PART 5 - CODES AND PROTOCOLS
SECTION C
ICT CODE OF PRACTICE FOR MEMBERS

1. Introduction

1.1 The Council is committed to e-governance and has accordingly agreed to provide equipment to all members of the Council who require it to ensure this aspiration can be achieved. All members of the Council have to be readily accessible by email and be able to receive information electronically. In recognition of the importance the Council views this provision; the Council has adopted the IT Code of Practice as part of the Members' Code of Conduct.

1.2 The sections of this document provide important information regarding the Council's protocol for Information Management. Failure to follow the guidelines detailed in this Code of Practice could lead to a breach of the Members' Code of Conduct.

2. Equipment and Software

2.1 The Council is only responsible for the control and maintenance of computer equipment provided by the Council. The Council provides equipment for the use by Councillors. No responsibility or work will be undertaken by ICT on computer or telephony equipment not provided by the Council. Members using their own computer equipment will be responsible for the cost and maintenance. Support for council provided equipment can only be provided at Surrey Heath Borough Council offices in Knoll Road.

2.2 All equipment and software provided by the Council remains the property of the Council at all times. The equipment provided is solely for the use of the Council Member for whom the equipment is provided and is not to be used by other members of the household, friends or relatives.

2.3 The Member is responsible for keeping the equipment provided in a good condition, subject to fair wear and tear. Due care must be undertaken to keep the provided equipment safe and secure, in accordance with the signed equipment agreement. Equipment must not be left unattended in a vehicle in plain sight and must be removed overnight. In the event of a device being lost which has access to Council information should be reported to the ICT team as soon as possible or by the next working day if over a weekend.

2.4 The Member must return all the equipment supplied by the Council, if the Member ceases to be a Member of the Council, the equipment is no longer required, on request by the Council, or if the Audit and Standards Committee is satisfied that the Member has broken this Code of Practice. The equipment should be returned, or made available for collection as soon as possible and within one month of the above circumstances occurring.

2.5 Access to USB storage is disabled on Council supplied equipment and all data should be saved in provided cloud storage solution.

2.6 Computer output must be disposed of with due regard to its sensitivity. Printed output with confidential or personal details must be shredded. Special confidential waste sacks can be provided by the Council for the disposal of sensitive waste.

3. Training and User Guides

3.1 User notes are normally provided for email, storage and equipment usage. An induction / training session will be provided as part of equipment issue, additional assistance and training can be provided on request through the ICT Service Desk.

4. Passwords / Authentication

4.1 Passwords must be kept secure and must not be disclosed to anyone, except to authorised ICT staff, where required. Passwords must not be written down or displayed in any way that would allow the password to become known to others. Multifactor Authentication (MFA) must be used in combination with a password to further enhance security.

4.2 Access to your Surrey Heath provided account outside of UK is restricted, should you require access outside the UK please provide at least 5 working days' notice to the ICT team.

5. Email, Storage and Internet Usage

5.1 The email, storage and software facilities provided by the Council should be principally used for Council business. Council business is defined as "business which is applicable to the work officially undertaken for the Council and relates to the services of the Council", this may include communication with your constituents. If storing ward work, for example; personal details of complaints, personal data held for constituency purposes, surgery lists, charity association data, canvassing data, political party records or data that does not relate directly to the statutory function of the Council this should be stored in a separate folder so that it can be easily identified to ensure that it is not released under FOI and is not retained by the Council for longer than is necessary. Data should be saved to Cloud storage and not directly to the laptop – ICT cannot be held responsible for any data loss as a result of data being saved directly to the device.

5.2 The Council will provide an official email account, for each Member, using the domain name of surreyheath.gov.uk. This email account should be used for all Council official and work related email sent and received by the Member. Web based personal or non-Council email accounts such as Hotmail and Gmail must not be used for Council business.

5.3 Under no circumstances should a rule be applied to your Surrey Heath provided email account to automatically redirect emails or calendar appointments. This includes to another Council if a Surrey County Councillor or a Parish Councillor.

5.4 As a Member of the Council it is important that appropriate language and style of communication is used. Councillor emails, storage, Teams, Social Media accounts and written communication fall under the Freedom of Information Act and Data Protection Subject Access Rights and need to be made available for release, subject to applicable exemptions being applied, on request from the Information Governance Manager.

5.5 Abusive, harassing or defamatory remarks, fraudulent or obscene messages or materials must not be used within email messages or attachments. The sending or forwarding of chain letters, text jokes, joke images or other forms of mass mailing is also prohibited. Members should always be aware that material that they personally may find inoffensive could be offensive or hurtful to others. Emails should be written in a business-like manner.

5.6 Unacceptable uses of the Internet from council provided equipment include, but are not limited to:

(i) the downloading, transmission or posting of any material which is pornographic, obscene, threatening, insulting or otherwise offensive in nature.
(ii) personal use for product advertisement, recreational or commercial activities.
(iii) any unlawful or illegal activities.
(iv) any other activity which, under the Code of Conduct, would bring the Council into disrepute.

5.6 All external outgoing email will be appended automatically with the Council's standard disclaimer.

5.7 To protect the Council network any suspicious activity or communications should be reported to the ICT Service Desk as soon as possible. You should not click on any links or forward any emails unless you are sure who they have come from and that they are legitimate, if in any doubt at all contact the ICT Service Desk.

6. Use of Social Network Sites

6.1 Members need to assess the risk posed by their individual use of social network sites such as Facebook or Twitter. If a member is unsure of whether to use a social networking or public online site, they should seek advice and guidance from the Group Leader or the Monitoring Officer. Members must be mindful that they follow the Surrey Heath Code of Conduct for Members when they represent Surrey Heath Borough Council on such sites.

7. Software Licensing

7.1 The Council operates software-licensing controls and deliberate downloading of unauthorised software from the Internet onto Council provided equipment is strictly forbidden. Authorised downloads would normally only include Council prescribed apps and documents designed for viewing or printing. Any additional software requests need to be approved by ICT Management.

8. Monitoring of Email, Storage and Teams

8.1 The Council reserves the right to monitor email, storage and Teams usage under the supervision of the Monitoring Officer.

8.2 Council supplied devices will be monitored to ensure they remain in compliance with configuration and updates. ICT have the ability to remotely wipe a device should it be lost or stolen, to maintain security. Devices that do not check-in online within a 90 day window will be automatically wiped (emails and data stored in the cloud will be retained).

8.3 Should a device loose configuration, ICT must be informed and will undertake the enrolment process to ensure the device receives the required policies

9. Abuse of the Code of Practice

9.1 Breach of the Code of Practice, as determined by the Audit and Standards Committee, may result in Council owned equipment being removed and /or wiped.

10. Data Protection

10.1 Elected members have data protection responsibilities for personal information they process in their work. This means they are responsible for making sure all personal data handled by their office is done in a way that complies with the requirements of the Data Protection Act and UK General Data Protection Regulations. Further guidance for Councillors when collecting and processing data can be found in the SHBC Data Protection Guidance for Councillors.

10.2 Elected members are data controllers under the UK General Data Protection Regulation for Ward work. It is the responsibility of each member to identify if they are required to register with the Information Commissioners Office.

10.3 Elected members should use the Council's email and storage facility provided to them by the Council for Council business, if a Councillor chooses to store ward work on the Council provided storage then as the data controller of that data they are responsible for ensuring that this is separated and clearly identified. Information stored on the Council network may be subject to the Council's Freedom of Information procedures and Data Protection policy.

10.4 Councillors are advised that they must not hold personal information for longer than is necessary for the purposes in which they received the information. It is advised to securely delete data when it is no longer required and to run annual

audits of the personal data that they are processing and storing to ensure they are not holding data for longer than is necessary.

10.5 Any data stored on the Council network by the member will be retained until such a time that the member leaves office. When the member has left office the Council will close access to the data and the data will be deleted from the network. Any Member's emails will be retained in line with the Council's email retention policy.

10.6 In the event of electronic or paper medium containing Council personal, sensitive or confidential information being lost or miscommunicated, the Data Protection Officer (Monitoring Officer), Information Governance Manager or ICT Manager must be notified immediately.

10.7 In order to protect themselves and the Council, all Members are strongly encouraged to undertake biennial training in relation to Data Protection.