

Listowel Family Resource Centre Ltd.

1. INTRODUCTION

Listowel Family Resource Centre is committed to a policy of protecting the rights and privacy of individuals in accordance with the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. For administrative purposes (e.g. to pay staff, to administer programmes, to record progress and to comply with legal obligations to funding bodies and government), the Centre needs to process personal data about its staff, volunteers and other individuals with whom it has dealings. To comply with the law, personal data must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

2. INDIVIDUAL RIGHTS

The individuals for whom the Centre stores personal data have the following rights:

- To have their personal data obtained and processed fairly, kept securely and not illegitimately disclosed to others;
- To be informed of the identity of the Data Controller and of the purpose for which the information is held;
- To get a copy of their personal data;
- To have their personal data corrected or deleted if inaccurate;
- To prevent their personal data from being used for certain purposes: e.g. blocked for research purposes;
- Under Employment Rights, not to be forced to disclose information to a prospective employer. No one can force another person to make an access request, or reveal the results of an access request, as a condition of recruitment, employment or provision of a service. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.

It should be noted that under the Freedom of Information Act (1997 and 2003) records containing personal information may be released to a third party, where the public interest so requires.

3. PRINCIPLES OF THE ACTS

The Centre will administer its responsibilities under the legislation in accordance with the eight stated data protection principles outlined in the Act as follows:

3.1 Obtain and process information fairly:

The Centre will obtain and process personal data fairly and in accordance with the fulfillment of its functions.

3.2 Keep data only for one or more specified, explicit and lawful purposes

The Centre will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

3.3 Use and disclose data only in ways compatible with these purposes

The Centre will only disclose personal data that is necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

3.4 Keep data safe and secure

The Centre will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The Centre is aware that high standards of security are essential for all personal data.

3.5 Keep data accurate, complete and up-to-date

The Centre will have procedures that are adequate to ensure high levels of data accuracy and will examine the general requirement to keep personal data up-to-date. Appropriate procedures will be put in place to assist staff in keeping data up-to-date.

3.6 Ensure that data are adequate, relevant and not excessive

Personal data held by the Centre will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.

3.7 Retain data for no longer than is necessary for the purpose or purposes or which they are kept

The Centre will implement procedures on retention periods for personal data. **(Appendix 2)**

3.8 Give a copy of his/her personal data to that individual, on request

The Centre will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

4. ROLES / RESPONSIBILITIES

Listowel Family Resource Centre has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees and volunteers of the Centre who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation. The Centre will provide support, assistance, advice and training as required in order to ensure that it is in full compliance with the legislation.

5. PROCEDURES AND GUIDELINES

This policy supports the provision of a structure to assist the Centre's compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

6. DATA BREACH

Where a disclosure or a breach of data occurs, the Centre should refer to the Data Protection Commissioners Personal Data Security Breach Code of Practice for guidance on dealing with such breaches or wrongful disclosures.

7. REVIEW

This Policy will be reviewed regularly in light of any legislative or other relevant indicators.

This Policy was discussed and ratified at meeting of the Voluntary Board of Directors dated:

Signed by the Chairperson: _____

Date: _____

Appendix 1: THE DATA PROTECTION RULES **Data Protection Acts, 1988 & 2003**

Transparency and informed consent - the touchstones of fairness in data protection.

You must ...

1. Obtain and process the information fairly

- a. At the time of providing personal information, individuals are made fully aware of:
 - i. the identity of the persons who are collecting it (though this may often be implied)
 - ii. to what use the information will be put
 - iii. the persons or category of persons to whom the information will be disclosed.
- b. Secondary or future uses, which might not be obvious to individuals, should be brought to their attention at the time of obtaining personal data
- c. If a data controller has information about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the information was collected), he or she is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

2. Keep it only for one or more specified and lawful purposes

- a. It is therefore unlawful to collect information about people routinely and indiscriminately, without having a sound, clear and legitimate purpose for so doing.

3. Process it only in ways compatible with the purposes for which it was given to you initially

- a. If you obtain personal information for a particular purpose, you may not use the data for any other purpose, and you may not divulge the personal data to a third party, except in ways that are "compatible" with the specified purpose.

4. Keep it safe and secure

- a. In determining what security measures should be put in place a number of factors may be taken into consideration;
 - i. The state of technological development - Measures must be reviewed over time.
 - ii. The cost of implementing the measures. - Larger organisations with greater resources can be expected to implement more advanced measures, or update measures more regularly, than smaller bodies.
 - iii. The harm that might result from unlawful processing. - Might someone be at a financial loss or be at risk of suffering injury as a result of disclosure or destruction of data?
 - iv. The nature of the data concerned. - There is a greater duty of care relating to the processing of sensitive personal data.

5. Keep it accurate and up-to-date

- a. *You must ensure that the personal information you keep is accurate and up-to-date.* You should be able to answer YES to the following questions:-

- i. Are your clerical and computer procedures adequate to ensure high levels of data accuracy?
- ii. Has the general requirement to keep personal data up-to-date been fully examined?
- iii. Have appropriate procedures been installed to ensure that each data item is kept up-to-date?

6. Ensure that it is adequate, relevant and not excessive

- a. The personal data you keep should be enough to enable you to achieve your purpose, and no more. You should be able to answer YES to the following questions:-
 - i. Is the personal information I hold really necessary for my business?
 - ii. Am I asking people to provide me with just the information I need, and no more?
 - iii. Do I have a good reason for asking people sensitive or personal questions?

7. Retain it no longer than is necessary for the specified purpose or purposes

- a. If there is no good reason for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future.
- b. If you would like to retain information about customers to help you provide a better service to them in the future, you must obtain the customers' consent in advance.

8. Give a copy of his/her personal data to any individual, on request.

- a. On making a written request to you any individual about whom you keep personal information on computer or in a relevant filing system is entitled to:
 - i. a copy of the data,
 - ii. a description of the purposes for which it is held,
 - iii. a description of those to whom the data may be disclosed and
 - iv. the source of the data unless this would be contrary to public interest
- b. An individual making an access request must:-
 - i. apply to you in writing,
 - ii. give any details which might be needed to help you identify him or her and locate all the information you may keep about him/her (e.g., previous addresses, customer account numbers).
 - iii. The individual must also pay you an access fee if you wish to charge one. You do not need to do so, but if you do it cannot exceed €6.35.