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

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.

- 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:-

Retention Periods.

- 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