computer for short periods and switch computers off at the end of the working day;

3.13.5 keep Council issued equipment safe and secure;

3.13.6 report any theft, loss or damage to Council issued equipment to the Corporate ICT Service Desk immediately.

3.14 Users must not:

3.14.1 attempt to disable or evade any security facility;
3.14.2 install any hardware without the prior, written, expressed consent of the Head of Service and the Head of ICT, or their delegated representative. Any computer used for independent dial-up or leased-line connections must not be part of the Council's network;
3.14.3 allow any non-Council user to access Council equipment, resources or systems.

3.15 To ensure security, it may be necessary to prevent machines with sensitive data from connecting to the Internet, or restrict usage of file transfers.

Copyright, Legal and Contractual Issues

3.16 Downloading and copying data and software or sending the works of others to third parties without permission can infringe copyright. The Council retains the copyright to any original material produced by a user in the course of their duties.

3.17 The Council must ensure all software is legally licensed. Corporate ICT is responsible for managing and maintaining the register of software and for holding licenses and the original media (diskettes, CDs etc).

3.18 The following is expected of users:

3.18.1 Copyright should be checked and appropriate permissions sought. In the case of subscription services the appropriate licences must be obtained
3.18.2 No software can be loaded onto or used on any computer owned or leased equipment unless approved by and licensed to the Council.
3.18.3 All software must be procured and installed by Corporate ICT.
3.18.4 Where a user needs to have knowledge of a software activation key, licence or other code, this information must be confidential.
3.18.5 Software must not be copied or distributed by any means without prior approval from the Head of ICT or their delegated representative
3.18.6 Software can only be downloaded with permission from the Head of ICT or their delegated representative. Downloaded software becomes Council property and must be used only under the terms of its licence. Users must arrange to licence and register such software, where required. Software downloaded without permission may be deleted.
3.18.7 Users must not transfer any software licensed to the Council or data owned or licensed by the council without authorisation from the manager responsible for the software or data.

3.18.8 The use of computer facilities can lead to contractual obligations in the same way as verbal or written transactions. Users must not exceed their delegated authority to enter into contracts or authorise expenditure.

3.18.9 Records of computer transactions must take place through archiving or backup. Where appropriate, confirmation of receipt of important e-mails must be gained from the recipient.

3.18.10 Transactions through computer facilities must be treated in the same way as transactions on the Council's headed paper.

Records Retention and Destruction

3.19 Records should only be retained where there is a justifiable business need and / or legal need to retain the record. Data Minimisation lies at the heart of the GDPR and the DPA. The Council has introduced a new Document Retention and Destruction Policy which must be strictly followed.

3.20 Where electronic records no longer need to be retained, they should be destroyed securely and systematically in accordance with the Council's Document Retention and Destruction Policy.

Network Efficiency

3.21 Maintaining an efficient, secure and safe ICT network helps to provide essential day to day services to Council residents. The Council's ICT Team will scan all files for harmful ICT viruses to keep the Council's systems safe.

3.22 Wherever possible, staff should schedule intensive operations such as large file transfers, video downloads and mass e-mailing during off-peak hours.

Monitoring

3.23 The Council's computer facilities will be routinely monitored to ensure this policy is adhered to and that these facilities are used properly. Any information (including personal emails, documents, etc) within the Council's network or equipment can be inspected, at any time, without notice.

4 Related Policies and Guidance

4.1 Information Governance Policy

4.2 Data Protection Policy

4.3 Records Retention and Destruction Policy and Schedules