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

Data Protection Policy

Document Control

Organisation	East Lindsey District Council
Title	Data Protection Policy
Author	Samantha Stocks
Protective Marking	Not Protected
Review Date	March 2015

Revision History

Revision Date	Reviser	Previous Version	Description of Revision

Introduction

The Data Protection Act 1998 (the Act) regulates the processing of information relating to living individuals. Processing includes obtaining, holding, using and disclosing such information. The Act applies to electronic records and manual records.

As a Council we are bound by the requirements of the Act and are fully committed to complying with it. This Policy ensures that all employees, elected members, temporary and / or agency workers, contractors, agents, consultants, partners and any other person who has access to any personal data held by, or held on behalf of, the Council, are fully aware of and abide by their duties and responsibilities under the Act.

We collect and use certain types of information about people with whom we deal with in order to carry out our day to day functions. These may include members of the public, current, past and prospective employees, clients, customer and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly whether it is on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as essential to the success of our functions and to maintaining confidence between us and those with whom we carry out business.

Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with eight principles of good practice that are legally enforceable.

Principle 1

- Personal information shall be processed fairly and lawfully and in particular shall not be processed unless specific conditions are met.

Principle 2

- Personal information 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.

Principle 3

- Personal information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed

Principle 4

- Personal Information shall be accurate and where necessary, kept up-to-date

Principle 5

- Personal information shall not be kept for longer than is necessary for that purpose or those purposes

Principle 6

- Personal Information shall be processed in accordance with the rights of data subjects under the Act

Principle 7

- Personal information shall be kept secure i.e. protected by an appropriate degree of security

Principle 8

- Personal information shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures a high level of data protection.

Personal Data

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from:-

- that data; or
- that data and other information which is in the possession of, or is likely to come into the possession of, the data controller[1] and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect if the individual.

[1] A person or organisation who (either alone or with other persons) determines the purpose and manner in which any personal data is processed, such as East Lindsey District Council

Sensitive personal data is defined as personal data which consists of information about:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical and mental health or condition
- sexual life; and
- criminal proceedings or convictions

Handling of personal data and sensitive personal data

We will, through appropriate management and the use of strict criteria and controls, ensure that we fully observe conditions regarding the collection and use of personal information.

All staff, as part of their conditions of employment, will abide by this policy and follow good data protection practice.

When we engage with third parties (individuals and organisations) we will expect them to abide by the Act. We will not enter into any contract, agreement or undertaking that will compromise our role as a Data Controller.

We will ensure that we meet our legal obligation to specify the purposes for which information is used and ensure that our entry on the public register of data controllers includes these purposes.

We will collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

When information is collected, on forms or by other methods, specific information will be supplied about the purpose for which the information is being gathered and the use that will be made of it.

Personal information will not be held for longer than usefully required and we will ensure that any information held is factually relevant to the area of work concerned.

Personal information will be destroyed securely once the appropriate retention period has elapsed.

We will take appropriate technical and organisational security measures to safeguard personal information and ensure access is restricted to only those individuals who require it to carry out their role.

Personal information will not be transferred abroad without suitable safeguards.

Responding to Requests

We have set out clear procedures for responding to requests for information under the Act to ensure that the rights of people about whom information is held can be fully exercised under the Act. These include the right to be informed that processing is being undertaken and for what purpose, the right of access to personal information within the statutory 40 calendar days, the right to prevent processing in certain circumstances and the right to correct, rectify, block or delete incorrect information.

Breaches and Offences

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

An accidental breach can also constitute an offence under the Act which could lead to 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.

Any **potential** breaches should be notified to the IGO immediately by completing the DPA Breach Notification Form which is available on the Intranet. The IGO will keep a log of all potential breaches and will, in liaison with the SIRO and Service Area Team Leader, decide on the most appropriate next course of action.

The ICO will be notified of all serious data breaches in line with published guidance - 'Notification of data security breaches to the Information Commissioner's Office (ICO)' The IGO will be responsible for notifying the ICO and assisting the ICO in any investigations.

Storage and security of personal data

All appropriate steps will be taken to ensure that personal data is kept secure at all times against unauthorised or unlawful loss 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.

- 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.

Data processing on behalf of the Council

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.

Where appropriate we will enter into a written Data Processing agreement setting out more fully the terms under which we require our data to be processed.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. This register shows what an organisation or individual has declared that they use personal information for. East Lindsey District Council is currently registered along with the Electoral Registration Officer.

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.

Information Sharing

Where we determine that there is a legitimate reason for sharing information in accordance with Schedule 2 and / or Schedule 3 of the Act, this will be undertaken using one of the following methods:-

- Ensuring that there is an information sharing agreement in place with the organisation
- 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.

Roles and Responsibility

The Senior Information Risk Officer for the Council will provide dedicated oversight for information governance and risk issues.

The Information Governance Officer (IGO) is the person who has specific responsibility for data protection within the Council but it is not the responsibility of the Information Governance Officer 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.

Enquiries about handling personal information, whether by a member of the public or a member of staff should be directed to the Information Governance Officer for advice and assistance.

A regular review and audit will be made of the way personal information is managed.