# Castle Point Borough Council

# Data Protection

# Corporate Policy

Castle Point Borough Council ("the Council") is committed to full compliance with the Data Protection Act 1998 ("the Act") 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 users") 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.

The Council will nominate an officer who will be responsible for coordinating all data protection issues for the Council, for ensuring that the Council's Notification to 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 when such requests are received.
All purposes for which personal data is obtained or processed will be notified to the Commissioner as required by the Act.

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.

All data will be processed fairly and lawfully, unless such processing falls to be exempt under section 29 of the Act (crime and taxation). 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 a risk assessment, 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.

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

All data users 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.

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.

Each functional area of the Council will compile and maintain a combined Data Protection Policy and Code of Practice, which will be subordinate to this policy and will be advertised and available for public inspection. Such policies and codes of practice shall incorporate procedures for the weeding, deleting and destruction of personal data to ensure compliance with the third, fourth, fifth and seventh data protection principles under the Act.

The Council will undertake a rolling audit and review of all data protection systems and controls to ensure compliance with the Act, this policy and individual service data protection policies and codes of practice, including data security.

All contractors, consultants, partners, or other servants or agents of the Council must:

1. 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. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm.

2. Promptly, pass any subject access requests relating to the Council's business to this Council's Data Protection Officer for the time being and provide that person with any information needed by them to comply with the subject access request.

3. Allow data protection audits by the Council of data held on its behalf.

4. Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

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.

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.

Any orders or requests for disclosure of personal data, which are deemed to fall under one of the categories of exemptions under sections 27 to 37 of the Act, or under any other statutory power shall be passed promptly to a nominated officer within each functional

area of the Council, who will be responsible for and take reasonable steps to ensure that the request does fall within the relevant exemption and comply with the request in a manner deemed by that person to be appropriate.

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

A copy of the Council's main data protection notification is attached as part of this policy.