Data Protection Policy

??? 2020

Version Number	4.0
Approved by	Corporate Policy and Resources Committee
Date approved	12 Apr 2018
Review Date	March 2023
Authorised by	Director of Resources
Contact Officer	Data Protection Officer

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
16/2/2012		Draft V0.3	Formally adopted by Policy & Resources Committee
15/8/2013		V1.0	Amendments resulting from annual review: Paras 3.1,3.3,9.1,13.1,14.2 – amended to reflect new job titles.
27/08/2014		V1.1	Review – no amendments req'd
6/10/2015		V2.0	Change Service Managers to Team Managers in para 5.3
23/11/2016		V2.1	Amendments resulting from annual review: Role of Data Protection Officer formalised; job titles updated; review period extended to 2 years; paras renumbered and minor typographical corrections.
12/4/2018		V3.0	UK GDPR Amendments
July 2021	John Bingham	V4.0	Cover page updated Review date remove Minor text changes GDPR – UK GDPR Additional policy added to part 4 related policies to include: 6.10 introduces appropriate policy document which has been added as appendix 2 Small changes made to 11.2 and 15.3

Contents

1. Policy Statement

1.1 The Chief Executive, Directors and management of West Lindsey District Council ("the Council"), located at The Guildhall, Marshall's Yard, Gainsborough, DN21 2NA are committed to complying with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information the Council collects in accordance with the Data Protection Act (DPA) and the UK General Data Protection Regulation (UK GDPR).

1.2 Compliance with the UK GDPR is described by this policy and other relevant policies such as the Information Security Policy along with connected processes and procedures.

1.3 To that end, the Board has developed, implemented, maintains and continuously improves a documented Personal Information Management System (PIMS) for the Council.

2. Scope

2.1 **Material Scope** (UK GDPR Article 2). The UK GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

2.2 **Territorial Scope** (UK GDPR Article 3). The UK GDPR applies to all controllers that are established in the European Union (EU) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

2.3 This Policy applies to all full time and part time employees of the Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers, and students or trainees on placement with the Council. Any breach of the DPA, UK GDPR or this PIMS will be dealt with under the Council's disciplinary policy and may also be a criminal offence in which case the matter will be reported as soon as possible to the appropriate authorities.

2.4 Partners and any third parties working with or for the Council, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Council without having first entered into a data confidentiality agreement. The agreement must be legally enforceable, must impose on the third party obligations no less onerous than those to which the Council is committed, and must give the Council the right to audit compliance with the agreement.

2.5 Elected members are also data controllers in their own right and must make sure that any personal information they hold/use in their office as elected member is treated in line with the DPA and UK GDPR.

2.6 This Policy applies to all personal information created or held by the Council, in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, Intranet, shared and personal network drives, email, mobile devices, removable media, filing cabinet, shelving and personal filing drawers).

2.7 The DPA does not apply to access to information about deceased individuals.

2.8 In order to work efficiently, the Council has to collect and use information about people with whom it works. This may include members of the public, employees (including past and prospective), elected members, clients, customers, and suppliers. We may also be required by law to collect and use information to meet the requirements of central government.

3. Objectives of the PIMS

3.1 The objectives of the PIMS are that it should enable the Council to meet its own requirements for the management of personal information; that it should support organisational objectives and obligations; that it should impose controls in line with the Council's acceptable level of risk; that it should ensure that the Council meets applicable statutory, regulatory, contractual and/or professional duties; and that it should protect the interests of individuals and other key stakeholders.

3.2 The Council is committed to complying with data protection legislation and good practice including:

a. processing personal information only where this is strictly necessary for legitimate organisational purposes;
b. collecting only the minimum personal information required for these purposes and not processing excessive personal information;
c. providing clear information to individuals about how their personal information will be used and by whom;
d. only processing relevant and adequate personal information;
e. processing personal information fairly and lawfully;
f. maintaining an inventory of the categories of personal information processed by the Council;
g. keeping personal information accurate and, where necessary, up to date;
h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
i. respecting individuals' rights in relation to their personal information, including their right of subject access;

j. keeping all personal information secure;
k. only transferring personal information outside the EU in circumstances where it can be adequately protected;
l. the application of the various exemptions allowable by data protection legislation;
m. developing and implementing a PIMS to enable the policy to be implemented;
n. where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the Council's PIMS; and
o. identifying staff with specific responsibility and accountability for the PIMS.

4. Related Policies

4.1 This Policy should be read in conjunction with:

- Appropriate Policy Document (Appendix 2)
- Legal Responsibilities Policy;
- Information Management and Protection Policy;
- Information Security Policy;
- Freedom of Information and Environmental Information Policy;
- Records Management Policy;
- Information Sharing Policy;
- Data Quality Policy; and
- Data Breach Reporting Policy and Procedure.

5. Notification

5.1 The Council (Registration No. Z5460805) has notified the Information Commissioner's Office (ICO) that it is a data controller and that it processes certain information about data subjects. The Council has identified and documented all the personal data that it processes in the Information Asset Register (IAR).

5.2 A copy of the ICO notification details is retained by the Data Protection Officer (DPO) in the Article 30 Record of Processing Activities (ROPA).

5.3 The ICO notification is renewed annually on 1 September.

5.4 The DPO is responsible, each year, for reviewing the details of notification, in the light of any changes to the Council's activities (as determined by changes in the IAR and management reviews) and to any additional requirements identified by means of data protection impact assessments.

6. Responsibilities

6.1 The ICO is the UK's established Supervisory Authority as specified in UK GDPR Article 51. The ICO is responsible for monitoring the application of the UK GDPR in order to protect the rights and freedoms of natural persons in relation to processing and to facilitate the free flow of data within the Union.

6.2 West Lindsey District Council is a data controller under the DPA and the UK GDPR (defined in Article 4).

6.3 The Chief Executive and Directors are responsible for ensuring compliance with the DPA, the UK GDPR and this Policy within their directorates.

6.4 Directors, and Team Managers are responsible for ensuring that the business areas they have responsibility for have processes and procedures in places that comply with the DPA, the UK GDPR and this Policy. Directors, and Team Managers are responsible for ensuring that data cannot be accessed by unauthorised personnel and to make sure that data cannot be tampered with, lost or damaged.

6.5 The Council has appointed a DPO who is accountable to the Board for the management of personal information within the Council and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the PIMS as required by this policy; and
- security and risk management in relation to compliance with the policy.

6.6 The Council is required under UK GDPR Article 30 to maintain a Record of Processing Activities (ROPA) and make this available to the Supervisory Authority (the ICO) on request. The DPO is responsible for reviewing the ROPA annually in the light of any changes to the Council's activities (as determined by changes to the IAR and management reviews) and to any additional requirements identified by means of data protection impact assessments.

6.7 The responsibility for providing day-to-day advice and guidance to support the Council in complying with the DPA, the UK GDPR and this Policy rests with the DPO.

6.8 Responsibility for administering Data Subject Access Requests (DSARs) is delegated to FOI/Admin Officer, Member and Support Services.

6.9 All members of staff, contractors and elected members who hold or collect personal data are personally responsible for their own compliance with the DPA and UK GDPR and must make sure that personal information is kept and processed in-line with data protection legislation

and good practice. Failure to do so may result in disciplinary action that could lead to dismissal.

6.10 Any processing of the special categories of personal data must comply with the DPA and UK GDPR (Article 9). The Council has published an Appropriate Policy Document to meet the requirements of the DPA Schedule 1. The Policy details the safeguards we have put in place when we process special category data, criminal conviction data, and sensitive data for law enforcement purposes and has been included in this document at Appendix 2.

6.11 If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data for the Council or if they will do so as part of the services they are providing to the Council, the lead Council officer must make sure that personal data is kept in line with the principles of the DPA and the UK GDPR. This requirement should be outlined in any contract the contractor enters into with the Council. A data confidentiality agreement must be in place before any work commences. The Council promotes information sharing where it is in the best interests of the data subject. The Council has data sharing protocols in place and will keep to the standards set out in these protocols. Where appropriate, the Council's DPO will make sure, when personal information is shared, it is done properly, legally and ethically.

7. Background to the UK GDPR

7.1 The General Data Protection Regulation replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

7.2 **The Six Guiding Principles of the UK GDPR**

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

The Council must be able to demonstrate compliance with these principles. This is **accountability** and can be considered as a "seventh" principle.

7.3 **Key Changes introduces by UK GDPR**

- ✓ Increased territorial scope
- ✓ Enhanced data inventory requirements

- ✓ Increased penalties for non-compliance
- ✓ Appointment of a Data Protection Officer
- ✓ Broader obligations for Data Controllers
- ✓ Direct obligations for Data Processors
- ✓ More timely data breach reporting
- ✓ Right to data portability
- ✓ Right to erasure ("right to be forgotten")
- ✓ Stronger requirements for data subject consent

7.4 **Lawful Bases for Processing Personal Data**

For processing of personal data to be lawful under the UK GDPR, a legal basis from UK GDPR Article 6 must be identified and documented.

Processing special category data is prohibited unless a legal basis from UK GDPR Article 6 and a condition from UK GDPR Article 9 have been identified and documented.

7.5 **Definitions used in the UK GDPR**

A list of definitions used in the UK GDPR is included at Appendix 1.

8. Risk Assessment

8.1 It is essential that the Council is aware of any risks associated with the processing of particular types of personal information.

8.2 The Council has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of the Council. The Council shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

8.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, the Council shall, **prior to the processing**, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

8.4 A single assessment may address a set of similar processing operations that present similar high risks.

8.5 Where, as a result of a Data Protection Impact Assessment (DPIA), it is clear that the Council is about to start processing of personal information that could cause damage and/or distress to the data subjects, the Data Protection Officer must escalate the assessment to the Senior Information Risk Owner (SIRO) for review. If there are significant concerns, either as to the potential damage or distress, or the quantity of

data concerned, escalate the matter to the Information Commissioner's Office (ICO) who is the UK's Supervisory Authority.

8.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the Council's documented risk acceptance criteria and the requirements of the UK GDPR.

9. Security of Data

9.1 All Employees/Staff are responsible for ensuring that any personal data which the Council holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Council to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the IT Access Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the IT Access Policy; and/or
- stored on (removable) computer media which are encrypted in line with the Encryption Policy (TBA)

Care must be taken to ensure that PC screens and terminals are not visible except to authorised personnel. All staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed to secure archiving or destroyed in accordance with the Retention and Disposal Schedule.

Personal data may only be deleted or disposed of in line with the Retention and Disposal Schedule. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by [TBA] before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

10. Rights of Data Subjects

10.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the UK GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO to assess whether any provision of the UK GDPR has been contravened.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- The right to object to any automated profiling without consent.

11. Right of Access to Data (Data Subject Access Requests)

11.1 Individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information that largely corresponds with the information that should be provided in a privacy notice.

This is called a Data Subject Access Request (DSAR) under the DPA and the UK GDPR and allows individuals to be aware of and verify the lawfulness of the processing.

11.2 The Council has a subject access process, which sets out procedures for access to personal data, and complies with the principles of the DPA and UK GDPR. Key points of the procedure are:

- The identity of the person making the request must be verified using "reasonable means".

- If the request is made electronically, then the information should be provided in a commonly used electronic format. Unless an alternate format is requested on receipt of the DSAR.
- A copy of the information must be provided **free of charge**.
- A **reasonable fee** based on administration costs may be charged:
  - When a request is manifestly unfounded or excessive, particularly if it is repetitive.
  - To comply with requests for further copies of the same information.
- When a request is manifestly unfounded or excessive, particularly if it is repetitive, the Council can choose to refuse the request. In this case the Council must explain, without undue delay and at the latest within one month, why to the individual, inform them of their right to complain to the ICO and to a judicial remedy.
- Information must be provided without delay and at the latest within one month of receipt.
- Where requests are complex and numerous periods of compliance can be extended by a further two months. Individuals must be informed of the reason for the extension within one month of the request being received.
- Where the Council processes large amounts of data about an individual it may ask the individual to specify the information that the request relates to.

11.3 Information may be withheld where the Council is not satisfied that the person asking for information about themselves is who they say they are. The Council may withhold information when the requester is an organisation or body where the Council is not satisfied that they have the right to receive that information. In these cases, the Council will refuse to provide the information until it receives all relevant requested documents.

12. Disclosure of personal information about third parties

12.1 Personal data must not be disclosed about a third party except in line with the DPA and the UK GDPR. If it appears necessary to disclose information about a third party to a person requesting data, advice must be sought from the Data Protection Officer.

13. Disclosure of personal information to third parties

13.1 The Council must make sure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees/staff should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not

disclosure of the information is relevant to, and necessary for, the conduct of the Council's business.

13.2 The DPA and the UK GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

13.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

14. Information Sharing

14.1 The Council may share information when it is in the best interest of the data subject and when, by not sharing data, vulnerable groups and individuals could be put at risk. This must be done in a secure and proper way. The Council will be transparent and open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards. The Council will simplify the legal framework governing data sharing, including rules to guarantee better and more guidance for staff.

15. Data Quality and Integrity

15.1 If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime, a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is preferable to avoid legal proceedings by working with the person to put right the data or allay their concerns.

15.2 Individuals can ask the Council to stop processing data. For example, if data is properly held for marketing purposes, an individual is entitled to ask that this is stopped as soon as possible. Requests must be made in writing but generally, all written or oral requests should be carried out as soon as they are made. The cessation must be confirmed in writing.

15.3 If data is held for any other purposes, an individual may request that processing that data be stopped if it is causing them unwarranted harm or distress. This does not apply if they have given their consent; if data is held about a contract with the person; if the Council is fulfilling a legal requirement; or if the person's vital interests are being protected. Valid written requests must be responded to in writing without undue delay and actioned within 1 calendar month.

16. Retention and Disposal of Data

16.1 The Council shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

16.2 The Council may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

16.3 The retention period for each category of personal data will be set out in the Retention and Disposal Schedule along with the criteria used to determine this period including any statutory obligations the Council has to retain the data.

16.4 The Council's Data Retention and Disposal Schedule will apply in all cases.

16.5 Personal data must be disposed of securely in accordance with the sixth principle of the UK GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure (TBA).

17. Data Transfers

17.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the UK GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

1. An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether

there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

Countries that are members of the EEA but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

2. Privacy Shield

If the Council wishes to transfer personal data from the EU to an organisation in the United States (for example, a US-based cloud service) it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The U.S. Department of Commerce is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

3. Assessment of adequacy by the data controller

In assessing adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred.
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

4. Model contract clauses

The Council may adopt approved model contract clauses for the transfer of data outside of the EEA. If the Council adopts the model contract clauses approved by the ICO there is an automatic recognition of adequacy.

5. Exceptions

In the absence of an adequacy decision, Privacy Shield membership, or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

18. Information Asset Register

18.1 The Council has established a data inventory (Information Asset Register (IAR)) and data flow process as part of its approach to address risks and opportunities throughout its UK GDPR compliance project. The Council's IAR and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

18.2 The Council is aware of any risks associated with the processing of particular types of personal data.

- The Council assesses the level of risk to individuals associated with the processing of their personal data. Data Protection Impact Assessments (DPIAs) are carried out, where required, in relation to the processing of personal data by the Council], and in relation to processing undertaken by other organisations on behalf of the Council.
- The Council shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.
- Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the Council shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
- Where, as a result of a DPIA it is clear that the Council is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not the Council may proceed must be escalated for review to the Data Protection Officer (DPO).
- The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.
- Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the Council's documented risk acceptance criteria and the requirements of the UK GDPR.

19. Complaints

19.1 Data Subjects who wish to complain to the Council about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer by:

1. Email dpo@west-lindsey.gov.uk
2. Tel 01427 676676
3. Using the Council's Complaint Procedure at http://www.west-lindsey.gov.uk/your-council/have-your-say/comments-compliments-and-complaints/

4. Data subjects may also complain directly to the Information Commissioner's Office and the Council provides contact details in the Council's Complaint Procedure at http://www.west-lindsey.gov.uk/your-council/have-your-say/comments-compliments-and-complaints/

19.2 Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Data Protection Officer. The right to do this is explained in the Council's Complaints Procedure can be found at http://www.west-lindsey.gov.uk/your-council/have-your-say/comments-compliments-and-complaints/

20. Exemptions

20.1 Under Part 4 of the DPA, it is sometimes necessary to withhold certain information that has been requested by individuals. The Data Protection Officer can offer advice in these circumstances.

21. Breach of the Policy

21.1 Any breach of this Policy must be investigated in line with the Data Breach Reporting Policy and Procedure.

21.2 In line with the Data Breach Reporting Policy and Procedure, the Council will always treat any data breach as a serious issue that could result in a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances in line with the employee code of conduct or, in the case of elected members, the Members' Code of Contact.

Appendix 1 - List of Abbreviations and Definitions used in this Document

Abbreviations used in this Document

Abbreviation	Description
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSAR	Data Subject Access Request
EEA	European Economic Area
EU	European Union
UK GDPR	General Data Protection Regulation
IAR	Information Asset Register
ICO	Information Commissioner's Office
PIMS	Person Information Management System
ROPA	Record of Processing Activities
SIRO	Senior Information Risk Owner

Definitions used in the UK GDPR

Establishment	The main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data	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.
Data Controller	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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Subject	Any living individual who is the subject of personal data held by an organisation.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
Personal data breach	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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Child	The UK GDPR defines a child as anyone under the age of 16 years old, although this is likely to be lowered to 13 by The Data Protection Bill. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Relevant Filing system	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Appendix 2 – Appropriate Policy Document - Linked

https://itshared.sharepoint.com/:w:/r/sites/Minerva/CorpDocs/_layouts/15/Doc.aspx?sourcedoc=%7B6BA41AD2-3ADF-4096-A90F-B5C5187CACE9%7D&file=Appropriate%20Policy%20Document.docx&action=default&mobileredirect=true&DefaultItemOpen=1