Castle Point Borough Council

Data Protection Act 2018
Corporate Policy

Introduction

Castle Point Borough Council ("the Council") is committed to full compliance with the Data Protection Act 2018 ("the Act") and the General Data Protection Regulations 2016 ("GDPR") within a "joined-up" service environment. The Council will therefore follow procedures designed to provide that all elected members, employees, contractors, consultants, partners, or other servants or agents of the Council (collectively referred to as "the data processors") who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the Act and GDPR.

Data Protection Officer and Senior Information Risk Owner

The Council has nominated Andrew Roby Smith Strategic Director as Data Protection Officer and Fiona Wilson Head of Law of 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 co-ordination 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 him as Data Protection Officer under the Act.

Notification Requirements

All purposes for which personal data is obtained or processed will be notified to the Commissioner as required by the Act as part of the registration process.

No personal data will be obtained, held or processed, for any purpose, without that purpose being notified to the Commissioner as required by the Act.

General Data Protection Regulations

GDPR can be broken down into six overall guiding principles:

1. Lawfulness, transparency and fairness;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy;
5. Storage limitation;
6. Confidentiality and integrity

These principles the Council shall adhere to when designing, implementing and operating its functions and services to the public which involve the processing of personal data.

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 GDPR.

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. This Policy can be found: https://www.castlepoint.gov.uk/council-strategies-and-policies

Processing Personal Data

In this policy document, the term "processing" means:

> Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-
>
> (a) organisation, adaptation or alteration of the information or data,
>
> (b) retrieval, consultation or use of the information or data,
>
> (c) disclosure of the information or data by transmission, dissemination or otherwise making available,
>
> (d) or alignment, combination, blocking, erasure or destruction of the information or data.

and "processed" shall be construed accordingly.

The Council shall identify what personal data is being collected, where the data is being sourced, why the data is being collected, how it is processed, who has access, how long the data is retained and where the data is being transferred to. This information will be recorded in each service Information Asset Register.

All data will be processed in accordance with the Act unless such processing falls to be exempt under section Article 10 of the Act (criminal convictions). In particular, form and document design will be kept under review, to ensure compliance with the data protection principles under the Act.

All processing of personal data by the Council will be subjected to Data Privacy Impact Assessments, taking into account:

(i) the likelihood of a breach of the data protection system;

(ii) the potential impact on the data subject, elected members, managers or staff, and

(iii) the level of controls in place with regard to the data,

together with the setting and testing of clear controls to minimise breaches of the Act.

All data processors are to be fully trained in and aware of this policy and their duties and responsibilities under the Act.

All elected members are to be made fully aware of this policy and their duties and responsibilities under the Act.

All data processors will ensure that appropriate security measures are undertaken to safeguard personal data, commensurate with the nature of the data concerned.

To ensure full compliance with the requirements of the Act protocols and procedures will be set and annually tested to ensure the authority's ability to respond to individual access requests promptly and, in any event, within the timescales laid down in law.

Breach of the Act and GDPR

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.

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. Privacy Notices shall be published on all forms and on the Council's website where personal data is sought from users of the Council's services.

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 eg 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 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 for disclosure of personal data shall be passed to the Council Information Officer who shall record details of the request and handle it in accordance with the Data Subject Request procedure. https://www.castlepoint.gov.uk/council-strategies-and-policies

Version: 1
Date: 25 May 2018