Lewes District Council

EASTBOURNE
Borough Council
Working in partnership with Eastbourne Homes

Data Protection Policy

October 2021
V03

Document information

Version Number	V03	
Document Status (Draft/Final)	Final	
Effective from date	October 2021	
Review date	October 2022	
Reason for document	Alignment of policies; and amendments to comply with the Data Protection Act 2018 and UK General Data Protection Regulation.	
Linked documentation	1. Data Sharing Policy 2. Data Protection Impact Assessment Policy 3. Personal Data Breach Plan 4. Access to Information Policy	
Author	Name	Rachael Page
	Job Title	Information Governance Manager
	Team	Legal
	Contact	rachael.page@lewes-eastbourne.gov.uk

Contents

1. Introduction

1.1 Lewes District Council and Eastbourne Borough Council support the objectives of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA) and seek to ensure compliance with this legislation.

1.2 The processing of data by the councils is essential to services and functions and will often involve the use of personal and/or 'special category' personal data. Compliance with data protection legislation will ensure that such processing is carried out fairly and lawfully.

1.3 In accordance with the UK GDPR and the Human Rights Act (1998) (HRA) Article 8, the processing of personal data must respect the rights and freedoms of every living individual (the 'data subject'). Equally, the legislation must be applied in a manner that enables the councils, as a public body, to function effectively.

1.4 This policy should not be read in isolation and regard should be given to the councils' Access to Information Policy.

2. Purpose

2.1 The purpose of this policy is to ensure that the provisions of the UK GDPR and DPA are adhered to whilst protecting the rights and privacy of living individuals**;**

2.2 In particular, this policy will:

- Assist the councils to comply with all requirements of the UK GDPR and DPA.
- Ensure that data access requests are dealt with in a timely manner.
- Ensure adequate consideration is given to whether or not personal data should be disclosed.
- Through privacy notices, ensure that individuals are made aware of what personal data is processed and stored by the councils about them and advise them of their rights under data protection legislation.

2.3 The councils will endeavour to promote greater openness, provide increased transparency of data processing and build public trust and confidence in the way that the councils manage information about their customers.

3. Aims

3.1 This policy sets out the councils' commitment to upholding the data protection principles set out in the UK GDPR and managing information held fairly and lawfully. It seeks to strike an appropriate balance between the councils' need to make use of personal information in order to manage their services efficiently and effectively and respect for the privacy of individuals.

3.2 To assist staff in meeting their statutory obligations under the UK GDPR and DPA and provide a guide to the public on the councils' obligations with regard to the processing of their personal data.

4. Council statement on data protection requirements

4.1 The councils will abide by the six data protection principles as detailed below:

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

- 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, in accordance with UK GDPR Article 89(1) not be considered incompatible with the initial purposes ('purposed limitation')

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

- 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 ('accuracy')

- 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject ('storage limitation')

- 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 ('integrity and confidentiality')

4.2 This policy applies to the acquisition and processing of all personal data within the councils and sets out how the councils will ensure that individual rights and freedoms
are protected.

- The councils will comply with Article 8 of the HRA in respect of the processing of personal data.

- The councils will keep all electronic and manual records in accordance with the Retention and Disposal Schedule and Data Retention Policy.

- Periodically a risk assessment will be undertaken, via audit reviews, for all data processing, and when inadequate controls are identified, technical and organisational security measures will be taken, appropriate to the level of risk identified.

- Personal data will only be used for the direct promotion or marketing of goods or services with the explicit consent of an individual.

- Data sharing and data matching with external agencies will only be carried out under a written agreement or contract setting out the scope and limits of the data sharing/matching. This should be in line with the councils' Data Sharing Policy.

- Elected Members and staff will be trained to an appropriate level in the use and supervision of personal data.

- Breaches of this policy may be subject to action under the councils' disciplinary procedure.

5. Roles and responsibilities

5.1 The councils' Corporate Management Team is responsible for approving this policy.

5.2 Overall responsibility for UK GDPR and DPA compliance will rest with the Chief Executive in consultation with the Data Protection Officer and Information Governance Manager.

5.3 The councils' Data Protection Officer and Information Governance Manager are responsible for the provision of advice, guidance and training regarding data protection legislation and will be responsible for keeping this document up to date.

5.4 All employees of the councils will be responsible for ensuring that Subject Access Requests are dealt with in accordance with this policy and that personal data is processed appropriately. This includes ensuring that personal data supplied to the councils is accurate, up-to-date and held securely.

5.5 Heads of Service will be responsible for ensuring operational compliance with this policy within their own departments and for becoming involved in consultations with the Data Protection Officer or Information Governance Manager when applicable.

5.6 Internal Audit will undertake reviews to assess the procedures and policies in place that relate to data protection.

6. Information requests

6.1 Requests from data subjects for copies of personal data the councils hold about them (Subject Access Requests) can be made in writing or verbally. This includes requests transmitted by electronic means, providing they are received in a legible form and are capable of being used for subsequent reference.

6.2 If a person is unable to articulate their request in writing, we will provide advice to assist them in formulating their request.

6.3 If the information sought is not described in a way that would enable the councils to identify and locate the requested material, or the request is ambiguous, the councils will seek additional clarification.

6.4 The councils will not provide assistance to an applicant who is not the data subject, unless it is confirmed that the explicit consent of the data subject has been obtained for a third party to request the data subject's personal data.

7. Prompt replies to requests

7.1 The councils are committed to dealing with requests for information promptly and no later than the statutory requirement of one calendar month.

7.2 The councils would not expect every application for information to take one calendar month and will endeavour, where possible, to provide the requested information at the earliest opportunity from the date of the request.

7.3 However, if the councils consider the request to be complex, they may extend the time by up to two extra calendar months.

7.4 In this instance the councils will notify the applicant in writing that the SAR requires further time and will provide an estimate of a 'reasonable time' by which they expect a response to be made.

7.5 These estimates shall be realistic and reasonable taking into account the circumstances of each particular case.

8. Data subject rights

8.1 Subject to some legal exceptions, individuals will have the rights below.

- Right to request a copy of any information we hold about them
- Right to rectification (if inaccurate data is held)
- Right to erasure ('right to be forgotten') in certain circumstances
- Right to restriction of processing in certain circumstances
- Right to data portability (personal data transferred from one data controller to another)
- Right to object (to profiling, direct marketing, automated decision-making)

9. Exempting information from non-disclosure

9.1 The UK GDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA there are circumstances which allow disclosure of a data subject's personal data to an appropriate third party, or for it to be used in a situation that would normally be considered in breach of UK GDPR.

9..2 The councils will only use an exemption where it is lawful and in the public interest to do so, i.e. prevention of crime, or where the functioning of the councils require the processing of personal information to be exempt so that it can provide statutory services to members of the public.

10. Refusal of subject access requests

10.1 The councils will not supply information to a data subject if:

- They are not satisfied with the identity of the data subject

- Compliance with the request will inadvertently disclose personal information relating to another individual without their consent
- The applicant has recently requested the same or similar information

10.2 The councils consider that when a valid reason, which is both robust and legally defendable, exists for refusing the disclosure of information to either the data subject or a third party, the information should be withheld.

10.3 When information is withheld, full explanations of the reasoning behind the refusal must be provided to the applicant. This explanation must also include the details of how the applicant can complain about the councils' decision.

10.4 All requests for personal data made by the data subject will be dealt with under Chapter 3 - Rights of the Data Subject section of the UK GDPR, not the Freedom of Information Act 2000.

11. Appeals and complaints

11.1 Where an applicant is dissatisfied with the councils' handling of a data protection matter , they are entitled to complain through the internal reviews procedure. All complaints should be forwarded to:

Information Governance Appeals Officer
Eastbourne Town Hall
Grove Road
Eastbourne
BN21 4UG

E-mail : foi.appeals@eastbourne.gov.uk

11.2 The applicant will receive a response to their correspondence within twenty working days. If the applicant remains dissatisfied with the councils' reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

E-mail: casework@ico.org.uk
Tel: 01625 545700

11.3 Any other complaints regarding the councils' processing of personal data should be sent to the councils' Data Protection Officer at Eastbourne Town Hall, Grove Road, Eastbourne, BN21 4UG or by email to: accesstoinformation@lewes-eastbourne.gov.uk.

Appendix 1

Interpretation of Terms

1. 'Personal data' means any information relating to an identified or identifiable living individual ('data subject')

   'Identifiable living individual' means a living individual who can identified, directly or indirectly, in particular by reference to:

   a) an identifier such as a name, an identification number, location data or an online identifier, or
   b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

2. 'Special category (sensitive) personal data' means data relating to:

   - Racial or ethnic origin
   - Political opinions
   - Religious/philosophical beliefs
   - Trade union
   - Processing of biometric/genetic data to identify someone
   - Health
   - Sex life or sexual orientation

3. 'Processing', in relation to personal data, means an operation or set of operations which is performed on personal data or on sets of personal data, such as:

   a) collection, recording, organisation, structuring, storage
   b) adaptation or alteration
   c) retrieval, consultation, use
   d) disclosure by transmission, dissemination or otherwise making available
   e) alignment or combination, or
   f) restriction, erasure or destruction.

4. 'Data subject' means the identified or identifiable living individual to whom personal data relates.

5. ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

‘

6. ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.