Councillor Data

Digital Services Guidance

1. Data Controller definitions.

1.1 As a Councillor, you carry out a number of roles, each of which needs to be treated separately in terms of this guidance.

1.2 During your period of office, you may have had access to and have processed personal data in the same way that Council employees do. This information would have been collected and held by yourself on behalf of the Council for Council purposes. In this instance, the data controller is the Council, therefore the data is owned and remains the property of the Council when you leave office.

1.3 "Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

1.4 You may also have collected personal data in your own right as a representative of residents in your ward, for example when dealing with complaints. Some of this correspondence may include information provided in confidence about such matters as the health, sexual orientation or religion of the resident you are dealing with (this is classed as sensitive personal data). You are personally responsible for the protection of this data as Data Controller as defined by the Data Protection Act 1998 and for ensuring that it is not breached to unauthorised parties.

1.5 When officers provide personal data to yourselves to assist with resolving the correspondence, the Council's rules make it clear that it is provided only to help the individual and must not be used for any other purpose. Responsible care for all personal data is laid down as part of the code of practice for Councillors.

2. ICT Allowance

2.1 All Councillors have received an allowance to purchase your own ICT equipment to undertake duties. The Council provided help and guidance to set up email accounts and provide access to a work share drive where data could be saved with regards to your duties. The Council own the email account and work space drive and will be kept and in time deleted by the Council when you leave office.

2.2 Within your time in office, the ICT service desk is available to you for help and guidance with your email accounts. Any help with your ICT equipment is sourced elsewhere.

2.3 As a Councillor, you are aware that they need to arrange for appropriate security to protect personal information. You must have taken into account the nature of the information and the harm that can result. You must have considered what technical and organisational measures, such as use of passwords, computer access privileges, procedures and training, are appropriate to keep the information safe.

3. Classifying data on emails

3.1 You are responsible for classifying data you hold within emails. You must have a clear understanding of what data is owned by the Council and what data is owned by yourselves.

3.2 When you leave office, any data left in your email account will be owned by the Council and kept for a minimum of 13 months before destroying. Any data in this email account will be subject to the data protection act and freedom of information requests.

3.3 We strongly recommend that you delete all personal correspondence with residents from your Council email inbox where you are the data controller, passing unresolved enquiries onto your successor if necessary. If you are proposing to do the latter, you should follow the details in section 5 of this guidance.

3.4 You must transfer any emails that include personal data owned by yourselves to your personal email account. This is achieved by:

- opening up the relevant email
- forwarding it on to your personal email account
- deleting the original email from your Council owned email account

3.5 Once you have left office, you will have access to your Council owned email account until midnight on 8 May 2017 to complete any unfinished business. After that date, access to the email account via any ICT device will be automatically closed. This account will then be owned by the Council and no further access will be given to yourself.

4.0 Classifying data in any storage media

4.1 You are responsible for classifying any data you hold in storage media. This includes the Council owned work space shared drive, USB sticks/CD's and external hard drives.

4.2 When you leave your post, any data left in Council owned storage media will be owned by the Council and kept for a minimum of 13 months before destroying. This data will be subject to the data protection act and freedom of information requests.

4.3 You are responsible for managing your storage media. Prior to leaving your post, you must transfer any personal data owned by yourselves. This is achieved by:

- creating a folder on your personal PC/Laptop
- locating your personal data on the relevant storage media
- moving the personal data from the storage media to the folder on your personal device

4.4 All Council owned storage media must be returned to the Council when you leave your post.

5.0 Passing personal data on to another Councillor

5.1 There may be situations where you represent a resident and may need to pass on that particular individual's personal information to another councillor in the same ward before you leave your post.

5.2 You will only be allowed to disclose to the other ward councillor the personal information that is necessary:

- to address the resident's concerns;
- where the particular issue raises a matter which concerns other elected members in the same ward; or
- where the resident has been made aware that this is going to take place and why it is necessary.

5.3 If a resident objects to a use or disclosure of their information, their objection should normally be honoured.

6.0 Data Protection duties

6.1 Your duties under the Data Protection Act apply throughout the period when you are processing personal data – as do the rights of individuals in respect of that personal data. You must comply with the Act from the moment you obtain the data until the time when the data has been returned, deleted or destroyed.

6.2 Your duties extend to the way you dispose of personal data when you no longer need to keep it – you must dispose of the data securely and, in a way, that does not prejudice the interests of the individuals concerned.

6.3 Here is a brief overview of the responsibilities you hold when in possession of personally identifiable data. This brief underpins the DPA (Data Protection Act) 1998; the full guidelines and responsibilities can be found within the DPA itself:

- The Data Protection Act 1998 (DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those that are responsible for processing it

- When councillors consider using personal information, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful, as required by principle 1 of the DPA.

- Where a councillor is representing an individual resident who has made a complaint, the councillor will usually have the implied consent of the resident to retain relevant personal data provided and to disclose it as appropriate. The resident will also expect that the organisations (including the local authority) who are the subject of the complaint will disclose personal data to the councillor. If there is any uncertainty regarding the resident's wishes, it would be appropriate to make direct contact with the resident to confirm the position.

- Sensitive personal information is treated differently; for example, where consent is being relied on this should be explicit in nature. However, in the context of a complaint, councillors – and organisations making disclosures to them - will usually be able to rely on the Data Protection (Processing of Sensitive Personal Data)(Elected Representatives) Order 2002 as a condition for processing.