Liquorice Park Millennium Green Trust

Data Protection Policy

This Data Protection Policy sets out how Liquorice Park Millennium Green Park Trust (the **Trust**) will process Personal Data in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (**GDPR**).

Definitions

Data Subject	means the identifiable natural person about whom the data relates
Data Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction
Data Controller	means the Trust (charity number 1071634) whose contact address is 10 Carline Rd, Lincoln, LN1 1HG
Data Processor	means any natural or legal person (e.g. a volunteer with the Trust), public authority, agency or other body which processes Personal Data on behalf of the Trust
Legitimate Interest	means the interests of the Trust, individual interests or broader societal benefits. It cannot be assumed that the existence of a Legitimate Interest is always an appropriate reason to process Personal Data however it is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact
Personal Data	means any information relating to an identified or identifiable natural person (Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular in reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, genetic, economic, cultural or social identity of that natural person
Sensitive Personal Data	means personal information about an individual's race, ethnic origin, political affiliation or opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information and information concerning an individual's health, sex life or sexual orientation
Special Condition	means one of the following conditions for processing Sensitive Personal Data: (a) the Data Subject has given explicit consent; (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Trust or the Data Subject; (c) the processing is necessary to protect the Data Subject's vital interests and the Data Subject is physically incapable of giving consent;

(d) processing relates to Personal Data which is manifestly made public by the Data Subject;
(e) the processing is necessary for the establishment, exercise or defence of legal claims; or
(f) the processing is necessary for reasons of substantial public interest

SECTION 1 – Processing Personal Data

1.1 Collecting Personal Data

1.1.1 Personal Data must only be collected where there is a legitimate requirement to do so, and with the consent of the Data Subject. Care should be taken to ensure the accuracy of this data.

1.1.2 Data which is collected must be adequate, relevant and limited to what is necessary.

1.1.3 Where Personal Data is collected by a Data Processor on behalf of the Data Controller, it must be collected in accordance with this Data Protection Policy and it must be provided to the Data Controller upon request.

1.2 Bases for Processing Personal Data

1.2.1 Personal Data must only be processed where there is a lawful basis for processing. The lawful basis must be determined before processing data. Lawful bases are:

1.2.1(a) consent has been provided by the Data Subject, such consent must have been freely given, unambiguous and able to be evidenced;
1.2.1(b) the processing is necessary for the performance of a contract the Data Controller has with the Data Subject;
1.2.1(c) processing the Personal Data is necessary for the Data Controller to comply with the law;
1.2.1(d) processing the data is necessary to protect someone's life;
1.2.1(e) there is a Legitimate Interest in processing the Personal Data. The Legitimate Interest must be identified, it must be shown that processing is necessary to achieve it and it should be balanced against the Data Subject's rights and freedoms.

1.2.2 If the data is Sensitive Personal Data a Special Condition must also apply.

1.2.3 Where there is no lawful basis for processing, the data should not be processed.

1.3 Lawful Processing

For Personal Data to be lawfully processed, the conditions set out in paragraphs 1.1 and 1.2 above must have been met. In addition, only those who have a requirement to process Personal Data in order to fulfil their role should have access to it.

1.4 Integrity and Confidentiality

Any Personal Data that is collected either by or on behalf of the Data Controller is to be treated with confidentiality and only processed in line with this Data Protection Policy. Personal Data must not be shared, sold or rented to third parties for their own purposes. Any individual who

has been provided with the Personal Data by the Data Controller in order to perform their role as a volunteer, must also not use that Personal Data for their own purposes.

1.5 Data Minimisation

When processing of Personal Data has been completed, it may only be stored for the length of time stated in the Trust's Data Processing Schedule. Data that is not required must not be stored and must either be deleted, redacted or destroyed as appropriate.

SECTION 2 – Systems and Processes

2.1 Storing Personal Data

2.1.1 Personal Data must be stored securely at all times. Storage can be in either physical or electronic copies.

2.1.2 Where Personal Data is stored in physical format it must be in a location that is secure and prevents unauthorised access to the data. Storage of physical payment data (credit/debit card details or any other form of payment) must not take place.

2.1.3 Where Personal Data is stored in electronic format it must be on a device which is running up-to-date security software and which has a strong password. If the device is portable, it should not be left unattended without locking.

2.2 Transferring Personal Data

2.2.1 Transfer of data in physical format should be undertaken with care, ensuring that potential unauthorised access to the data is minimised. This means keeping it with you at all times and transporting the data so that it is covered and not visible (e.g. within a folder).

2.2.2 Transfer of data by email to more than one recipient must be sent using 'bcc' to ensure that personal email addresses are not disclosed.

2.3 Subject Access Requests

To ensure the Data Controller is able to respond to Subject Access Requests within 30 days of receipt, any Data Processors must provide any data requested to the Data Controller within 5 working days.

2.4 Breaches of this Policy

Any breach of this Policy must be reported immediately to the Chair of the trust (currently Philip Cragg)

V28.12.22

As amended by PRC