BISHOP'S CASTLE TOWN COUNCIL
Data Protection Policy

The Data Protection Principles

Even if you are exempt from notification, you are **still** required to comply with the eight data protection principles. The principles are set out below.

1. **Data must be obtained fairly and lawfully**
Information should be 'fairly processed' i.e. when you collect the information from individuals you should be honest and open about why you want it.

2. **Data must be held only for specific and lawful purposes and not processed in any matter incompatible with those purposes**
You must have a legitimate reason for processing the data. You should explain (in most cases in writing): who you (the data controller) are - giving the name of your Council; what you intend to use the information for and to whom you intend to give the personal data. This may be a specific third party, or a may be a more general description such as "other Councils' etc

3. **Data must be relevant, adequate and not excessive for those purposes**
Data users should monitor the quantities of data held and ensure that they hold neither too much nor too little. Hold only the data which you actually need.

4. **Data must be accurate and where necessary kept up to date.**
Personal data should be accurate. If it is not, it must be corrected.

5. **Data must not kept for longer than necessary**
Only in exceptional circumstances should data be kept indefinitely. In order to comply with the principle you should have a system for the removal of different categories of data from your system after certain periods, for instance, when the information is no longer required for audit purposes

6. **Data should be processed in accordance with the rights of data subjects under this Act**

This means that individuals must be informed, upon request, of all the information held about them. They can prevent the processing of data for direct marketing purposes and are entitled to compensation if they have been caused damage by any contravention of the Act.

7. **Security precautions in place to prevent the loss, destruction or unauthorised disclosure of the data**
Data controllers should ensure that they provide adequate security for the data taking into account the nature of the data, and the harm to the data subject which could arise from disclosure or loss of the data. A system of passwords should be in use to ensure that only staff who are authorised can gain access to personal data. Passwords should be changed

fairly frequently. Councils should have established, written procedures setting out who is authorised to access which records and for what purpose.

8. **Not to transfer data outside the European Economic Area unless you are satisfied that the country in question can provide an adequate level of security for that data**

Sensitive Data

The Act defines eight categories of sensitive personal data. These are:

a) the racial or ethnic origin of data subjects;
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether they are a member of a trade union,
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by them of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

If you hold personal data falling into these categories it is likely that you will need the explicit consent of the individual concerned. You will also need to ensure that your security is adequate for the protection of sensitive data.

Manual Data

The Data Protection Act 1998 also covers some records held in paper form. Such records need not be notified to the Commissioner, but should be handled in accordance with the data protection principles. Manual records are covered by the Act if they form part of a relevant filing system. It is for data controllers to assess their manual records.

It is important to note that individuals may seek **compensation** through the courts if they have suffered damage because of **any** contravention of the Act.

Dealing with subject access requests

If you receive a written subject access request, you must deal with it promptly, and in any case within 40 days from the date of receipt. If you need further information, the 40 days will begin when you receive this further information. You are entitled, if you wish, to ask for a fee of not more than £10 and the 40 days does not begin until this is received.

In response to a subject access request individuals are entitled to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone it may be disclosed to, and any information available to you about the source of the data.