DATA PROTECTION ADVICE FOR MEMBERS

What is Personal Data?

Under the Data Protection Act 1998, Personal Data is defined as data that relates to a living individual who can be identified:

(a) from those data, or
(b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual, and any indication of the intentions of the data controller or any other person in respect of the individual (Section 1(1)).

Personal data will therefore cover basic details such as name, address, telephone number, and Date of Birth, as well as opinions, facts and figures with regard to a particular individual. Processing personal data encompasses the following:

Any activity (obtaining, recording, holding, organisation, adaptation, alteration, retrieval, consultation, use, disclosure, alignment, combination, blocking, erasure and destruction.) that involves Personal Data, which is undertaken either directly, by a Data Controller, or on their behalf by a Data Processor.

Processing personal data must be purposeful, should not be excessive and not misleading as to the reasons for collecting and/or disclosing information. It should be held securely and accessed only on a 'needs to know' basis. Personal data should not be kept for longer than is necessary and should not be shared for reasons outside of the original purpose for which it was collected.

Key Definitions and Processes

Data Subject: - the individual who is the subject of the personal data held by a Councillor. Or who is mentioned within any correspondence held by a Councillor.

The Act only applies to living individuals who have a Right of Access. This is defined as the right to be informed if their personal data is being processed by a Data Controller or by someone on his behalf. This is followed by the right to have the information communicated to him/her in intelligible form (normally hard copy) detailing the information being processed, where or how it was obtained, why it is being processed and to whom it is has or will be disclosed.

Councillors have an obligation to respond to requests for information, formally described as a **Data Subject Access Request**. This must be made in writing. Councillors must satisfy themselves as to the identity of the applicant, as unauthorised disclosures to third parties not entitled to receive the information breaches the Act. All such requests should be acknowledged immediately, and in any event a response must be made within 40 calendar days of receipt of the request. It is a criminal offence to destroy information requested under the right of Subject Access once it has been received by the Data Controller or his/her Data Processor.

Data Subjects have other rights conferred on them by the Act. These are:

- The right to prevent processing likely to cause distress and/or damage
- The right to Prevention of Direct Marketing
- Prevention of Processing for Automated Decisions

Where Councillors receive a request pertaining to any of the rights conferred to data subjects under the Act due care must be given to statutory obligations and council best practice in this area.

Data Controller: - the person who determines the purposes for which and the manner in which personal data will be processed.

Councillors fall under this definition where they are processing other people's personal data for the purpose of their constituency, party political or other non-personal civic activities. All Councillors must comply with the 8 Data Protection Principles and must provide the Right of Access to personal data. All Councillors are **required to register individually with the Data Protection Registrar**. Officers will undertake this on behalf of Members, but only on completion of the necessary form. The Council will pay the registration fee of £35. All Councillors are responsible for the security of the personal data they hold.

Examples of personal data falling under the control of Councillors include:

- Details of complaints
- Case work on behalf of a constituent
- List of contacts
- Personal data held for general constituency work.
- Canvassing on behalf of your party

Data Processor: - the person or organisation who processed the information on behalf of the data controller.

Councillors **do not** have an automatic right of access to any of the personal data processed by the Authority, and must adhere to internal data protection and security procedures with regards to the obtaining and use of such data. Personal data will only

disclosed to Councillors where they can demonstrate that it is necessary in relation to their specific Council duties or work with their constituents. Councillors are not entitled to obtain from the Authority personal data relating to non-constituents. Information obtained from the Authority should be treated in confidence, and only disclosed in line with the Council's wishes. Councillors must seek authorisation to disclose personal data obtained in such circumstances to other organisations.

Examples of personal data processed on behalf of the Authority include:

- Constituency Work
- Case Work
- Committee Work

All requests for personal data held by the Council should be made in writing to the department concerned, stipulating in what capacity and for what purpose the information is required.

Summary of Obligations
Process personal data including its storage and disposal in line with the 8 Data Protection Principles (see below)

Register with the Data Protection Registrar

Provide and ensure the right of Data Subject Access to personal data held in your capacity as a Councillor, Cabinet Member, Party Member or Activist or other non-personal civic duties

Provide and ensure the other rights conferred on individuals under the Act

Obtain personal data in line with the constraints sent out in this code of governance

Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 .Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

If you have any queries regarding Data Protection, please contact the Corporate Data Protection Team at dataprotection@westminster.gov.uk