# about PRIVACY NOTICES

You have the right to be informed what the council does with your personal data in accordance with the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) and the UK General Data Protection Regulation (UK GDPR). We do this through a privacy notice for our services which covers the following information in addition to that provided in our privacy policy.

### Purpose of our Processing

* This is a summary of why the service area needs to process your personal data. The main reasons we need information about you are to:
* deliver our district council services to you
* manage those services we provide to you
* recruit, train and manage the employment of our workers who deliver those services
* help investigate any worries or complaints you have about your services
* keep track of spending on services
* check the quality of services
* help with research and planning of new services

### How we collect your data

There are many ways in which we obtain your personal data. Mostly this is what you provide information to us directly, such as when contacting us about our services, completing forms and online applications or registering to take part in surveys. There are some situations when we receive or obtain your personal data from others besides yourself, for example when contacting you about parking notices. We are only able to collect your data for purposes we describe.

### Lawful basis for processing personal data

We only process your personal data where we have a lawful reason to do so as set out in Article 6 of UKGDPR. There are six available lawful bases we may rely on.

### Categories of personal data being processed

This will list the types of personal data, in UKGDPR terms, which we use. For example, your name, address or telephone number. It can also include information that, when put together with other information, can then identify a person. An example of this is your reference number for your account with us.

### Special categories of personal data being processed (sensitive data)

These are sensitive types of personal data that need more protection. This part of the privacy notice will tell you which, if any, that the service area will need to use. Some service areas may request special category personal data, including ethnic origin information, in order to ensure we can look at the impact our policies and practices have on different groups of people. The special personal information is likely to include anything that can reveal your:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes, such as fingerprint or face recognition)
* health (mental and physical)
* sex life, or sexual orientation

### Condition for processing special categories of personal data

If we do use any of the sensitive types of personal data stated above, this requires additional protection and Article 9 of UKGDPR identifies additional conditions for processing. This section will state which of the 10 available conditions we rely on for processing your special category personal data if applicable.

### Processing of personal data relating to criminal convictions and offences

Article 10 of UKGDPR requires us to only process criminal offence data if we identify a specific condition for doing so. The definition of criminal data is broad and includes allegations, including unproven allegations, criminal activity, proceedings and investigations. It also includes information relating to a lack of convictions and the data may be that of victims and witnesses of crime. This section will identify which of the 28 conditions for the processing of criminal offence data, as set out in paragraphs 1 to 37 of [Schedule 1 of the DPA 2018](https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted), we rely on.

### Who your data may be shared with

We may receive from and share your information with a number of other organisations as part of our processing and to help us deliver services, but only do so where we have a lawful basis to do so. Where we have these arrangements there is always an agreement in place to make sure that the organisation complies with data protection law.

We may also share your personal information when there is a legal duty to do so, or we feel there's a good reason that's more important than protecting your privacy. This doesn't happen often, but we may share your information:

* in order to find and stop crime and fraud
* if there are serious risks to the public, our staff or to other professionals
* to safeguard the protection of a child or vulnerable adult

The council is under a legal duty to protect the public funds it administers. To do this we may use the information you have provided to the council for the prevention and detection of fraud. We may also share this information with other bodies responsible for auditing or administering public funds for these purposes.

The Cabinet Office is responsible for carrying out data matching exercises. Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out. For more information on how the Cabinet Office use your personal data please view the [National Fraud Initiative privacy notice](https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text)

### Sharing data outside United Kingdom

We aim to restrict processing of your data to the UK. There may be some service providers, for example cloud-based software services, which store data outside of the UK. If any of the specific services areas do involve any processing outside of the UK, we are required to ensure the level of protection of your personal data is adequate. We ensure there are additional protections on your information ranging from secure ways of transferring data to ensuring we have a robust contract in place with that third party.

### Automated decision making

Automated individual decision-making is a decision made by automated means without any human involvement. Examples of this include an online decision to award a loan, or a recruitment aptitude test which uses pre-programmed algorithms and criteria. Automated individual decision-making does not have to involve profiling, although it often will do. Additional rules apply to protect individuals if we carry out solely automated decision making, and we must identify whether any of our processing needs these additional rules.

### How long will the data be kept

There's often a legal reason for keeping your personal information for a set period of time, and this ranges from months for some records to decades, or even permanently, for other records. When the end of the specified retention period is reached the data and information will be deleted or securely destroyed. Details of how long we keep your personal information can be found in the specific service are privacy notices.