

CRAWLEY BOROUGH COUNCIL

Data Protection Policy

1. Introduction

- 1.1 This document sets out Crawley Borough Council's Data Protection Policy and how it complies with the Data Protection Act 2018 (the Act) and the General Data Protection Regulation (GDPR).
- 1.2 The Act and the GDPR regulates the way in which personal data about individuals whether held in a computer or in a manual filing system is obtained, stored, used, disclosed and destroyed. This Policy applies to anyone working with personal data that is controlled or processed by or on behalf of Crawley Borough Council, all staff and elected Members of the Council.
- 1.3 We expect all our staff, elected Members and anyone who processes personal data on our behalf to comply with this Policy and the Data Protection Principles.
- 1.4 The GDPR makes a distinction between Personal Data and Special Category Data as set out in the GDPR.
- 1.5 "Personal Data" means any data or information in paper or in digital format, relating to a living individual.
- 1.6 "Special Category Data" is defined as personal data consisting of information as to:
 - Racial or ethnic origin
 - Political opinion
 - Religious/philosophical beliefs
 - Trade Union membership
 - Physical or mental Health or condition
 - Sexual life or sexual orientation
 - Biometric data

2. Policy Statement

- 2.1 The Council needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include members of the public, current, past and prospective employees, elected Members, customers and suppliers in addition the Council may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly however it is collected, recorded and used.
- 2.2 Crawley Borough Council regards the lawful and appropriate treatment of personal information as very important to the success and effectiveness of its operations and essential to maintaining the confidence between the Council and those whom it carries out business. It is essential that it respects the rights of all persons whose personal information it holds and treats personal information lawfully in accordance with the Act and the GDPR and that it is able to show that this is the case.

2.3 Crawley Borough Council will comply with the Act and the GDPR principles and ensure that Personal Data is:

- Processed fairly and lawfully and in a transparent manner
- Obtained for one or more specified, explicit and lawful purposes
- Use personal data in the most efficient and effective way to deliver better service
- Adequate, relevant and only limited to what is required
- Accurate and where necessary kept up to date
- Not kept in a form which permits identification of data subjects for longer than is necessary
- Processed in accordance with the rights of data subjects
- Processed in a manner that ensures appropriate security of the personal data
- Kept secure to safeguard information (including unauthorised or unlawful processing or accidental loss).

3. The Data Protection Principles

3.1 Crawley Borough Council will abide by the six data protection principles as set out below:

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) not be considered incompatible with the initial purposes ('purposed limitation')
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
6. 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 and confidentiality')

4. Roles and Responsibilities

- 4.1 The Council is a Data Controller under the Act and the GDPR and must comply with the Data Protection principles and be able to demonstrate compliance.
- 4.2 The Council's Data Protection Officer (DPO) is the Head of Legal and Democratic Services, the Deputy Data Protection Officer (DDPO) is the Legal Services Manager.
- 4.3 The DPO is responsible for the provision of advice, guidance, training, monitoring of compliance with Data Protection legislation including liaison with the Information Commissioner. The DPO will be responsible for keeping this document up to date.
- 4.4 The Council's Corporate Information Governance Group is responsible for approving this Policy and for managing compliance with the Act and the GDPR.
- 4.5 Overall responsibility for the Act and the GDPR will rest with the Chief Executive, Corporate Management Team and the Council's Corporate Information Governance Group in consultation with the Data Protection Officer.
- 4.6 Heads of Service will have overall responsibility for ensuring operational compliance with this Policy for the services that they are responsible for.
- 4.7 All employees of the Council will be responsible for ensuring that Subject Access Requests are dealt with in accordance with this Policy and that personal data is processed appropriately. All employees are responsible for ensuring that personal data which they use or process is kept secure and is not disclosed to any unauthorised person or organisation. Access to personal data should only be given to those who have and can show a need for access to the data for the purpose of their duties.
- 4.8 Personal data security breaches will be dealt with in accordance with in accordance with the Council's data breach management process, all staff will be aware of this and will follow this process which is accessible on the CBC intranet. Serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's office by the Data Protection Officer.
- 4.9 Where an elected Member has access to and processes information on behalf of the Council, the Member does so under the Council's registration and therefore must comply with this Policy. When Members process personal data whilst acting as representatives of their constituents in their wards or whilst representing a political party they do so as Data Controllers registered separately with the ICO.
- 4.10 Internal Audit will be responsible for undertaking reviews to assess the procedures and practices relating to Data Protection.

5. Data Subjects Rights

- 5.1 Data subjects which include the public, staff and Members have the following rights in relation to their personal data:
 - to be informed about what data is held, why it is being processed and who it is shared with;
 - to access their data;
 - to rectification of the record;

- to erasure of their data;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including profiling.

5.2 The Data Protection Officer will ensure appropriate processes are in place to ensure the Council enables the exercise of any of these rights.

6. Subject Access Requests

6.1 Requests for access to personal data (SAR) are processed by the Data Protection Office. There will be no charge for this provided that the request is not excessive or repetitive, manifestly unfounded or where you request copies of the same information, when we will charge a fee based on the administrative cost.

Requests must be in writing.

The Council aims to respond promptly to a Subject Access Request and no later than the statutory time limit.

However, if the Council considers the request to be complex, the time may be extended by up to two calendar months.

In this instance, the Council will notify the applicant in writing that the SAR requires further time and will provide an estimate of a reasonable time by which they can expect a response. These estimates shall be realistic and reasonable taking into account the circumstances of each particular case.

7. Disclosure to Third Parties

7.1 Personal data may need to be shared with other organisations or third parties in order to deliver services or perform our duties. The Council will only share personal data with other organisations and third parties where the sharing is necessary to achieve a clear objective and it is fair and lawful to do so. Data sharing agreements should be completed when setting up “on-going” or “routine” information sharing arrangements with third parties. However, these are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing the information should be kept.

7.2 The Council will maintain a Register of all Data Sharing Agreements.

8. Compliance

8.1 The Council will ensure that services document what personal data is held by the service, where it came from, who it is shared with, how long it is to be kept, the purpose and legal basis for collecting that data.

8.2 The Council has an overarching Data Protection Privacy Notice and a range of Service specific Privacy Notices which explain the following:-

- Name and contact details of the Data Controller and Data Protection Officer.
- The purpose and legal basis for processing the data.

- Retention Periods.
- The identity of those with whom data is shared
- Individual's rights.

- 8.3 Where processing is reliant on consent from an individual whose data is held, the Council will ensure consent is obtained and is current and actively managed. Consents will contain a positive opt-in with a mechanism to allow withdrawal of consent.
- 8.4 Legal advice, training and guidance will be given to Council staff and elected Members on Data Protection.
- 8.5 This Policy will be reviewed at the end of the first six months following the implementation of the Act and the GDPR and thereafter annually by the Corporate Information Governance Group.
- 8.7 It will be the responsibility of staff to complete a Privacy Impact Assessment (PIA) in the following situations that involve personal data:
- At the beginning of a new project or when implementing a new system.
 - When major changes are introduced into a system or process.

A PIA should be carried out at an early stage in the development of proposals.

9. Complaints

Where an applicant is dissatisfied with the level of service they have received on Data Protection matters they are entitled to complain about the actions of the Council through the Council's complaints procedure. This can be done by email by way of completion of a [Feedback form](#) or by writing to the Council.

Crawley Borough Council
Town Hall
The Boulevard
Crawley
West Sussex
RH10 1DU

If you remain dissatisfied with the Council's reply, you have the option of taking your complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

E-mail: casework@ico.org.uk
Tel: 01625 545700

Appendix 1 Definition of Terms

To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are provided for assistance:-

Data is any information held or recorded in any form by a public authority.

Automated decision-making means a decision made without human intervention solely by automatic means.

Data Controller means the Council as the organisation who determines how data is processed.

Data Processor means any person, other than an employee of the Council, who processes data on behalf of the data controller e.g. someone contracted to the Council to print documents containing personal data.

Data subject is the individual about whom personal data is processed.

Personal Data means Data which relates to a living individual who can be identified-

- (a) either directly from that data, or
- (b) indirectly from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Notice means a notice created by the data controller and made available to the data subject which explains how personal data is being processed.

Special category data (Sensitive Personal Data) means personal data consisting of information as to any of the following:-

- racial or ethnic origin
- political opinion
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- genetics;

- biometrics (where used for ID purposes);
- physical or mental health or condition
- sexual life or sexual orientation.
- personal data relating to criminal allegations, proceedings or convictions.

Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including organisation, adaptation or alteration, disclosure and destruction of the information or data and includes onward disclosure or sharing.

Profiling means the creation, manipulation collation or bringing together of information held or acquired about an individual for the purpose of recording or predicting an individual's conduct or behaviour.