Data Protection Policy

1. Introduction

1.1 An essential activity of Warminster Town Council is the requirement to gather, process and store information about its employees, people in the community, suppliers, business contacts and other sources in order to operate efficiently.

2. Data Protection Act

2.1 The Data Protection Act 1998 was put into place to help protect people's personal data. It aims to ensure that people know where their data is held, what it is used for and who it is shared with. It also ensures that an organisation treats people's data correctly and has systems and controls in place for effective management of that data.

2.2 A Council acting as an employer is required to comply with the Data Protection Act. In such circumstances, the Council will be deemed to be a data controller for the purposes of the Act and in this capacity it will determine the purposes for which and the manner in which any personal data is, or is to be, processed. "Processing" includes obtaining, recording, holding or using information.

2.3 The Data Protection Act is underpinned by eight important principles which state that personal data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate
5. not to be kept longer than is necessary
6. processed in line with the data subject's (individual) rights
7. secure
8. not transferred to countries outside of the EU without adequate protection

3. Subject Rights

3.1 The Act creates rights for those people who have their data stored and also responsibilities for those who store, process or collect personal data.

3.2 A person who has their data processed by the Council has a number of rights in relation to the data which is held about them. The person can do the following:

- View the data which is held for a maximum fee of £10;
- Request that information which is incorrect be corrected;
- Require that data is not used in a way which may cause damage or distress;
- Require that their data is not used for direct marketing.

4. Subject Access Requests

4.1 Under section 7 of the Data Protection Act, a person may make a subject access request in relation to information held about them. A person who makes a request and pays a maximum £10 fee is entitled to the following information:

- To be told whether any personal data is being processed;
- A description of the personal data which is held, why the data is being processed and whether this data will be given to any other organisations or people;
- A copy of the information comprising the data; and
- The source of the data.

4.2 Once the Council receives such a request, should the data be disclosable, the request must be dealt with within 40 calendar days of receiving the request.

4.3 If the personal data which is the subject of the request is normally held for less than 40 days, then the request may be legitimately refused.

5. A Subject Access Request Which Concerns Other People's Information

5.1 A person may request access to data about them which also carries information regarding a third party. In such circumstances, the Council will assess whether the request can be complied with, without infringing the third party's privacy.

5.2 If the Council receives a request from an employee to access some personal data and complying with the request would mean disclosing information relating to another individual who can be identified from that information, then the request will be legitimately declined unless the third party consents to the disclosure or it is reasonable for the Council to comply with the request without the third party's consent.

5.3 There is an obligation upon a data controller to comply with as much of a request as possible. If the consent of the third party cannot be obtained and compliance with the request is reasonable, then the Council will consider separating the disclosable information from the non-disclosable information.

6. What is 'Personal Data'?

6.1 The Data Protection Act covers any data which concerns a living and identifiable individual.

6.2 Personal data could be a name accompanied by other information about the individual such as address, age or telephone number.

6.3 The Act does not cover information which is anonymous or aggregated data provided that the anonymisation or aggregation is not reversible.

7. Exceptions

7.1 There are circumstances in which a data controller is not obliged to supply certain information to the requester. Some of the most important exemptions apply to:

- Crime prevention and detection;
- Confidential references given by you (but not ones given to you); and
- Information covered by legal professional privilege.

8. Registration as a Data Controller

8.1 For the purposes of the Data Protection Act, the Council is registered with the Information Commissioner's Office (ICO) as a data controller. This registration is renewed annually.

8.2 As an employer, the Council has obligations in relation to the data it holds on computer or in structured filing systems about its employees. The main requirements of the Data Protection Act can be complied with in relation to this data if the Council:

- has individuals' consent to holding the information about them;
- uses the information only for the purposes for which they obtained it;
- keeps the information up-to-date, secure and only for so long as it is needed;
- does not disclose the information to others without the individual employee's consent.

9. Disclosure Information

9.1 The Council will as necessary undertake checks on both staff and members with the Disclosure and Barring Service and will comply with its Code of Conduct relating to the secure storage, handling, use, retention and disposal of disclosures and disclosure information. It will include an appropriate operating procedure.