Data Protection Policy

Data Protection Procedure Diverse Little Colours (DLC) Last Updated: November 2023 Approved by Trustees: November 2023 Review Date: November 2023

Introduction and Scope Diverse Little Colours (DLC), the Data Controller needs to use certain types of personal information on, for example, the elderly residents, carers, and families of residents and others with whom it communicates. In addition, it may occasionally be required by statute to collect and use certain types of information to comply with the requirements of external bodies. This policy outlines DLC's commitment to data protection and compliance with the UK Data Protection Act. The purpose of this policy is to ensure that all personal data held by the CIC is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of DLC including trustees, staff, and volunteers.

Data Protection Lead DLC will appoint a Data Protection Lead who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities. If you have any queries please contact our Data Protection Lead: Name: Rajinder Sawhney Position: Director Contact: yogawithrajinder@gmail.com

DLC fully endorses and adheres to the seven principles of GDPR. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for DLC must adhere to these principles.

Data Protection Principles Data is:

Processed lawfully, fairly and in a transparent manner. There are several grounds on which data may be collected, including consent. We are clear that our collection of data is legitimate, and we have obtained consent to hold an individual’s data, where appropriate. We are open and honest about how and why we collect data and individuals have a right to access their data.

Collected for specified, explicit and legitimate purposes and not used for any other purpose. We are clear on what data we will collect and the purpose for which it will be used. Only collect data that we need. When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.

Adequate, relevant, and limited to what is necessary. We collect all the data we need to get the job done. And none that we don't need.

Accurate and, where necessary, kept up to date. We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up to date is, such as beneficiary, staff or volunteer records. We correct any mistakes promptly.

Kept for no longer than is necessary. We understand what data we need to retain, for how long and why. We only hold data only for as long as we need to. That includes both hard copy and electronic data. Some data must be kept for specific periods of time (e.g. accounting, H&SW). We have a process that ensures data no longer needed is destroyed.

Processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage. Data is held securely, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected. Data is kept safe. Our IT systems have adequate anti-virus and firewall protection that's up to date. Staff understand what they must and must not do to safeguard against cyberattack, and that passwords must be strong and not written down or shared. Data is recoverable. We have adequate data back-up and disaster recovery processes.

DLC shall be accountable for and be able to demonstrate compliance with the above points.

Maintaining Confidentiality DLC will treat all your personal information as private and confidential and not disclose any data about you to anyone other than the Trustees of DLC to facilitate the administration and day-to-day running of the project. All DLC staff and volunteers who have access to Personal Data will be required to agree to sign a Confidentiality Policy and a Data Protection Policy.

There are four exceptional circumstances to the above permitted by law:

Where we are legally compelled to do so. Where there is a duty to the public to disclose. Where disclosure is required to protect your interest. Where disclosure is made at your request or with your consent.

Use of Personal Information DLC will use your data for three main purposes:

The day-to-day administration of DLC. We work in liaison with relevant professionals and agencies outside the project to meet service user's specific needs. We will only share information if required by law. Contacting you to keep you informed of DLC activities and events and external activities that we think may be of interest to you. Statistical analysis; gaining a better understanding of DLC demographics. N.B. although

collated DLC data may be passed to a third party (funders), such as number of small groups or small group's attendance, no personal data will be disclosed.

Upshot Database Information contained on the database will not be used for any other purposes than set out in this section. The database is accessed through the cloud and therefore, can be accessed through any computer or smart device with internet access.

Access to the database is strictly controlled through the use of name specific passwords, which are selected by the individual. Those authorised to use the database only have access to their specific area of use within the database. This is controlled by the Data Controller and other specified administrators. These are the only people who can access and set these security parameters. People who will have secure and authorised access to the database include DLC Staff & data inputters (Mentors & Volunteers). The database will NOT be accessed by any authorised users outside of the UK, in accordance with the Data Protection Act, unless prior consent has been obtained from the individual whose data is to be viewed. All access and activity on the database is logged and can be viewed by the Database Controller. Subject Access - all individuals who are the subject of personal data held by DLC are entitled to: Subject Consent - The need to process data for normal purposes has been communicated to all data subjects. Ask what information DLC holds about them and why. Ask how to gain access to it. Be informed how to keep it up to date. Be informed what DLC is doing to comply with its obligations under the 1998 Data Protection Act. Personal information will not be passed onto any third parties outside of DLC.

Rights to Access Information Employees and other subjects of personal data held by DLC have the right to access any personal data that is being held in certain manual filing systems. This right is subject to certain exemptions. Personal Information may be withheld if the information relates to another individual. Any person who wishes to exercise this right should make the request in writing to the DLC Data Officer.. If personal details are inaccurate, they can be amended upon request. DLC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.