St Albans City & District Council
Data Protection Policy:
UK General Data Protection Regulation & Data Protection Act 2018

1. Introduction

1.1 St Albans City & District Council are known as **the Data Controller** because we process **personal data**. The **Data Controller** is the person responsible for ensuring that all personal data is processed lawfully in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) (implementing the Law Enforcement Directive). **Personal data** is any information that identifies or relates to the individual.

1.2 In order to carry out functions we are required to provide, and other services we choose to provide, we must collect and use personal data about individuals. We collect personal data from a variety of individuals including current, past and prospective councillors, employees, consultants, agents, partners, suppliers, customers and others with whom we communicate. We regard the lawful and correct handling of personal data as essential to operate the Council successfully in the way we provide services. We consider it is important that we maintain the confidence of our customers that we will keep their personal data secure.

1.3 We will ensure that personal information is dealt with properly and lawfully in compliance with the legislative requirements of the UK GDPR and the DPA, regardless of whether it is collected, recorded, and used in paper or electronic format.

2. Scope

2.1 Staff will use this policy in conjunction with the Data Protection procedures developed by the Council, which detail the responsibilities, requirements and reporting procedures under the legislation.

2.2 In accordance with the requirements of the UK GDPR & the DPA, we are registered with the Information Commissioner's Office (ICO) for activities which involve processing personal data. Our registration can be found on the ICO's register of Data Controllers [Z5700229]. 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 Data Protection Principles as required by the UK GDPR & DPA which specifically require that personal information/data is handled as set out in the six data protection principles [Art 5(1)] and accountability requirement:

1. Personal information shall be processed lawfully, fairly and in a transparent manner [Lawfulness, Fairness and Transparency Principle]

2. Personal information must be collected for specified, explicit and legitimate purposes [Purpose Limitation Principle]

3. Personal information shall be adequate, relevant and limited to what is necessary [Data Minimisation Principle]

4. Personal information must be accurate and, where necessary, kept up to date [Accuracy Principle]

5. Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [Storage Limitation Principle]

6. Personal information must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures [Integrity & Confidentiality Principle]

7. We are responsible for compliance with the principles and we must be able to demonstrate compliance with the principles. [Accountability Principle] [Art 5(2)]

2.4 Failure to comply with UK GDPR's data protection principles could result in a breach of the Regulation and result in a financial penalty of up to €20,000,000 (approximately £17,000,000). Failure to comply with the Data Protection Policy and Procedure or other information management policies and procedures could result in disciplinary action for staff.

3 Key Commitments

3.1 We will do the following to ensure compliance with the UK GDPR and DPA :

- Comply with our **Data Protection Procedure; other policies & procedures**
- Provide personal data when requested under a **Subject Access Request** in accordance with the Data Protection Procedure within a calendar month
- Consider and respond to all **Individuals' Rights** requests within a calendar month in accordance with our Individuals' Rights guide. 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
- Comply with the **Data Protection Principles** in all processing
- Provide **privacy notices** whenever we collect personal data or change the way we are using your personal data
- Take appropriate technical and organisational **security measures** to safeguard personal data.

3.2 In addition, we will ensure that:

- The Data Protection Officer oversees compliance in accordance with Articles 34-37 of the UK GDPR
- Everyone managing and handling personal information receives training, so that they understand their responsibilities with regard to good data protection practice
- Requests for subject access to personal data are handled by the relevant departmental IMG (Information Management Group) member or the FOI Team
- We regularly review and audit the way personal information is managed, to make sure we comply with the UK GDPR & DPA, including updating policies and procedures; maintaining up to date Information Logs & Disposal Schedules and revising privacy notices.

4. Review

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

Author	
Policy created	March 2018
Policy reviewed	May 2018, April 2019, April 2020, November 2020, June 2021, February 2022, May 2023
Policy created by	Solicitor- Regulatory Team Leader & Complaints and Information Assurance Officer
Policy review due	May 2024