Data Protection Policy

1. Introduction

1.1 Crewkerne Town Council (referred to in this document as "the Council") processes a wide range of data relating to its employees, councillors, residents and customers, and other data subjects in order to deliver council services and to discharge its legal and statutory responsibilities.

1.2 The Council is committed to being as transparent as possible about its operations and details of information which is routinely available are contained in the Council's Publication Scheme, which is consistent with the statutory model publication scheme for local councils.

1.3 The Council takes the protection of personal data seriously and is committed to protecting this information in accordance with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The Council acknowledges its responsibility as a Data Controller and will be able to demonstrate compliance with the Data Protection Principles under the accountability principle. Where appropriate, the Council's appointed Data Protection Officer (DPO) or Clerk will oversee compliance and act as the main point of contact for data protection matters.

1.4 When handling such information, the Council, and all staff or others who process personal information on its behalf, must comply with the six Data Protection Principles which are set out in the General Data Protection Regulation (GDPR). These state that personal data shall be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- 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.

2. Data Protection Terminology

2.1 **Data subject**: means the person whose personal data is being processed.

Personal data: information about a living individual which is capable of identifying that individual, e.g. a name and address.

Special category data: includes information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data.

Data controller: the person or organisation who determines the purposes for which and the manner in which any personal data is to be processed. The Council is the data controller.

Data processor: the person or organisation that processes the data on behalf of the data controller.

Data breach: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Processing: anything done with/to personal data (obtaining, recording, adapting or holding/storing).

Consent: is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

3. Processing of Personal Data

3.1 The Council will maintain a Record of Processing Activities (ROPA) to document what personal data it holds, why it is collected, who has access, and how long it is retained. This ensures accountability and transparency in accordance with Article 30 of the GDPR.

3.2 The Council processes personal data in order to:

- Fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- Pursue the business of the Council through its powers and duties as a public body.
- Fulfil its contractual terms with other organisations.
- Assist regulatory and law enforcement agencies.
- Process information including the recording and updating details about its councillors, employees, partners and volunteers.
- Process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint or to provide feedback to the Council.
- Undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- Prevent or detect fraud through the necessary audit tasks carried out for the Council.
- Monitor its activities including the equality and diversity of its activities.

3.3 The GDPR sets out the following six lawful bases for processing personal data:

- The individual has consented to the processing.
- Processing is necessary for the performance of a contract or agreement with the data subject.
- Processing is required under a legal obligation.
- Processing is necessary to protect the vital interests of the individual.
- Processing is necessary to carry out public functions.
- Processing is necessary in order to pursue the legitimate interests of the data controller.

3.4 The Council will ensure that at least one of these conditions is met for personal information to be processed.

3.5 Particular attention is paid to the processing of any sensitive personal information and the Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual.
- Required by law to process the data for employment purposes.
- A requirement in order to protect the vital interests of the individual or another person.

4. How the Council uses Personal Information

4.1 The Council will only use any personal information for the purposes for which it is provided and will only hold the information for as long as necessary. All council employees and councillors who have access to personal data and are associated with the handling of that data are obliged to respect the confidentiality of the data. The Council will endeavour to keep the personal information it has accurate and up to date but will amend or erase that information upon request.

4.2 The Council will maintain a log of instances where personal data is viewed, shared, or disclosed, ensuring a clear audit trail of access and processing.

4.3 Personal data will be retained in accordance with the Council's Records Management Policy, after which it will be securely deleted or destroyed.

5. Information Sharing

5.1 The Council may need to pass personal information to other people and organisations that support the Council in provision of services. These providers are obliged to ensure that they process such data in accordance with the requirements of GDPR.

5.2 The Council uses organisations to assist with storing information. In such cases the Council will gain assurance that these organisations have security arrangements in place which are compliant with GDPR.

5.3 Where personal data is shared with or processed by a third party on behalf of the Council, a written Data Processing Agreement will be in place setting out the obligations of both parties, including confidentiality, security measures, and deletion of data after processing.

6. Information Security

6.1 Crewkerne Town Council will make every effort to ensure that personal information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and procedures including password protection, access control, encryption where appropriate, and staff training on data protection responsibilities. The Council will only keep personal data for the purpose it was collected for and only for as long as is necessary.

7. Data Breaches

7.1 If a member of staff or a councillor believes that a breach of security of personal data has occurred, they must inform the Town Clerk at the earliest possible opportunity. The Clerk will assess the breach and, where required, notify the Information Commissioner's Office (ICO) within 72 hours. The Clerk will also record all breaches, whether or not they are reported to the ICO, and ensure that lessons are learned to reduce the risk of recurrence.

8. Children

8.1 The Council will not process any data relating to a child (under 13) without the express parental/guardian consent of the child concerned.

9. Rights of a Data Subject

9.1 Under the General Data Protection Regulation (GDPR), individuals have a number of rights in relation to their personal data. These rights allow individuals to understand, control and, where appropriate, restrict how their personal information is used by the Council.

- **Access to Information:** an individual has the right to request access to the information the Council has on them. They can do this by contacting the Council.
- **Information Correction:** If they believe that the information the Council has about them is incorrect, they may contact the Council to allow the data to be corrected.
- **Information Deletion:** If the individual wishes the Council to delete the information about them, they can do so by contacting the Council.
- **Right to Object:** If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Council.
- **Right to Restrict Processing**: To request that the Council limits how their data is used.
- **Right to Data Portability**: to request that their data be provided in a structured, commonly used and machine-readable format.

9.2 The Council does not use automated decision making or profiling of personal data.

10. Privacy Notice

10.1 The key aspects of this policy are contained within a Privacy Notice which can be found on the home page of the Council's website. This Notice will be reviewed every four years to ensure it remains accurate and up to date.

11. Subject Access Requests (SARs)

11.1 Individuals wishing to request access to their personal data should submit a written request to the Town Clerk. The Council will respond within one calendar month, in accordance with GDPR requirements. Proof of identity may be required to ensure that data is only disclosed to the correct individual.

Version Control:

Adopted at the Policy & Resources Committee: 14th May 2018 Min. No. 17/18 45
Update at the Policy & Resources Committee: 13th October 2025 Min. No. 016 25/26 g

This policy will be reviewed every four years, or sooner if required by changes in legislation or council practice.

Review Date: October 2029