Thame Town Council

Corporate Data Protection Policy

1. Aims

1.1 This policy sets out the Council's commitment to the lawful and fair handling of personal data in accordance with the Data Protection Act 1998. For detailed guidance on Data Protection and procedures, please refer to the Data Protection Manual.

2. Background

2.1 The Data Protection Act 1998 ("the Act") regulates the holding and processing of personal data - that is information relating to living individuals, which is held either on the computer or in some cases in manual form. The Act also gives rights to individuals whose personal information is held by organisations.

2.2 The Council needs to collect and use personal information in order to carry out its functions effectively. Information can be held concerning its current, past and prospective employees, suppliers, service users, residents and others with whom the Council communicates.

2.3 The Council and in some circumstances its individual employees could face prosecution for failure to handle personal data in accordance with the Act.

3. Policy Statement

3.1 Any personal data which the Council collects, records or uses in any way whether it is held on paper, computer or other media will be subject to appropriate safeguards to ensure that the Council complies with the Act.

3.2 The Council fully endorses and adheres to the eight Data Protection Principles which are set out in the Act and summarised below:

Personal data shall be:

- fairly and lawfully processed
- processed for specified and lawful purposes and not in any other way which would be incompatible with those purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not kept for longer than is necessary
- processed in line with the data subject's rights
- appropriate measures taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of personal data
- kept secure not transferred to a country, which does not have adequate data protection laws.

4. Action

4.1 In order to meet the requirements of the data protection principles and its obligations under the Act, the Council will ensure the following:

4.1.1 Renew its entry of the Register of Notifications held by the Information Commissioner's Office.

4.1.2 Appoint officers with specific responsibility for data protection in the Council.

4.1.3 Any forms used to collect data will contain a 'fair processing notice' to inform the data subject of the reasons for collecting the personal information and the intended uses.

4.1.4 Any personal information that has been collected will be used only for the purposes for which it was collected.

4.1.5 Data subjects (individuals to whom the personal information relates) are able to exercise their rights under the Act, including:

- the right to be informed that their personal information is being processed
- the right of access to their personal information
- the right to correct, rectify, block or erase information that is regarded as wrong

4.1.6 Personal data will only be disclosed to third parties when it is fair and lawful to do so in accordance with the Act and with any Information Sharing Protocols.

4.1.7 Sensitive personal data will only be processed with the explicit consent of the data subject or if an exemption applies under the Act. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

4.1.8 Procedures are in place to check the accuracy of personal data collected, retained and disclosed.

4.1.9 Review the time that personal information is retained or stored to ensure that it is erased at the appropriate time.

4.1.10 When a Subject Access Request (SAR) is received, the Council has 40 calendar days in which to respond and a maximum fee of up to £10 can be charged for the information requested. Payment needs to be made in full before the information will be provided and the 40 calendar days becomes effective from this date. There are exceptions when the request for information may be refused as detailed within the new ICO guidance notes.

4.1.11 All officers who hold or process personal information will receive appropriate training in order to comply with the Act.

4.1.12 Audit compliance with this policy and the Act and any incidents involving breaches of this policy and the Act are recorded, analysed and disciplinary action taken as appropriate.

4.1.13 This policy is reviewed regularly and updated when necessary.

5. Further Information

5.1 The Information Commissioner's Office (ICO) is the independent authority set up to monitor compliance with the Act. It also issues guidance and good practice notes. The ICO's website address is www.ico.gov.uk.

5.2 The ICO can only consider complaints about an organisation's failure to comply with the Act when the organisation's complaints route has been exhausted. Complainants should therefore be referred first to the Town Council's Complaints Procedure.