PART 5 (SECTION H)

Members' Protocol on Data Protection

1.0 Introduction

This document provides the framework for Members on those parts of the Data Protection Act (DPA) which directly affect them in the course of their duties and must be followed at all times.

2.0 The Data Protection Act

2.1 The Data Protection Act 1998 came into force on 1st March 2000. The Act regulates the ways that organisations (data controllers) collect, store and process personal data.

These regulations apply to all automated systems including computers, CCTV, tape recording, e-mail, photographs and, from 24th October 2001, many paper-based and other manual filing systems.

The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 amended the existing provision to facilitate the processing of "sensitive personal data" by Elected Representatives in some circumstances.

2.2 The Data Protection Act 2018 incorporates the provisions of the Europe wide General Data Protection Rules (GDPR), Law Enforcement Directive and local derogations to the GDPR.

The GDPR further strengthens the rights of individuals (data subjects) to access their personal data records and have any mistakes corrected.

2.3 This protocol will refer to the definitions due to be enacted in the Data Protection Act 2018, which will comply with the GDPR.

2.4 "Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as;

- a name
- an identification number
- location information
- an online identifier
- or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2.5 “Special Category” or previously “Sensitive Personal Data” is personal data revealing;

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- information concerning health
- information concerning a natural person’s sex life or sexual orientation.

2.6 The DPA imposes a number of controls in relation to personal data. The main controls are:

(a) Personal data **may not** be “processed” except in accordance with the provisions of the DPA.

“Processing” being a very wide term which includes almost anything that can be done with data.

In addition to activities such as organising, adapting and altering the data, “processing” includes such basic activities as obtaining, deleting, holding or even merely reading the data.

Stricter conditions for processing apply in the case of “special category” personal data.

(b) Processing of personal data may only be carried out by registered Data Controllers.

The Council has registered its activities with the Information Commissioner’s Office (ICO) and can therefore process personal data as a Data Controller.

Members must be registered with the ICO for the purposes of their constituent activities.

(c) Data must be handled in accordance with the Data Protection principles which are set out in the Act. Specifically the Lawfulness of Processing should be tested and documented.

i) Subject has given consent to the processing;
ii) Processing is necessary for the performance of a contract;
iii) Processing is necessary to comply with a legal obligation;
iv) Processing is necessary to protect the vital interests (life or death) of the subject or other person;
v) Processing is necessary for the performance of a task in the public interest or with official Authority;
vi) Processing is for legitimate interests of the Controller.

(d) The DPA sets out a number of Rights of Individuals who are the subject of any personal data ("Data subjects"). For example, a right of access to the information held about them by a data controller ("Subject access").

(e) One of the most important aspects of the DPA is that it imposes strict controls in relation to the disclosure of personal data to third parties.

3.0 Implications for Elected Members

3.1 Although elected members will not be "data controllers" in respect of data held for the purposes of Council business, personal information which is protected by the provisions of the DPA may come into their possession in the course of their duties as councillors. The following guidance is offered in this regard:

3.1.1 Am I entitled to see personal data held by the Council?

Council officers **may** release the information to you, as "elected members" are specified in the Council's registration details (see paragraph 2.3(b) above) as a class of persons to whom personal information will be disclosed.

Before releasing any information to you, however, the officer dealing with your request will ask you the purpose for which the information is required and assure themselves that the use of the information is legitimate in terms of assisting you with your committee, portfolio or constituency role as a Councillor.

If the information is not essential to enable you to carry out your duties and the person who is the data subject has not given their consent for the information to be disclosed to you, you will not be allowed access to the information in question.

There are some situations where obtaining a person's information without consent may be possible. This would be tested on a case by case basis.

3.1.2 If I am given access to personal data, can I disclose it to any other person?

You may disclose the information to the individual to whom it relates to. However, this is provided that it does not contain personal data from which any third party can be identified directly or indirectly, if that third party has not consented to the disclosure.

It is important to remember that personal data relating to an individual must not be disclosed by you to any other person without the consent of the individual concerned. This would be considered an unlawful disclosure.

Members must not forward council emails containing personal data to other email accounts, including both personal email accounts or third party email accounts without understanding who has access to those email accounts, for what purpose the email is being sent and whether consent is required.

3.1.3 When in the Council Offices

The Council has recently updated the office environment of the Council offices and now, many more staff are located on large open plan offices.

Members may from time to time have cause to speak to officers who are at their desks. Members may inadvertently have access to several strands of information including but not limited to;

- Information on computer screens
- Information from officers discussing an on-going live case
- Information relating to a person that may be personal or special category information

Members must avoid looking at Officers' computer screens and must not use or repeat information they have inadvertently heard during the course of their legitimate visit to the offices.

3.1.4 What are the consequences of unlawful disclosure?

If you do disclose such information to a third party without consent, there are three possible consequences:

(a) You may have compromised an individual's privacy, causing damage or distress. This may result in a personal claim against you or the council. In some cases this has previously resulted in loss of life for a data subject as a result of an information breach;

(b) You may have committed an offence under the Data Protection Act for which you may be prosecuted in either the Magistrates' Court or the Crown Court. Upon conviction in the Magistrates' Court, you would be liable to a fine of up to £5,000. In the Crown Court, the maximum penalty is an unlimited fine;

(c) You would be in breach of the Code of Conduct for Members of the Council, which states that a member "must not disclose information given to him in confidence by anyone, or information acquired which he believes is of a confidential nature, without the consent of a person authorised to give it, or unless he is required by law to do so". Any member acting in breach of the

Code of Conduct may be the subject of a report to a panel of the Audit and Governance Committee.

4.0 Members as Data Controllers

4.1 As previously mentioned, elected members will not be "data controllers" in respect of data held for the purposes of **Council business**. It will invariably be Council officers who control the processing of data held for such purposes.

Any proposed use of the data by members, other than that detailed when requesting information, must be cleared with the relevant Council officer.

Members can of course access personal data with the consent of the data subject e.g. when acting on behalf of a citizen in their ward.

4.2 It may, however, be the case that members maintain their own computerised records containing personal data (e.g. address lists) for their own use. If the data is held for personal, family or household purposes, there is no requirement for a member to register themselves as a data controller with the Information Commissioner's Office (ICO).

4.3 However, if the data is held or used for the purpose of constituency casework or for canvassing political support amongst the electorate, formal notification must be made to the Office of the Information Commissioner under the provisions of the Data Protection Act.

4.4 When you are campaigning for election or otherwise acting on behalf of a political party you should be covered by the notification of the Party to whom you belong, but check with your constituency Chairperson or Secretary.

Any Member who considers that they may be affected in this way should seek further advice from:-

Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545745
e-mail: data@dataprotection.gov.uk

5.0 Enquiries from Constituents

5.1 It is, of course, the case that individuals may make their own request under the Data Protection Act for disclosure of personal information held on them by the Council. If you are approached by a constituent who merely wants sight of such information, you should advise them to make a request for this in writing, to:-

The Data Protection Officer
Boston Borough Council
Municipal Buildings
West Street
Boston
PE21 8QR

6.0 Responsibilities to Report

6.1 A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

6.2 It is every elected member's responsibility to take privacy of personal information seriously. The potential for an unlawful disclosure, and personal data breach must be reported as soon as possible to the **Councils Data Protection Officer** to comply with the statutory obligation to inform the ICO within 72 hours.

6.3 A "personal data breach" is when information may have processed by persons not expressly permitted to have access to that information.

6.4 Examples include:

a) A misdirected email;
b) A letter sent to the wrong address;
c) Loss of a PC/tablet/mobile phone containing personal data;
d) Notes of meetings lost;
e) Overheard conversations regarding subjects.

6.5 Failure to notify the ICO within 72 hours would seriously affect the Council's position should the ICO make a determination against the Council.

7. Members Obligations to Understand the Requirements of this Protocol

7.1 The Council will provide opportunities for training and Member development through the Councillor Development Group.

7.2 If a Member does not understand the meaning of the requirements of this Protocol, it is their personal responsibility to raise directly with the Monitoring Officer, their Group Leader or Chairman of the Councillor Development Group to ensure the appropriate training is identified and offered.

Relevant Legislation affecting this Protocol

Legislation:
The Data Protection Bill 2018
The General Data Protection Regulations (EU) 2016/679
The 'Law Enforcement Directive" - EU Data Protection Directive 2016/680
Department for Digital, Culture, Media and Sport - Data Protection Bill (2018)
The Data Protection Act 1998
Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002

The Council's Monitoring Officer may update this protocol from time to time following developments in guidance from the Information Commissioner's Office, case law and any changes to legislation.

Protocol prepared on the 15/3/2018.