Friends of Trendlewood Park

FRIENDS OF TRENDLEWOOD PARK
DATA PROTECTION POLICY

Approved: October 2024

Signed: 

Chair of The Friend of Trendlewood Park

Introduction

Friends of Trendlewood Park (FoTP) is a voluntary organisation dependent on grants and donations from local government and other interested parties.

FoTP is not a commercial organisation and does not sell it services. FoTP relies on the good will of volunteers and the local community.

It is necessary for FoTP to know who its volunteers are so that they can be communicated with.

There is a communication route to the FoTP through its website which is accessible by the general public via the internet.

These factors mean that FoTP does hold some personal data. Consequently, FoTP has to comply with the United Kingdom General Data Protection Regulations (UK GDPR).

This document outlines how the personal data held by FoTP is protected and managed.

Data Protection Officer

FoTP shall have a nominated Data Protection Officer (DPO). The person nominated as DPO shall be agreed by the FoTP Committee.

Information relating to personal data being held can be made to the DPO via the message form on the 'Contact Us' page of the FoTP website.

Data Protection

Personal data held by FoTP is to be held securely by the person(s) nominated by the FoTP Committee to hold the data.

The person(s) holding the data are required exercise reasonable security measures to prevent the data from being accessed or stolen by unauthorised persons or organisations. These measures should include:

- Holding the data at a private property which can be secured when it is vacant i.e. doors can be locked, windows and other potential ingress points can be closed and secured.
- Hardcopy data is stored out of sight and not readily accessible to other persons that might legitimately be in, or enter, the property i.e. it is not left unattended in plain sight on desks, tables, chairs etc.
- When not in use hardcopy data is filed away out of sight, ideally in a lockable facility.
- Electronic data stored on removable devices should ideally be encrypted. Whether encrypted or not removable devices are to be treated the same way as hardcopy information see above.
- Where electronic data stored on a local computer (PC, laptop, tablet) the computing device must be electronically lockable and have security features that requires at least one of following to unlock it:
    - Password.
    - Finger Print.
    - Face Recognition.
- When not in use the computing device must be in the locked condition.
- When no one is present in the property housing the computing device the computing device must be switched off.

- If electronic data is held remotely i.e. in a 'cloud' type facility the cloud must be password protected and only be accessible by the person legitimately holding the personal data.

How FoTP Processes and Uses Personal Data

FoTP may store some, or all, of the following personal information:

- Name.
- Age range (18-79 or above 80).
- Address including: House number or name, Street, Town, County, Post code.
- Email address.
- Phone number.
- Emergency contact details including a name and phone number.
- Areas of likely involvement with FoTP.
- Medical conditions.
- Individual or family membership.
- Request to receive or not park photos.
- Specific message(s) sent to FoTP contact address.

This data can only be used for the following purposes:

- To contact volunteers about FoTP related activities, events, news, or specific issues.
- In an emergency situation to contact someone known to the volunteer that has suffered an emergency of some kind.
- When a request to receive photos of the park is made the email address of the requesting person is shared with the FoTP volunteer providing photos of the park.
- To respond to specific queries supplied via the Contact Us form on the internet.
    - Note it may be necessary to pass on such messages to a third body such as North Somerset Council or Nailsea Town Council. Where this is necessary the message will either be passed on without identifying the original sender, or the original sender's permission will be sought before forwarding the message to a third party.

If the FoTP DPO receives a request to disclose someone's personal data, then following reasonable checks to confirm the identity of the requesting person and that they have a legitimate right to access the data, the data will be disclosed to them.

How FoTP Decides What Data to Delete

FoTP will review its data annually and delete the records of volunteers that have left FoTP and those of any volunteers known to have died.

In such cases all information relating to the individual will be removed and securely disposed of.

- Hardcopy information will be removed by shredding, burning or otherwise destroying the forms such they are not easily reconstructed by an unauthorised third party.
- Electronic information will be removed by deleting the appropriate entries and any backups that might be held.

Should a volunteer notify FoTP that they are leaving but express a desire to return to the organisation at a later time they may be asked if FoTP has permission to retain their personal data.

If the FoTP DPO receives a request to delete someone's personal data, then following reasonable checks to confirm the identity of the requesting person, that person's personal data will be deleted as soon as possible using the methods outline above.

Cookies and Other Electronic Information

FoTP does not hold this type of information directly. However, some information such as Internet Protocol (IP) address, browser and device characteristics, operating system, referring URLs, device name, country, location and use of FoTP website may be gathered by our web hosting system and held by them. This information is used for internal analytics, reporting and website security purposes.

The FoTP website has a manage consent option allowing users to optout of providing such information.

Requests for data of this type should be passed to Onro Digital at the following address: info@onrodigital.co.uk