# Data Protection Policy

Prepared by Vikki Smith
Issue Date: 04/03/2019 20/04/2018
Status: Approved Version 1.3

DAVENTRY DISTRICT COUNCIL

## 1. Introduction

### 1.1 Purpose

The purpose of this document is to set out how the Council will manage the lawful and fair handling of personal data in accordance with the Data Protection Act and the General Data Protection Regulations.

For detailed guidance on Data Protection and procedures, please refer to the Data Protection Manual.

### 1.2 Background

The General Data Protection Regulations (the "Regulation") regulates the holding and processing of personal data - that is information relating to identified or identifiable natural person, 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.

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.

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

### 1.4 Change History

| Version | Revision Date | Reviser | Previous Version | Description of Revision |
|---|---|---|---|---|
| 1.0 | 29/06/2001 | Mary Gallagher | | Original |
| 1.1 | 25/05/2011 | Vikki Smith | 1.0 | Update format and content |
| 1.2 | 02/02/2015 | Vikki Smith | 1.1 | Amend security and include privacy by design |
| 1.3 | 13.03.2018 | Vikki Smith | 1.2 | Updated to reflect GDPR |

## 2. Policy

This policy defines the actions the Council will undertake to ensure that any personal data which the Council collects, records or uses in any way (whether it is held on paper, computer or other media) is subject to appropriate safeguards to ensure compliance with the data protection legislation. It will be reviewed every three years, or sooner, if there is a significant change.

## 2.1 Data Protection Principles

The Council fully endorses and adheres to the six Data Protection Principles which are set out in the Regulation and summarised below:-
Personal data must be:

a) processed lawfully, fairly and in a transparent manner
b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary
d) accurate and where necessary kept up to date
e) 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
f) processed in a manner that ensures appropriate security

In addition there is Accountability. The Council is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the ICO.

## 2.2 What the Council will do

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

1. Annually renew its entry of the Register of Notifications held by the Information Commissioner's Office (ICO). Its registration number for such purposes is Z7520115.

2. Maintain an Information AssetRegister of particulars about the types of personal data the Council holds, purposes for which it is held and used and types of organisations to which personal data may be disclosed.

3. Appoint a Data Protection Officer with responsibility for gathering and disseminating information and issues relating to information security, data protection and other related legislation.

4. Ensure any forms used to collect data will contain a 'privacy notice' to inform the data subject of the reasons for collecting the personal information and the intended uses

5. Ensure any personal information that has been collected will be used only for the purposes for which it was collected

6. Develop processes that enable data subjects (individuals to whom the personal information relates) are able to exercise their rights, including:-

- Right to access their personal information held by the organisation
- Right to rectification of inaccurate personal data
- Right to erasure – does not apply to data processed for the public task
- Right to restriction of processing
- Right to data portability – only where consent is relied upon or where the data subject has entered into a contract with the Council
- Right to object
- Right to prevent significant decisions being taken about them solely by automatic

processing

7. Only disclose personal data to third parties when it is fair and lawful to do so in accordance with data protection legislation and with any Information Sharing Agreements

8. Ensure all contracts and service level agreements between the Council and external third parties (including contract staff), where personal data is processed, make reference to data protection legislation as appropriate

9. Ensure sensitive/special category personal data will only be processed if the conditions are met or if an exemption applies. Special Category data is personal data revealing racial, or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

10. Ensure procedures are in place to check the accuracy of personal data collected, retained and disclosed

11. Ensure that personal information is retained or stored only for as long as legally required

12. Ensure that personal information is handled securely and in compliance with the Code of Good Practice set out in ISO 17799 which sets out the requirements for an Information Security Management System. The Council has an "Information Security Incident Management Policy" in place. This sets out the requirement to keep all computer systems and data secure and how to report security incidents.

13. Approach all projects with the "privacy by design" concept, to ensure data protection and privacy are built into new systems and processes from the start.

14. Ensure all officers who hold or process personal information will receive appropriate training in order to comply with data protection legislation

15. Audit compliance with this policy and ensure any incidents involving breaches of this policy or data protection legislation are recorded, analysed and appropriate action taken.