West Lindsey DISTRICT COUNCIL The Entrepreneurial Council

Information Governance Policy

Data Protection Policy

JSCC Approved :
CP&R Approved:

Version Number	3.0
Approved by	
Date approved	
Review Date	
Authorised by	Director of Resources
Contact Officer	Information Governance Officer

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
16/2/2012	Steve Anderson	Draft V0.3	Formally adopted by Policy & Resources Committee
15/8/2013	Corporate Information Governance Group	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	Carolyn Lancaster	V1.1	Review – no amendments req'd
6/10/2015	Carolyn Lancaster	V2.0	Change Service Managers to Team Managers in para 5.3
23/11/2016	Corporate Information Governance Group	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.

Contents

1. Policy Statement

1.1 Information is the lifeblood of West Lindsey District Council (the Council). Without it, our jobs would be impossible to do.

1.2 To work efficiently, we must collect and use information about people with whom we work. 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.

1.3 All personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means. We all have a responsibility for its safe handling.

1.4 This document sets out the principles of data protection; our responsibilities; the access rights of individuals; information sharing; and how we shall deal with complaints. The Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 (DPA).

2. Scope

2.1 This Policy applies to all full time and part time employees of West Lindsey District Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers, and students or trainees on placement with the Council.

2.2 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 Data Protection Act 1998.

2.3 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).

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

2.5 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. The Principles of Data Protection

3.1 The DPA stipulates that anyone processing personal data must apply the eight principles of good practice. These principles are legally enforceable.

3.2 Schedule 1 to the DPA lists the principles fully. In summary, the principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;

2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

4. Shall be accurate and, where necessary, kept up to date;

5. Shall not be kept for longer than is necessary for that purpose or those purposes;

6. Shall be processed in accordance with the rights of data subjects under the DPA;

7. Shall be kept secure i.e. protected by an appropriate degree of security;

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

3.3 The DPA provides rules for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data (see glossary for definitions). Sensitive personal data requires stricter processing rules.

4. Responsibilities

4.1 West Lindsey District Council is a data controller under the Data Protection Act 1998.

4.2 The role of Data Protection Officer is held by the Council's Monitoring Officer.

4.3 Directors are responsible for ensuring compliance with the DPA and this Policy within their directorates.

4.4 Directors, Strategic Leads, 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 and this Policy. Directors, Strategic Leads, 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.

4.5 The responsibility for providing day-to-day advice and guidance to support the Council in complying with the DPA and this Policy rests with the Data Protection Officer. Responsibility for the Data Protection Policy and communicating this to staff is delegated to the Information Governance Officer. Responsibility for administration tasks such as dealing with Subject Access Requests is delegated to the Team Manager, Customer Strategy and Services.

4.6 All members of staff or contractors and elected members who hold or collect personal data are personally responsible for their own compliance with the DPA and must make sure that personal information is kept and processed in-line with the DPA. Failure to do so may result in disciplinary action that could lead to dismissal.

4.7 Any processing of sensitive personal data must comply with the principles set out in the DPA.

5. Related Policies

5.1 This Policy should be read in conjunction with:

- Legal Responsibilities Policy;
- Information Management and Protection Policy;
- Information Security Policy;
- Freedom of Information and Environmental Information Policy;
- Information Sharing Policy;
- Data Quality Policy; and
- Data Protection Breach Policy.

6. Agents, Partner Organisations and Contractors

6.1 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. This requirement should be outlined in any contract the contractor enters into with the Council. A data confidentiality agreement should normally 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 Data Protection Officer will make sure, when personal information is shared, it is done properly, legally and ethically.

7. Access Rights by Individuals (Subject Access Requests)

7.1 An individual may ask for a copy of any data held about them, or information about the reasons it is kept and processed. This is called a Subject Access Request under the DPA. The Council has a subject access process, which sets out procedures for access to personal data, and complies with the principles of the DPA. Information that may be disclosed should be provided in clearly understandable terms within 40 calendar days of receipt of a valid written request, proof of the individual's identity and payment of a £10 fee.

7.2 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.

8. Disclosure of personal information about third parties

8.1 Personal data must not be disclosed about a third party except in line with the DPA. 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.

9. Information Sharing

9.1 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.

10. Data Quality, Integrity and Retention

10.1 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.

10.2 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.

10.3 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 within 21 days.

11. Complaints

11.1 An individual has the right to complain about the response they have received regarding their request for information as well as to complain about other breaches of the DPA. Details of the Council's Complaints Procedure can be found at http://www.west-lindsey.gov.uk/your-council/have-your-say/comments-compliments-and-complaints/

12. Exemptions

12.1 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.

13. Notification

13.1 The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which West Lindsey District Council is registered.

13.2 The Data Protection Officer will review and update the Data Protection Register annually before notifying the Information Commissioner. Staff and elected members should notify the Data Protection Officer of any changes to the processing of personal data between the annual reviews.

14. Breach of the Policy

14.1 Any breach of this Policy must be investigated in line with the Data Protection Breach Policy and associated procedures.

14.2 In line with the Data Protection Breach Policy, 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.

15. Review of the Policy

15.1 This Policy shall be reviewed every 2 years.

16. Abbreviations

Abbreviation	**Description**
DPA	Data Protection Act 1998
EIR	Environmental Information Regulations 2004
FoIA	Freedom of Information Act 2000

17. Glossary

Data Controller	A data controller is the "person" recognised in law (i.e. an individual; organisation; or other corporate and unincorporated body of persons) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Subject	The individual who the data or information is about
Information Commissioner	The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Notified Purposes	The purposes for which the Council is entitled to process that data under its notification with the Information Commissioner's Office.
Personal Data	Defined in s(1) of the DPA, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (the Council is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing.
Processed fairly and lawfully	Data must be processed in accordance with the 3 provisions of the DPA. These are the data protection principles, the rights of the individual and notification.
Sensitive Data	Information about racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.
Subject Access Request	An individual's request for personal data under the Data Protection Act 1998.