St Albans City & District Council
Data Protection Policy

1. Introduction

1.1 St Albans City & District Council (the Council) needs to collect and use certain information about people. This is "personal data" within the meaning of the DPA. These people include current, past and prospective Councillors, employees, consultants, agents, partners, suppliers, customers and others with whom it communicates. The Council regards the lawful and correct treatment of personal information as essential to the successful operation of its services and maintaining the confidence of its customers including those with whom it carries out business.

1.2 In addition there may be a legal requirement to collect and use certain types of information to comply with the requirements of Central Government Departments for business data or primary legislation.

1.3 The Council will ensure that personal information is dealt with properly and lawfully in support of the legislative requirements of the Data Protection Act 1998 (DPA), regardless of how it is collected, recorded and used, whether in paper form, electronically in a computer, or recorded on other material.

2. Scope

2.1 The policy should be read in conjunction with the Data Protection procedures developed by the Council, which detail the responsibilities of Officers and the requirements and reporting procedures under the legislation.

2.2 In accordance with the requirements of the DPA, the Council has registered with the Information Commissioner's Office (ICO) for activities which involve processing personal data. Any amendments are advised to the ICO as soon as they become apparent and registration is renewed annually.

2.3 The Council will adhere to the eight Data Protection Principles as required by the DPA which require specifically that personal information/data shall:

- Be processed fairly and lawfully and in particular shall not be processed unless specific conditions are met;
- Be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Be accurate and, where necessary, kept up to date;
- Not be kept longer than is necessary for that purpose or those purposes;
- Be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
- Have appropriate technical and organisational measures in place to safeguard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data;
- Not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3 Key Commitments

3.1 The Council will through appropriate management and strict application of criteria and controls:

- Seek to acknowledge all DPA requests within **3 working days**;
- Confirm the **identification** of the individual making the request with suitable photographic identification documentation;
- Respond promptly and fully within the **40 calendar days** specified by the DPA (which commence once all the necessary information to deal with the request together with the required fee have been received);
- Inform the requester that a **statutory fee** of £10 is payable and the request will not be commenced until it is paid;
- Observe the DPA requirements regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is to be used when it is collected;
- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality and accuracy of information used;
- Apply checks to determine the length of time information is retained;
- Ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 1998. This includes the right to be informed that processing is being undertaken; the right to access your personal information; and to prevent processing in certain circumstances or correct, rectify, block or erase information which is regarded as incorrect or inaccurate;
- Take appropriate technical and organisational security measures to safeguard personal information including data transferred by email
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that personal information is promptly and securely disposed of when no longer required.

3.2 In addition the Council will ensure that:

- There is a senior officer with specific responsibility for Data Protection in the organisation;
- Everyone managing and handling personal information understands that they are responsible for following good Data Protection practice;
- Everyone managing and handling personal information is appropriately trained and supervised to do so;
- Queries about handling personal information or requests to have access to or have copies of someone’s own personal data are dealt with promptly and courteously in accordance with S7 Subject Access Request (DPA) by the relevant IMG member (Information Management Group);
- A regular review and audit is made of the way personal information is managed, including CCTV systems;
- Methods of handling personal information are regularly assessed and evaluated;
- Regular assessments of the Councils’ compliance with the Data Protection Act 1998 take place.

4. Review

4.1 This policy and the associated procedures will be subject to annual review.

Author	
Policy created & reviewed	September 2011 Reviewed February 2012, December 2013, August 2015, March 2017
Policy created by	Regulatory Solicitor & Complaints and Information Assurance Officer
Policy review due	March 2018