CASTLE POINT BOROUGH COUNCIL
DATA PROTECTION POLICY

This policy sets out how we will protect personal data, special category data and criminal offence data.

The UK GDPR governs the processing of personal data, gives individuals rights over their personal data and ensures organisations handle data in accordance with Art. 5 of the UK GDPR (the Data Protection Principles). The Data Protection Act 2018 supplements the UK GDPR with additional provisions for law enforcement and intelligence services, provides for the regulation of processing in areas not covered by the UK GDPR, and sets out the framework for the Information Commissioner's powers and enforcement mechanisms. The policy meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It further meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

In line with these legal requirements, this policy outlines how Castle Point Borough Council ensures compliance with the UK GDPR and the Data Protection Act 2018.

It sets out the safeguards and accountability measures in place for processing personal data, including special category and criminal offence data.

Data Protection Officer and Senior Information Risk Owner

The Council has designated Angela Law (Assistant Director – Legal & Democratic Services and Monitoring Officer) as Data Protection Officer and Ben Brook (Assistant Director – Policy & Performance) as the Senior Information Risk Officer. These Officers will be responsible for coordinating all data protection issues for the Council, for ensuring that the Council's Registration with the Information Commissioner (the Commissioner) is kept up-to-date, for the receipt of subject access requests and the coordination of and compliance with the requirements of the Act and GDPR when such requests are received. The Data Protection Officer shall comply with the statutory obligations assigned to her as Data Protection Officer under the Act.

The following principles, derived from Article 5 of the UK GDPR, underpin all data processing activities carried out by the Council:

Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

(We ensure that processing is fair by providing detailed privacy notices to individuals whose personal data is being processed. All individuals are advised of their right to contact the Data Protection Officer with any queries regarding the processing of their personal data. We will only process personal data fairly and will not mislead individuals about how their data may be used.)

Principle 2 - Personal data shall be 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 not be considered to be incompatible with the initial purposes.

(We meet this obligation by explaining through our privacy notices which legal basis we are relying on when processing personal data. We will only use the data for the purposes for which it was collected unless we advise individuals, prior to any additional use, of our intentions and the rights they have in relation to any further use.)

Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

(We meet this obligation by only collecting what is required for a particular purpose and ensuring that we have sufficient relevant information for that purpose.)

Principle 4 – Personal data shall be 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

(We meet this obligation by ensure that personal data is accurate and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.)

Principle 5 – Personal data shall be 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

(We meet this obligation by ensuring that personal data is managed in line with our retention schedule, and either deleted or completely anonymised when it is no longer necessary for us to use it. The period for which we retain personal data is explained in each privacy notice relevant to that service.)

Principle 6 – Personal data shall 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

(We meet this obligation by ensuring that our technical and organisational controls. Our organisational controls include:

- Appropriate roles and responsibilities including a Data Protection Officer and Senior Information Risk Owner
- Robust policies and procedures which are regularly reviewed
- Regularly training our staff in their data protection responsibilities
- Ensuring our processing activities are transparent and secure, including

    - Records of Processing Activities
    - Data Protection Impact Assessments

- Contractual Controls to govern the use of personal data by our suppliers
- Physical security controls including

    - Restricted access to physical storage of sensitive personal data
    - Visitor management

- Security breach management

Our Technical Controls include:

- Firewalls, anti-malware and patching
- Disaster Recovery and Business Continuity arrangements
- Role based access controls to personal data
- Password management
- Sending email securely)

Principle 7 - The controller shall be responsible for, and be able to demonstrate, compliance with the principles

(We meet this obligation by maintaining Records of Processing Activities which are available on demand to the Information Commissioner. We routinely carry out Data Protection Impact

Assessments for any processing of special categories of data or where there is a high risk to individuals' privacy. We have appointed a Data Protection Officer and have defined policy and process to manage the exercising of data subjects' rights.)

Data Subjects Rights (transparency)

Under GDPR data subjects have defined rights that include:

- The right to information and transparency;
- The right of access and rectification;
- The right to erasure ("right to be forgotten");
- The right to restrict processing;
- The right to data portability;
- The right to object.

The Council in its policies and procedures and practices shall seek to recognise circumstances that engage a data subject's rights outlined in legislation

Privacy Notices

The Council is open and transparent in the way that it processes and uses personal data it collects. Each service area of the Council will therefore maintain and publish Privacy Notices which are available for public inspection and on the Council's website.

The Council's Privacy Notice provides the following information:

- the lawful purposes of the data being processed;
- category of personal data in question;
- the recipients to which the data has been disclosed;
- any third country recipients;
- the time frame that personal data will be retained;
- right to erasure (right to be forgotten) and restriction;
- right to file a grievance with the Data Protection Officer/Information Commissioner;
- whether or not personal data is being used for automated decision-making and profiling purposes e.g. direct marketing;
- logic and reasoning behind the processing of data and the intended use of the processed data

Retention of Personal Data

The Council shall put in place practices for the weeding, deleting and destruction of personal data in accordance with the Council's Data Retention Policy and to ensure compliance with the right to be forgotten under the Act.

The Council will undertake a rolling audit and review of its data protection policies and procedures and systems dealing with the processing of personal data together with the controls in place to ensure compliance with the Act.

Contractors, consultants, partners and third parties

All contractors, consultants, partners, or other servants or agents of the Council are considered Data Processors under GDPR:

1. Are subject to a level of direct accountability and liability.
2. Are contractually bound through contractual terms and conditions to ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Council are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act.
3. Notify the Council's Data Protection Officer and provide that person with any information needed by them where they consider there is a breach of the Act and/or GDPR
4. Understand that any breach of any provision of the Act and/or GDPR will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm and a breach of the Act.
5. Promptly, pass any Data Subject Access Requests relating to the Council's business to this Council's Data Protection Officer and provide that person with any information needed by them to comply with the Data Subject Access Request.
6. Allow data protection audits by the Council to ensure compliance with their contractual obligations as well as their obligations under the Act and GDPR
7. Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

Data Subject Access Requests

The Council has adopted a process and procedure for handling Data Subject Requests to ensure consistency, predictability and accountability in relation to these requests. Any requests should be made to the Data Protection Officer in accordance with the Subject Access Procedure. You will need to be able to provide a suitable form of identification before the request is processed.

Cyber Security Policy

The Council has adopted a Cyber Security Policy which outlines how the Council shall manage its ICT security in relation to the processing of personal data.

Data Breach

A privacy breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, basically the compromise of personal information to an unauthorised party. This may be through cyber breaches; electronic data breaches via hackers, malware, phishing and other devious means. Example of such breaches includes breaches of credit card data, personal health records, financial information and many other personal data types.

No disclosure of data is to be undertaken by any data processor which breaches any of the provisions of the Act or GDPR as interpreted by the Council, the Commissioner or the courts for the time being.

The Council regards any unlawful breach of any provision of the Act by any employee of the Council as being a disciplinary matter. Any employee(s) who breach this policy will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct.

The Council has in place a Privacy Breach Incident Response Procedure and identified an Incident Response Team for dealing with data breaches.

For further information about how we process personal data please see our online privacy notices on our website or contact our Data Protection Officer, Angela Law on by email at dpo@castlepoint.gov.uk or by calling 01268 882200.