## 

## DATA PROTECTION POLICY

Chichester District Council manages personal data in accordance with the provisions of the Data Protection Act 1998. The Act applies to personal information about living, identifiable, persons.

The collection, holding and use of data is governed by eight principles.

Data protection principles

Chichester District Council manages personal data in accordance with the provisions of the General Data Protection Regulations (GDPR). The Regulations apply to personal information about living, identifiable, persons.

The GDPR outlines six data protection principles that this Council follows when collecting, processing and storing individuals' personal data. The data controller is responsible for complying with the principles.

The Principles are:

**1. Lawfulness, fairness and transparency**

The first principle is relatively self-evident: organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects.

The Council has a Register of Processing which sets out why we obtain, hold and use personal information.

**2. Purpose limitation**

The Council only collects personal data for a specific purpose, clearly state what that purpose is, and only collects data for as long as necessary to complete that purpose.  In almost all cases the Council "basis of processing" is to carry out the public duties of a local authority.

Some Processing is done for archiving purposes in the public interest or for scientific, historical or statistical purposes.

**3. Data minimisation**

The Council must only process the personal data that they need to achieve its processing purposes. This both improves security and makes it easier for the Council to keep data accurate and up to date.

**4. Accuracy**

The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

**5. Storage limitation**

Similarly, organisations need to delete personal data when it's no longer necessary.

The time the Council generally considers that it needs to hold onto data will relate directly to the reason why it is processing it and for each area that is detailed on the processing register.  More detail of this can be seen in the Retention Scheme (below)

**6. Integrity and confidentiality**

The GDPR states that personal data 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".

Technological and organisational best practices are constantly changing but the Council will work hard to maintain security of your information. This includes encryption and/or pseudonymising personal data wherever possible, and other options which are suitable and appropriate for the type of information being held.

Persons wishing to make an access request regarding personal data held by the council should write to 'The Data Protection Officer' at the council, stating the topic(s) of information required, and enclosing the statutory fee of £10.

For further information, see the website of the Information Commissioner.