www.emmausfederation.co.uk

DATA PROTECTION POLICY

Date: 12th December 2014

Contents

1. Aim

1.1. The aim of this policy is to ensure Lincolnshire County Council (the Council) is compliant with the Data Protection Act 1998 (the Act).

1.2. It supports the Council's aim in demonstrating commitment to the Act.

2. Introduction

2.1. The Data Protection Act 1998 aims to protect all personal data which is collected, processed, stored and disposed of by an organisation.

2.2. The Council has a statutory duty to comply with the requirements of the Act as it collects personal data when conducting its business.

2.3. The Information Commissioner's Office (ICO) is responsible for regulating and enforcing the Act.

3. Scope

3.1. This policy shall apply to all elected members, Council employees, and any person handling data on behalf of the Council including consultants, volunteers, contractors and suppliers.

4. Definitions

4.1. The following definitions shall apply (as defined by the Act):

4.2. **Data** means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, i.e. highly structured readily accessible paper filing system.

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record i.e. health, education, housing and social services records; or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

4.3. **Personal data** means information which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.4. **Sensitive Personal Data** means personal data consisting of information as to:

4.4.1. the racial or ethnic origin of the data subject,

4.4.2. his/her political opinions,

4.4.3. his/her religious beliefs or other beliefs of a similar nature,

4.4.4. whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

4.4.5. his/her physical or mental health or condition,

4.4.6. his/her sexual life,

4.4.7. the commission or alleged commission by him/her of any offence, or

4.4.8. any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

4.5. **Processing,** in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data

4.6. **Data subject** means an individual who is the subject of personal data.

4.7. **Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data controller may also act jointly with another organisation to process personal data,.

4.8. **Data processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

5. The Eight Data Protection Principles

5.1. The Council, and therefore any person who handles personal data on behalf of the Council, shall adhere to the eight principles of the Data Protection Act 1998, which are:

5.1.1. Personal Data shall be processed fairly and lawfully;

5.1.2. Personal Data shall be obtained for a specified and lawful purpose and not processed in a manner incompatible with that purpose;

5.1.3. Personal Data shall be adequate, relevant and not excessive for the purpose;

5.1.4. Personal Data shall be accurate and, where necessary kept up to date;

5.1.5. Personal Data shall not be kept longer than necessary;

5.1.6. Personal Data shall be processed in accordance with the rights of the data subject;

5.1.7. Appropriate technical and organisational measures shall be taken against unauthorised/unlawful processing of personal data and accidental loss, destruction or damage of personal data;

5.1.8. Personal Data shall not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6. Council Responsibilities

6.1. The Council shall ensure that:

6.1.1. It is a registered Data Controller. The registration number for the council is **Z8397628.**

6.1.2. It has a Data Protection Officer with specific responsibility for ensuring compliance with the Data Protection Act;

6.1.3. Individuals processing personal information understand that they are responsible for complying with the data protection principles;

6.1.4. Individuals processing personal information are appropriately trained to do so;

6.1.5. Individuals processing personal information are appropriately supervised;

6.1.6. Individuals with enquiries about handling personal information know who to ask;

6.1.7. Enquiries about handling personal information are dealt with promptly and courteously;

7. Roles

7.1. The following roles shall be in place:

7.1.1. The Council's Chief Information Officer (CIO) shall be responsible for ensuring everyone handling personal data complies with the Act.

7.1.2. The Information Governance Team shall be responsible for ensuring everyone handling personal data receives adequate Data Protection training and support.

7.1.3. The Information Security Board shall provide advice and guidance to the Council regarding the security of personal data.

8. Privacy Notice

8.1. The Council shall ensure that a privacy notice is published on the Council website – "How we use your information".

8.2. It shall explain in general terms the purpose or purposes for which the Council will process the data collected.

8.3. It shall explain where we keep information and why we hold it.

8.4. It shall explain who we share personal data with.

8.5. It shall provide contact details of relevant staff to allow requests for further information.

8.6. In certain circumstances it shall be necessary for Departments to provide additional information, to that described, within their own privacy notice, for example when and where you might share personal data with others.

8.7. A copy of the privacy notice shall be provided on request.

8.8. Members shall rely on the Council's privacy notice when acting on behalf of the Council.

9. Data Subjects

9.1. The Council shall ensure individuals (data subjects) have the right to access their personal data held by the Council (subject to exemptions). The process to be followed shall be set out in a Subject Access Request procedure.

9.2. The Council shall ensure that personal data is accurate (where reasonably possible) and shall investigate any complaint that relates to data accuracy.

9.3. The Council shall ensure that any objection to the processing of an individual's personal data is investigated.

9.4. The Council shall not process personal data about an individual for direct marketing purposes, when the individual has specified he/she does not want direct marketing, e.g. sending unsolicited mail.

9.5. The Council shall investigate complaints received regarding how it processes personal data. Complaints shall be referred to the Council's complaints procedure in the first instance.

10. Privacy Impact Assessment (PIA)

10.1. The Council shall endeavour to complete a Privacy Impact Assessment at the early stages of a project to assist in identifying risks to the individual(s) and the Council.

10.2. Project Managers shall consult with the Information Governance Team at an early stage to identify PIA requirements.

11. Data Security

11.1. The Council shall ensure it has policies and procedures in place to support the secure processing of personal data. Further guidance is available in the Council's Information Security Policy Framework.

11.2. The policies and procedures shall be made available on the Council Intranet and where appropriate the Council external website.

11.3. The Council shall ensure it has effective security controls in place to assist in the prevention of inappropriate disclosure or loss of personal data.

11.4. Access to personal data shall be strictly controlled.

11.5. The Council shall investigate all breaches of security which involve personal data.

11.6. Individuals shall report actual or potential breaches of security involving personal data to the Information Governance Team as soon as is practicable.

12. Training & Awareness

12.1. The Council shall provide mandatory basic Data Protection training to all Staff handling personal data.

12.2. Individuals shall maintain a good awareness of Data Protection.

12.3. Additional training shall be provided for staff working in specialist roles.

12.4. The Information Governance Team shall provide support and guidance to any person handling personal data on behalf of the Council.

13. Information Sharing

13.1. The Council shall ensure that information is shared only when it is within the provisions of the Data Protection Act 1998.

13.2. The Council shall ensure that when information is shared it is justified.

13.3. The Council shall ensure that adequate security is in place to protect the data when it is shared with another organisation including the process for secure deletion.

13.4. The Council shall ensure that arrangements are in place to provide individuals with access to their personal data.

13.5. The Council shall ensure common retention periods for the data are established.

13.6. The Council shall ensure the secure transfer of personal data between itself and other organisations.

13.7. The Council shall ensure that information sharing protocols exist between the Council and partnership agencies such as the Police, the NHS and voluntary organisations.

13.8. Employees shall refer to these protocols when considering whether to disclose personal data.

13.9. Advice shall be sought from the Information Governance team prior to sharing personal data with another organisation.

14. Contracts

14.1. Contracts shall include measures to ensure personal data is handled in accordance with the eight principles of the Data Protection Act.

14.2. Personal data shall only be supplied for the agreed purposes as set out in the contract, and shall not be used or disclosed for any other reason.

14.3. The Council shall ensure that before personal data is shared with a third party as part of a contract appropriate security controls are in place.