Elected Members' Guide to the Data Protection Act (DPA)

- The Data Protection Act 1998 (DPA) is designed to protect personal information about living individuals (personal data) from misuse.
- The DPA applies to all uses of personal data, such as storing, reading, sharing, deleting and so on; the use of personal data is called "processing".
- The DPA provides individuals with a right of access to their personal data and places certain obligations for using personal data.

What is personal data?

Personal data is any information that identifies a living individual, for example, name, address, date of birth and national insurance number. Statistical information can also be personal data if the datasets are small enough, for example statistics based on postcodes can identify individuals as sometimes a postcode only relates to one house.

What is sensitive data?

You have to be extra careful with information that is classed as sensitive as the rules for its use are more stringent. Sensitive personal data is information about an individual's:

- race or ethnic origin
- political opinion
- religious beliefs
- trade union membership
- physical or mental health
- sexual life
- criminal proceedings or convictions

What are the 8 principles of Data Protection?

The Act contains a legally binding code for the correct handling of personal data, called the "Data Protection Principles", which must be adhered to. These principles are designed to prevent individuals being misled as to the purpose for which their personal details are to be used and place limits on how widely these details can be processed and how long they can be kept. Personal data shall be:

1. Processed fairly and lawfully (To make the processing fair the individual(s) must be informed that their data is being collected, who holds their information, who the data controller is, what the data will be used for, an indication of how long the data will be kept and information on any disclosure to any third parties. To make the processing lawful there are conditions within the DPA that have to be met, but also use of the data must not breach any other legislation)
2. Processed only for specified and related purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept longer than necessary
6. Processed in accordance with individuals rights
7. Kept secure
8. Not transferred to countries without adequate data protection regimes

People's rights to access their information

The DPA provides individuals with the right to access their personal information. They must submit their request in writing, pay a fee, provide sufficient information for you to locate what they require and you must be satisfied of their identity. You have to respond to a request for access to personal information within **40 calendar days** and provide all the information they are entitled to in permanent form. There are a number of reasons why information shouldn't be provided, known as exemptions. The Information Management Service can assist you if you receive such a request.

Notification

If you use any constituents' personal information electronically (even to schedule surgeries etc), you are required to hold an up to date notification with the Information Commissioners Office. You do not need to register solely in your capacity as a member of a council committee, or in a party office. These would be covered by the council's or party's registration.

Notification involves providing the Commissioner with details of the types of processing of personal data undertaken. These details are then published by the Commissioner in the form of a public register, accessible by the public. **Notification is a legal requirement**

Failure to notify when required is a criminal offence; punishable with a fine of up to £5000 in the Magistrates Court.

How to Notify

The Information Commissioner has produced a standard form for elected members to adopt to help complete the Notification process; a copy of this Notification form forms part of your induction pack. The Council's **Information Management Service** can assist elected members in completing it and will pay the £35 charge.

Consequences of breaching the DPA

If you don't comply with data protection the consequences can be severe:

- **An individual** can be caused harm or distress
- **You** can suffer criminal prosecution, litigation, damaging publicity and financial loss
- The Information Commissioner's Office can hand out penalties of up to £500,000 for serious breaches of the Data Protection Act 1998. The maximum fines will be used in cases where the incident has caused individuals "substantial damage and distress", whether it was deliberate or negligent.

The Data Protection Act – a cautionary tale

The following is a good example of an elected member falling foul of data protection legislation and why councillors need to be aware of the provisions of the DPA.

In the run up to the 1999 local election, a candidate in Bromsgrove obtained a list of the names and addresses of free bus pass holders from a Council officer. He then used the information to target them with pamphlets warning them of cuts to the free bus pass scheme that he claimed would be made by a rival party if they obtained power. Unfortunately for this elected member, there were two complaints made by members of the public. When the matter went to court, the Councillor concerned pleaded guilty to two breaches of the Data Protection Act relating to unlawfully obtaining personal data and processing without a valid notification. The Councillor was fined £500. The agent for the Information Commissioner prosecuting said it was a deliberate invasion of privacy, with the Councillor using his privileged position to obtain personal data.

As the example in Bromsgrove highlights, members should not automatically assume they have 'carte blanche' access to personal information and might be asked to show that they are acting on behalf of the individual that they are requesting information about.