

Streets of Light Data Protection (GDPR) and Privacy Policy

Introduction

Streets of Light holds and processes personal data about living individuals for the purpose of creating and sharing the annual Streets of Light trail maps.

We are committed to complying with data protection law and the rights of individuals under it, as well as to the principles set out below. We recognise that this relates to all personal data, whether it is held on paper, on computer or other media.

All staff and volunteers who obtain, handle, process or store personal data for Streets of Light must adhere to these principles.

The Data Controller and Data Protection Officer is Helen Ward.

All contact should be to streetsoflight@outlook.com or via 01992 582951

Contents

Data Processing	2
Personal data.....	2
How we legally use personal data	2
Special categories of data.....	2
Children's personal data	3
Working with Data Subjects - Individuals' Rights	3
Sharing and Disclosing Data	4
Retention Schedules.....	4
Destroying Data.....	4
Data Security.....	4
Data Protection Breaches	4

Data Processing

Streets of Light processes data for the following purposes:

- To create and share trail maps for the annual Streets of Light event
- To promote Streets of Light to individuals and organisations
- To respond effectively to enquiries, complaints etc.

We will make sure that all personal data is:

- Processed lawfully, fairly and in a transparent manner
- Processed for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and up to date
- Not kept longer than necessary
- Processed securely
- Processed in keeping with the rights of data subjects

Personal data

Personal data is any data which can identify a living individual (“data subject”). This includes:

- Contact details

How we legally use personal data

Processing is only lawful if at least one of these conditions in Article 6 of the GDPR is met:

- The processing is necessary for a **contract** with the data subject
- The processing is necessary for us to comply with a **legal obligation**
- The processing is necessary to protect someone’s life (**‘vital interests’**)
- The processing is necessary for us to perform a task in the **public interest** which has a clear basis in law
- The processing is necessary for **legitimate interests** of the data subject or of Streets of Light or another organisation UNLESS these are overridden by the interests, rights and freedoms of the data subject.
- If the data subject has given their clear **consent**.

Special categories of data

Special categories of data include information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trades union membership, health, genetic or biometric data, sexual life and orientation. Processing of this data is only lawful if **in addition to** one of the categories above, one of the following conditions in Article 9 of the GDPR is met:

- **Consent** of the data subject
- It is necessary for carrying out **obligations under employment, social security or social protection law**
- It is necessary to protect someone’s **vital interests** and the individual is incapable of giving consent
- Processing relating only to **members and former members** and provided there is no disclosure to a third party without consent

- Processing relating to personal data manifestly **made public by the data subject**
- Processing necessary for **pursuing legal claims**
- Processing necessary for **substantial public interest** (proportional to the aim pursued and with appropriate safeguards)
- Processing necessary for **medical assessment** (such as assessing the working capacity of an employee)
- Processing necessary for **public health**
- Processing necessary for **archiving purposes** in the public interest or scientific, historical or statistical research purposes

Children's personal data

Consent cannot be given by children under 16; consent of a parent or guardian is needed in this case. Data processing not relying on consent is not affected.

Working with Data Subjects - Individuals' Rights

All requests from data subjects relating to their data protection rights should be forwarded to the Data Protection Officer immediately, before any action is taken. Note that data protection rights do not outweigh other legal requirements, in particular safeguarding.

Data subjects' rights must be made explicitly clear to them at the point of first communication and in privacy notices.

The right to be informed

- Data privacy notices will be published wherever data is collected, particularly on website forms, email circulars and paper forms.

The right of access

- An individual is entitled to obtain confirmation that their data is being processed, access to that personal data, and other supplementary information.
- Information will be provided without delay, and at the latest within one month of request.
- No fees will be charged unless requests are manifestly unfounded, excessive or repetitive. However there are statutory charges for some services such as searches in marriage registers.

The right of rectification

- An individual is entitled to have personal data rectified if it is inaccurate or incomplete.
- Data will be rectified as soon as possible and at the latest within one month.
- If incorrect data has been passed on to third parties, they will be informed of the rectification where possible.

The right to erasure

- An individual has 'the right to be forgotten' where there is no compelling reason for the continued processing of their data.
- A request for erasure will be considered as soon as possible and the reasons for erasure or continued processing will be investigated.
- If appropriate, erasure will happen as soon as possible.

The right to restrict processing

- An individual can block or suppress processing of personal data under circumstances. In this case all processing must cease until the grounds for restriction are investigated.

The right to data portability

- Any data provided to an individual must be in an easily accessible format.

The right to object

- An individual can object to their data being used for 'legitimate interests', tasks in the public interest, direct marketing, and for scientific/historical research and statistics.
- If an objection is lodged, all processing must cease until the grounds for objection are investigated. There are no grounds to refuse an objection to direct marketing.

Sharing and Disclosing Data

- Third party computer applications where data is held 'in the cloud', e.g. Google - data protection is included in their general terms and conditions. The cloud servers used by these companies must be within the EU.

Retention Schedules

- Contact details are held until after the following year's Streets of Light details have been published and advertised.

Destroying Data

- Paper records are shredded; computer records will be deleted.
- Computer hardware that has held personal data will be professionally wiped before being recycled.

Data Security

- Electronic data is held on password-protected computer systems.
- Data kept on paper is held in locked filing cabinets and/or locked offices.

Data Protection Breaches

- Any breach or suspected breach should be reported immediately to the Data Protection Officer.
- Records of breaches will be kept.
- Any breach which may result in a risk to any person will be reported to the ICO within 72 hours.
- Any breach which may result in a high risk to any person will be reported to the data subject(s) affected without delay.