



CORPORATE PRIVACY NOTICE

Overview

We are committed to protecting your privacy when you use our services. This privacy notice explains how we use information about you and how we protect your privacy.

Underpinning this corporate privacy notice are also individual service area privacy notices which will contain detailed information specific to that department.

What is Personal Information?

Personal information can be anything that identifies and relates to a living person. This can include information that when put together with other information can then identify a person. For example, this could be your name and contact details.

“Special” personal information

Some information is “special” and needs more protection due to its sensitivity. It is often information you would not want widely known and is very personal to you. This is likely to include anything that can reveal your:

- Sexuality and sexual health
- Religious or philosophical beliefs
- Ethnicity
- Physical or mental health
- Trade union membership
- Political opinion
- Genetic or biometric data
- Criminal history

Why we use your information

We may use information collected about you to:

- deliver services and support to you
- manage those services we provide to you
- 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



- to help with research and planning of new services
- prevent and detect crime and fraud

We only use collect and use the information we need to deliver a service or meet a requirement.

We will not sell your information to any third party.

Who do we share your information with?

We use a range of organisations to either store personal information or help deliver our services to you. Where we have these arrangements there is always an agreement in place to make sure that the organisation complies with data protection law.

We often complete a data privacy impact assessment (DPIA) before we share personal information to make sure we protect your privacy and comply with the law.

Sometimes we have a legal duty to provide personal information to other organisations. For instance we may need to give that data to courts including if the court orders that we provide the information.

We may also share your personal information when 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 for example:

- In order to find and stop crime and fraud; or
- If there are serious risks to the public, our staff or to other professionals;
- To protect a child; or
- To protect adults who are thought to be at risk for example if they are frail, confused or cannot understand what is happening to them

We are committed to protecting your privacy and handling your personal information responsibly. However, there may be situations where we need to share your information without your consent to protect you or others from serious harm.

If we believe there is a serious risk to your life, health, or safety—or that of someone else—we may share relevant personal data with appropriate services or authorities. Wherever possible, we will discuss this with you and seek your consent. But if obtaining consent is not possible or appropriate, we may still share your information under the following lawful bases:

- **Article 6(1)(d) UK GDPR** – where processing is necessary to protect the **vital interests** of the data subject or another person.



- **Article 6(1)(e) UK GDPR** – where processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority.
- **Article 9(2)(g) UK GDPR**, together with **Schedule 1, Part 2, Paragraph 18 of the Data Protection Act 2018** – where processing of special category data is necessary for reasons of **substantial public interest**, including safeguarding of children and individuals at risk.

We will only share the minimum information necessary and ensure that any sharing is proportionate, justified, and recorded in line with our safeguarding procedures. If it is safe to do so, we will inform you about what information was shared, with whom, and why.

This approach is consistent with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025, which all support lawful data sharing in safeguarding and emergency situations

Your rights

If we are holding your personal information you have the right:

- to be informed about how and why we process your personal information and how long we retain it for as well how you can complain
- of access which includes confirmation that your personal information is being processed and access to your personal information
- to rectification so that if you identify any of the personal information we hold about you is incorrect you can write to us asking us to correct it
- to erasure otherwise known as the right to be forgotten so that you may unless we require it to continue to provide a service to you request the deletion or remove of personal information
- to restrict processing which enables you to block or suppress is processing your personal information
- to data portability which allows you to obtain and reuse your personal information for your own purposes across different services
- to object to us processing your information based on legitimate interest or performance of a task in the public interest of official authority, direct marketing and for scientific/historical research and statistics
- related to the automated decision making and profiling which safeguards you against the risk that a potentially damaging decision is taken without human intervention

How long do we keep your personal information?



The Council maintains a Retention Schedule which sets out how long each service keeps your information. There is often a requirement under the relevant legislation which sets out a period of time. If none is specified then the corporate guidelines is generally for 6 years. The retention schedule can be found here and is currently being updated: [Retention schedule](#)

Access to personal information

CPBC tries to be as open as it can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a “subject access request” under the Data Protection Act 2018. If we do hold information about you we will:

- Give you a description of it;
- Tell you why we are holding it;
- Tell you who it could be disclosed to; and
- Let you have a copy of the information in an intelligible form

To make a request to CPBC for any personal information we may hold you need to put the request in writing addressing it to Data Protection Officer or writing to the address provided below.

We shall also require 2 items as proof of identification one of which must have a photograph of you with your name (e.g. drivers licence, passport) and the other with your name and address (e.g. utilities bill, bank or credit card statement).

Changes to this private notice

We keep our privacy notice under regular review. This privacy notice was last updated July 2025.

How to contact us

If you want to request information about our privacy policy you can email us: dpo@castlepoint.gov.uk or write to us at:

Data Protection Officer
Castle Point Borough Council
Council Offices
Kiln Road
Thundersley
Benfleet
Essex SS7 1TF



CPBC's Data Protection Officer

CPBC's Data Protection Office is Angela Law and she may be contacted at the above address.

Information Commissioners Office

If you want to any further information about your privacy rights or to make a complaint you can contact the Information Commissioner's Office at the address below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire Sk9 5AF

Email: <https://ico.org.uk/global/contact-us/>

Website: www.ico.org.uk