**Data Handling & Confidentiality Policy**

**Purpose of policy**

To adhere to the guidelines of the Data Protection Act 2018 ( this is the UK -GDPR equivalent and has been ratified as satisfying all the necessary protections that the EU GDPR 2018 contains), to ensure that we handle information in a fair and lawful manner and with due regard for confidentiality. Our work brings us into contact with confidential information and we take every precaution to ensure that it is treated with due respect.

The Lizard CHILD Trust (LCT) holds information of staff, students, apprentices, volunteers, service users and learners on file for the purposes of record keeping, safeguarding and tracking the reach of our services. All information held by LCT is held with the written consent of the data subject and is held only as long as is necessary for processing or as defined by statutory regulations. Children’s information requires the consent of the parent or adult who has parental responsibility for the child and this consent is obtained as part of the enrolment process of children. The consent of the holder of parental responsibility should not be necessary in the context of Child Protection.

In order to maintain security and to prevent processing in infringement of this Act LCT evaluates the risks inherent in the processing and implements measures to mitigate those risks. Continuing analysis of risk factors ensures that measures are appropriate to minimise the risk of breach of confidentiality.

As a Data Controller it is the responsibility of LCT to ensure that any organisation that processes data on our behalf (e.g. that holds personal data on our clients for our use) adheres to the new regulations under the Data Protection Act 2018, and that we have a contract with these organisations that is compliant with this Act. Data Processors have a duty to ensure their systems are secure and comply with the Data Protection Act 2018.

**Duties**

Everyone responsible for using data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

* Used fairly and lawfully
* Used for limited, specifically stated purposes
* Used in a way that is adequate, relevant and not excessive
* Accurate
* Kept for no longer than is absolutely necessary
* Handled according to people’s data protection rights
* Kept safe and secure
* Not transferred to a third country or international organisation without adequate protection.

The Data Protection Act 2018 states that there is stronger legal protection for more sensitive information such as:

* Race
* Ethnic background
* Political opinions
* Religious beliefs
* Health
* Sexual health
* Criminal records
* Trade Union Membership
* Genetic and biometric data used for the purpose of uniquely identifying a natural person

There are separate safeguards for personal data relating to criminal convictions and offences.

Such information will be handled following the strict guidelines provided by the Act.

**Storage**

All Personal Records are kept under the same secure conditions. Hard copy storage of Personal records are kept in a non-portable lockable unit. Personal records are also kept as electronic files on password protected computer systems on site and on secure servers. They are only accessible to authorised personnel.

Reviewed March 2022