Data Protection Policy

1. Introduction

The Deafness Resource Centre Ltd (DRC) is committed to a policy of protecting the rights and privacy of individuals, the DRC needs to collect and use certain types of Data in order to carry out its work. This personal information must be collected and dealt with appropriately. The DRC is responsible for complying with the Data Protection Act 1998 and the new General Data Protection Regulation that will be introduced from 25th May 2018.

2.

3. Data Controller

DRC is the Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

4. Disclosure

DRC may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the DRC to disclose data (including sensitive data) without the data subject's consent. These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

DRC regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. DRC intends to ensure that personal information is treated lawfully and correctly.

To this end DRC will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulations (GDPR)

Personal Data and Sensitive Personal Data (now known as Special Categories of Personal Data) - under the Act data must be:

- Data – recorded information (electronically, manually or automatically)
- Personal – data is personal if it is concerned with identifiable, living individuals.

Specifically, the Principles require that personal information:

- shall be processed fairly and lawfully and in a transparent manner in relation to individuals
- collected for specific and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- shall be accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard for the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- shall not be transferred to a country or territory outside 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 information.

5.

DRC will, through appropriate management, strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information,
- meet its legal obligations to specify the purposes for which information is used,
- collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- ensure the quality of information used,
- ensure that the rights of people about whom information is held, can be fully exercised under the Act. These are:
    - Be informed – who is responsible for data protection in the organisation; why it's being collected; whether the information is shared and if so, with whom, how it is stored, for how long and how it's disposed of; the right to withdraw consent and the right to complain
    - Access to information - individuals have the right to access their information free of charge
    - Rectification – individuals can ask for their information to be rectified if incomplete or incorrect
    - Erasure - Individuals have the right to request their information be erased where there is no compelling reasons for its continued processing
    - Restrict processing - Individuals have a right to 'block' or suppress processing of personal data
    - Data portability - Individuals have the right to obtain and reuse their personal data
    - To object – Individuals can object to their data being used

- take appropriate technical and organisational security measures to safeguard personal information,
- ensure that personal information is not transferred abroad without suitable safeguards,
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- set out clear procedures for responding to requests for information.

6. <u>Data collection</u>

The Deafness Resource Centre collects and processes personal data on staff, volunteers, clients and contractual agents. In processing the data the DRC will clearly identify the lawful basis relied

upon to do so legitimately.

(a) Consent: the individual has given clear consent for the DRC to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract the DRC have with an individual, or because they have asked the DRC to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for the DRC to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for the DRC to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for DRC legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

7. Obtaining Information

DRC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, DRC will ensure that the Data Subject

- clearly understands why the information is needed and on what lawful basis personal data is processed
- understand that they have the right to refuse to their data being processed
- understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- grants explicit consent, either written or electronic for data to be processed
- is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- has received sufficient information on why their data is needed and how it will be used
- understands that they have the right to access their information (Subject Access Request) and the process for doing so.

8. Data Storage

Information and records relating to data subjects will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for as long as it is needed or required statute and will be disposed of appropriately in line with DRC Data Retention Policy.

It is DRC's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

9. Data access and accuracy

All Data Subjects have the right to access the information DRC holds about them. DRC will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, DRC will ensure that:

1. **it has a Data Protection Lead with specific responsibility for ensuring compliance with Data Protection,**
2. **everyone processing personal information understands that they are contractually responsible for following good data protection practice,**
3. **everyone processing personal information is appropriately trained to do so,**
4. **everyone processing personal information is appropriately supervised,**
5. **anybody wanting to make enquiries about handling personal information knows what to do,**
6. **it deals promptly and courteously with any enquiries about handling personal information,**
7. **it describes clearly how it handles personal information,**
8. **it will regularly review and audit the ways it holds, manages and uses personal information**
9. **it regularly assesses and evaluates its methods and performance in relation to handling personal information**
10. **all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them**

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations.

In case of any queries or questions in relation to this policy please contact the DRC Data Protection Lead (chief Officer). Further guidance can be obtained from www.ico.org.uk

10. The following list of definitions of the technical terms used is intended to aid understanding of this policy.

Data Controller – The person who (either alone or with others) decides what personal information the DRC will hold and how it will be held or used.

Data Protection Lead – The person(s) responsible for ensuring that it follows its data protection policy and complies with GDPR is the Chief Officer

Data Subject/Service User – The individual whose personal information is being held or processed by DRC (for example: a client, an employee, a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data

* See definition

General Data Protection Regulations– UK legislation introduced on 25th May 2018

Notification – Notifying the Information Commissioner about the data processing activities of DRC as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the GDPR Act 2010.

Processing – means collecting, amending, handling, storing or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g.

name and address. It does not apply to information about companies and agencies but applies to named persons or employees within the DRC.

11. Sensitive data – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings relating to a data subject's offences