East Lindsey District Council
www.e-lindsey.gov.uk

Data Protection Policy

Document Control

Organisation	East Lindsey District Council
Title	Data Protection Policy
Author	Alison Sparks
Protective Marking	Not Protected
Review Date	May 2019

Revision History

Revision Date	Reviser	Previous Version	Description of Revision
25 May 2018	Alison Sparks		Alignment of policies and compliance with updated Data Protection Act and General Data Protection Regulation
19-06-2019	Alison Sparks	Version 1	Annual review and additional information for law enforcement processing.

CONTENT

1. Introduction

1.1 East Lindsey District Council supports the objectives of the General Data Protection Regulation (GDPR), and The Data Protection Act 2018 (DPA) and seeks to ensure compliance with the data protection legislation that regulates the processing of information relating to living individuals.

1.2 The GDPR & DPA (the Legislation) provide protection for individuals as to how their personal information is used by organisations, businesses and the Council. The Council as a 'Data Controller' is registered with the Information Commissioner's Office and is required to keep records of processing activities, which must be made available to the Information Commissioner's Office upon request.

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

1.4 The GDPR and the Human Rights Act (1998) (HRA) Article 8, make it clear that the processing of personal data must respect the rights and freedoms of the data subject (a living individual), but at the same time be adequate enough for the Council to function effectively.

2. Purpose

2.1 As a Council we are bound by the requirements of the Legislation and are fully committed to complying with it. The purpose of this policy is to ensure that all employees, elected members, temporary staff, agency workers, contractors, agents, consultants, partners and any other person, who has access to any personal data of living individuals held by, or held on behalf of the Council, are fully aware of and act in accordance with the provisions of the Legislation to ensure that the personal data is processed lawfully and fairly.

2.2 It will apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

2.3 All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall complete training, at least annually, to ensure compliance with their responsibilities.

2.4 In particular this policy will:

- Assist the Council to comply with all requirements of the GDPR and DPA.

- Meet the requirements at paragraph 5 of Part 2 of Schedule 1 and paragraph 38 and 39 of part 4 of Schedule 1 DPA and is the appropriate Policy Document as required by the Schedule, which explains the Council's policies regarding the retention and erasure of personal data including that for special category and criminal offence data.

- Detail the safeguards in place when processing special category and criminal offence data

- Ensure that personal data is readily available on request and that requests from data subjects are dealt with in a timely manner.

- Ensure adequate consideration is given to whether or not personal information should be disclosed.

- Ensure increased awareness of data subjects to the amount of personal data processed and stored by the Council about them and advise them of their rights under the data protection legislation.

3. Aims

3.1 This policy sets out the Council's commitment to upholding the data protection principles set out in the Legislation and managing the information it holds lawfully, fairly and transparently.

3.2 It seeks to strike an appropriate balance between the Council's need to make use of personal information in order to manage its services efficiently and effectively and respect the privacy of individuals.

3.2 It looks to assist staff to meet their statutory obligations under the GDPR and DPA and provide a guide to the public on the Council's obligations with regard to the processing of their personal data.

4. The Council's data protection responsibilities

4.1 This policy applies to the processing of all personal data within the Council and sets out how the Council will ensure that individual rights and freedoms are protected, including the Council's commitment: -

- To comply with Article 8 of the HRA in respect of the processing of personal data.

- As the Data Controller, to make individuals aware of the purpose(s) it is processing their personal data for and will seek consent where appropriate. '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.

- To provide general information to the public about their statutory rights under the GDPR and DPA on our website.

- To hold the minimum amount of personal data necessary to carry out its functions, and every effort will be made to ensure the accuracy and relevance of the data processed.

- To keep all electronic and manual records in accordance with its Records Management Policy.

- To keep the personal data the council holds in accordance with the six principles of data protection under the GDPR and in line with the Council's Retention and Disposal Schedules.

- To periodically undertake a risk assessment, 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.

- To ensure personal data is only being used for the direct promotion or marketing of goods or services with the consent of an individual.

- To data sharing and data matching with external agencies only being carried out under a written contract or information sharing agreement setting out the scope and limits of the data agreement. This should be in line with the Council's Information Sharing Agreement Guide.

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

- That any breaches of this policy may be subject to action under the Council's disciplinary procedure.

4.2 Article 5 of the GDPR sets out the Data Protection Principles and our procedures for complying with them are listed against each one:

Personal data shall be:

- **Principle 1** - Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). This Council will ensure that personal data is only processed where it is lawful to do so; ensure it is processed fairly and provide privacy information, where required, to ensure transparency.

- **Principle 2** - 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 Article 89(1) not be considered incompatible with the initial purposes ('purposed limitation'). This Council will only collect personal data for specific, explicit and legitimate purposes and will not use it for an incompatible purpose without, where required, informing the data subject first.

- **Principle 3** - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). This Council will collect the minimum amount of data required for the purpose ensuring it is adequate and relevant to that purpose.

- **Principle 4** - 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'). This Council will ensure data is accurate and up to date where possible.

- **Principle 5** - 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 required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'). This Council will not keep identifiable personal data where it is no longer necessary (unless waiting for systems updates/replacements where needed) and will keep destruction records of data that has been deleted.

- **Principle 6** - 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'). This

Council has appropriate technical and organisation measures in place to ensure the security of its data.

- **Accountability Principle** - The Council will demonstrate its accountability by ensuring that appropriate records are kept of processing activities; Data Protection Impact Assessments are carried out for new or high risk processing; that the appointed Data Protection Officer provides independent advice, monitors the Council's compliance and reports to the highest level of management and that the Council's internal procedures and policies ensure that data is processed in compliance with the law.

4.3 In terms of the **storage and security of personal data**, appropriate steps will be taken to ensure that personal data is kept secure against unauthorised or unlawful loss, destruction or disclosure and in particular ensure that:

- Paper files and other records or documents containing personal / sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by the use of secure passwords which have forced changes periodically. (Every 90 days)
- Individual passwords should be such that they are not easily compromised.
- When personal data is required to be transferred to another person, organisation, or other third party that all appropriate measures have been taken to maintain appropriate security levels including encryption, where appropriate and the use of secure email accounts.

5. Roles and Responsibilities

5.1 The Council's Leader (Corporate Affairs Portfolio Holder) is responsible for approving this policy and for managing compliance with the GDPR and DPA.

5.2 The Senior Information Risk Officer (SIRO) has overall responsibility for the GDPR and DPA within the Council, but it is not the SIRO's responsibility to ensure all of the Data Protection principles are complied with. For instance ensuring that all personal information is accurate and up-to-date is the responsibility of the individual employee processing the information.

5.3 The Council's Data Protection Officer (DPO) is 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 Council 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 Council is accurate, up-to-date and held securely.

5.5 Assistant Directors and Service Managers will be responsible for ensuring operational compliance with this policy within their own Units/Teams.

5.6 Internal Audit will undertake periodic independent reviews to assess the Council's arrangements for data protection.

6. Information requests

6.1 Requests from data subjects for copies of personal data the Council holds about them (Subject Access Requests - SAR) can be made verbally or in writing. Where requests are made verbally a record must be made in writing and then sent to the requester to confirm the accuracy of the request.

6.2 If a person is unable to articulate their request in writing the Council 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 Council to identify and locate the requested material, or the request is ambiguous, the Council will seek additional clarification.

6.4 The Council 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.

6.5 Requests for 'everything' will be considered to be 'manifestly unfounded' or 'excessive' and clarification will be sought from the requestor to establish the exact nature of the information they require.

7. Replies to requests

7.1 The Council is committed to dealing with requests for information promptly and no later than the statutory guideline of ***one month.***

7.2 The Council 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 Council consider the request to be complex, they may extend the time by up to two extra calendar months. Any decision to extend time must be made by the DPO.

7.4 In this instance the Council's DPO 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 As well as access rights data subjects also have the following rights:

- 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).
- Right to withdraw consent.

8.2 If a data subject asks an employee to exercise any of these rights the employee must discuss it with the DPO who in consultation with the Service Manager will determine whether the request should be complied with.

9. Exempting information from non-disclosure

9.1 The 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 a third party, or for it to be used in a situation that would normally be considered to breach the GDPR.

9.2 Exemptions from the non-disclosure of personal data are given below. This list is not exhaustive.

- Crime and taxation:

  a) The prevention and detection of crime
  b) The apprehension or prosecution of offenders, or
  c) The assessment or collection of any tax or duty or of any imposition of a similar nature

- Crime and taxation: risk assessment systems

- Immigration
- Information required to be disclosed by law etc. or in connection with legal proceedings
- Safeguarding

9.3 The Council will only use these exemptions where it is lawful to do so, i.e. prevention of crime, or where the functioning of the Council requires the processing of personal information so that it can provide statutory services to members of the public. Any exemptions will only be applied with the consent of the Data Protection Officer.

10. Refusal of subject access requests

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

- The Council is 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
- The request is for 'everything'

10.2 The Council 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 Council's decision to the Information Commissioner's Office.

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 GDPR, not the Freedom of Information Act 2000.

11. Complaints

11.1 Where an applicant is dissatisfied with the level of service they have received, they are entitled to complain about the actions of the Council through the internal appeals procedure. All complaints should be forwarded to the Data Protection Officer or E-mail: Information.management@e-lindsey.gov.uk

11.2 The applicant will receive a response to their correspondence within twenty working days. If the applicant remains dissatisfied with the Council's reply, they have the option of escalating their complaint by

forwarding their complaint to the Council's Senior Information Risk Officer or E-mail: Information.management@e-lindsey.gov.uk

11.3 If the applicant remains dissatisfied with the Council's reply they have the option of escalating 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 Cheshire
SK9 5AF
E-mail: casework@ico.org.uk
Tel: 01625 545700

12. Breaches and Offences

12.1 A deliberate breach of the rules and procedures identified in this policy by a member of staff will likely constitute an offence under the Legislation and if proven could result in disciplinary action.

12.2 Any accidental breach can also constitute an offence under the Legislation which could lead the Information Commissioner's Office taking enforcement action and imposing a financial penalty on the Council. Any breach could also lead to adverse publicity for the Council.

12.3 Any potential breaches ***must*** be notified to the SIRO, DPO or Deputy DPO ***immediately*** by completing the DPA Breach Notification Form which is available on the Council's intranet. The DPO will keep a log of all potential breaches and will, in liaison with the SIRO and Service Manager, decide on the most appropriate course of action.

12.4 The ICO will be notified of all serious breaches in line with published guidance and in any event ***within 72 hours*** of the alleged breach. The DPO or Deputy DPO, in consultation with the SIRO will be responsible for notifying the ICO and assisting the ICO in any investigations.

12.5 The Council uses a risk matrix to categorise breaches and assist with identifying those which should be reported to the ICO although the final decision on reporting rests with the SIRO.

13. Data processing on behalf of the Council

13.1 All contractors, consultants, partners or other agents of the Council must ensure that they and all their staff who have access to personal data held by or processed 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.

13.2 Where appropriate or required by law we will enter into a written Data Processing agreement and ensure a contract is in place setting out more fully the terms under which the Council requires its data to be processed.

14. Information Sharing

Where we determine that there is a legitimate reason for sharing information this will be undertaken using one of the following methods:

- Ensuring that there is an information sharing agreement in place with the organisation.
- Where the relationship is one of controller/processor ensure that there is a contract in place setting out the basis upon which the processor may treat and process the personal data.
- Using an appropriate mechanism as defined within the Act for sharing information.

We retain the right of non-disclosure of information should we deem that the mechanism for sharing personal data is not appropriate, unless we are compelled to do so by a Court Order or other lawful mechanism.

15. Special Categories of Personal Data and Criminal Convictions Data appropriate Policy Document

15.1 This is the appropriate policy document that sets out how we will protect special category and criminal convictions personal data.

15.2 It 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.

15.3 It also 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.

15.4 The Council, through appropriate management controls will, when processing special category personal information and criminal data about any individual:

- Maintain a record that will contain the following information:

  a) which condition(s) are being relied on under Article 9 (2) of the GDPR or the relevant Schedule of the DPA 2018; and

  b) collect and process the data in accordance with its retention and erasure policies and, if it is not, provide reasons for not following those policies.

- Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

- When processing data for Law Enforcement Purposes the council will comply with the data protection principles in S.35-40 of Part 3 DPA 2018 and if the processing is 'sensitive' ensure that the processing is strictly necessary and satisfies one of the conditions in Schedule 8 and this Policy document meets the requirements of Section 42 for the purposes of sensitive processing.

- When processing criminal offence data (other than for law enforcement purposes) or special category data the Council will comply with the data protection principles as listed at 4.2 above and Schedule 1 DPA 2018.

15.5 The Council's retention and erasure periods can be found in its retention schedules and Information Asset Registers. Where data cannot be deleted then a reason should be recorded on the Asset Register.

15.6 If in doubt please consult with the Data Protection Officer.

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 10

   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:

☐ 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. ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

7. ‘Filing system’ means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

8. ‘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.

9. Article 9 GDPR

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

10. Criminal Offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

11. Law Enforcement Processing means processing under Part 3 of the Data Protection Act 2018 for the law enforcement purposes and is described in S.31 of the Act as for the ‘prevention, investigation,

detection or prosecution of criminal offences or the execution of criminal penalties including safeguarding against and prevention of, threats to public security'.