Lincolnshire Parent Carer Council

Registered Charity No: 1141060

Data Protection Policy

Purpose:

Lincolnshire Parent Carer Council must ensure all information is processed in accordance with the Data Protection Act 1998. This policy explains how staff and volunteers are expected to comply with the Act.

Procedure:

Staff must comply with this policy to ensure the Data Protection Act is not breached. Any breach of the Act has serious consequences for the organisation and its customers.

Introduction:

The Data Protection Act 1998 (the Act) aims to protect all personal data which is collected, processed, stored and disposed of by an organisation. Personal data is information about a living, identifiable person. The Act applies to data in paper and electronic format.

Lincolnshire Parent Carer Council (LPCC) has a statutory duty to comply with the requirements of the Act as it collects data about individuals when conducting its business. The Information Commissioner's Office (ICO) is responsible for regulating and enforcing the Act. The ICO is an independent authority which has legal powers to ensure organisations comply with the Act.

Policy Statement

LPCC is committed to ensuring compliance with the Act, and will:

- Respect the rights of each individual
- Be open and honest about the personal data it holds

- Provide training and support to those handling personal data in the course of their duties
- Notify the ICO that it processes personal data. This is a statutory requirement and notification must be submitted annually. Notification must be kept up to date with any changes to the use of personal data being updated within 28 days.
- Inform the ICO of breaches of the Act (where required)

Scope

This policy applies to all staff and volunteers.. Everyone handling personal data must understand and comply with the principles of the Data Protection Act.

Definitions

Personal data is information which relates to a living individual who can be identified

A data subject is an identifiable living individual

A data controller is a person who determines the purposes for which data are to be processed and the manner in which that data are processed. A data controller may also process data on behalf of another. LPCC is a data controller.

Data protection principles

The Act states that anyone who processes personal data must comply with eight principles,

Processing personal data fairly and lawfully

1. Personal Data shall be processed fairly and lawfully. In practise this means that LPCC:-
    - must have legitimate grounds for collecting and using the personal data;
    - must not use the data in ways that have unjustified adverse effects on the individuals concerned;
    - must be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

- Must handle people's personal data only in ways they would reasonable expect;
- Must make sure we do not do anything unlawful with the data.

Processing personal data for specified purposes

2. Personal data 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 other purposes. In practice, this means that LPCC:-
    - Must be clear from the outset about why we are collecting personal data and what we intend to do with it;
    - Must comply with the Acts fair processing requirements- including the duty to give privacy notices to individuals when collecting their personal data;
    - Must comply with what the Act says about notifying the Information Commissioner and
    - Must ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair;

Information Standards –the amount of personal data you may hold

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. In practice it means that LPCC should ensure that;
    - We hold personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual; and
    - We do not hold more information than we need for that purpose.

Information Standards – keeping personal data accurate and up to date

4. Personal data shall be accurate and, where necessary, kept up to date. To comply with these provisions LPCC must:-

- Take reasonable steps to ensure the accuracy of any personal data you obtain;
- Ensure that the source of any personal data is clear
- Carefully consider any challenges to the accuracy of information; and
- Consider whether it is necessary to update the information.

Information Standards – retaining personal data

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purposes or those purposes. In practice it means that LPCC will:-
    - Review the length of time it keeps personal data;
    - Consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;
    - Securely delete information that is no longer needed for this purpose or these purposes; and
    - Update, archive or securely delete information if it goes out of date.

The Rights of individuals

6. Personal data shall be processed in accordance with the rights of data subjects under this Act. The rights of individuals it refers to are:
    - A right of access to a copy of the information comprised in their personal data;
    - A right to object to processing that is likely to cause or is causing damage or distress;
    - A right to prevent processing for direct marketing;
    - A right to object to decisions being taken by automated means;
    - A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
    - A right to claim compensation for damages caused by a breach of the Act.

Information Security

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data. In practice it means that LPCC will have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular LPCC will need to:
    - Design and organise security to fit the nature of the personal data you hold and the harm that may result from a security breach;
    - Be clear about who in the LPCC is responsible for ensuring information security;
    - Make sure we have the right physical and technical security, backed up by robust policies and procedures and reliable and well trained staff and volunteers; and
    - Be ready to respond to any breach of security swiftly and effectively.

Sending personal data outside the European Economic Area

8. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures that an adequate of protection for the rights and freedoms of data subjects in relation to the processing of personal data

The conditions for processing

The conditions for processing are set out in Schedules 2 and 3 to the Data protection Act . Unless a relevant exemption applies at least one of the following conditions must be met:

- The individual who the personal data is about has consented to the processing
- The processing is necessary;
  - in relation to a contract which the individual has entered into
  -because the individual has asked for something to be done so they can enter into a contract
- The process is necessary because of a legal obligation

- The process is necessary to protect the individuals 'vital interests' This condition only applies in matters of life or death.
- The process is necessary for administering justice, or for exercising statutory, governmental or other public functions
- The process is in accordance with the legitimate interests condition.

Information Sharing

When data is collected the Privacy Notice must clearly explain what data we expect to share, who it is likely to be shared with and in what circumstances. Sensitive personal data will only be disclosed with the informed consent of the data subject, and the signed consent form must be retained on the relevant case file. In some cases verbal consent may be given and this must be recorded accurately within the relevant case file.

Consent cannot be assumed by a non-response to a request for consent. There are circumstances in which personal data may be disclosed without obtaining the data subject's consent such as safeguarding the data subject or others, and to assist with the prevention and detection of crime. Wherever possible, express informed consent for sharing sensitive personal data will be sought from the data subject. Where this is not possible or contrary to the public interest, the LPCC will ensure that the sharing of data meets the relevant condition or exemptions from the non-disclosure provision contained within the Act.

Information Sharing protocols exist between the LPCC and partnership agencies in the Statutory and Voluntary sector. Staff and volunteers must refer to these protocols when considering whether to disclose personal data.

Confidentiality

The LPCC provides guidance during their induction process , and expects all staff and volunteers to comply with its policies on confidentiality. Personal data is provided in confidence and must be processed and used in accordance with the eight Data Protection principles and the LPCC's Privacy Notice. Wherever possible the data subject must be informed when we disclose data to a third party. Where LPCC has a statutory duty to provide information in

relation to a Police Investigation, or where an individual is at risk of harm, information may be disclosed without notifying from the data subject

Responsibilites

All LPCC staff and volunteers are responsible for ensuring everyone handling personal data complies with the Act. Please see our confidentiality policy with regard to keeping information confidential.

If there are any issues regarding data protection they should be reported the Chair or Vice chair as soon as reasonably possible.

Policy review date .... April 2014