West End Refugee Service

Data Protection Policy

Background

The purpose of a Data Protection Policy is to lay down the principles that must be observed by all staff and volunteers who work in an organisation where they have access to person-identifiable information.

West End Refugee Service (WERS)is committed to processing data in accordance with its responsibilities under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

WERS processes personal data in accordance with the following 7 data protection principles set out by the Information Commissioner's Office (ICO):

- Processing personal data lawfully, fairly and in a transparent manner;
- Collecting personal data only for specified, explicit and legitimate purposes;
- Processing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- Keeping accurate personal data and taking all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- Adopting appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction and damage;
- Processing in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- Removing personal data when requested, assuming consent was the lawful basis for processing.

WERS will keep the required documentation about its data processing according to Article 30 of the UK GDPR.

General policy statement

WERS believes that the rights to privacy, confidentiality and appropriate use of data are essential to ensure all individuals have full confidence in the organisation and are treated with respect and dignity. WERS recognises that misuse of data can be damaging and distressing.

The purpose of this policy is to enable WERS to:

1. comply with the law in respect of the data it holds about individuals;
2. follow good practice;
3. protect WERS' clients, staff, trustees, volunteers, members and supporters; and
4. protect WERS from the consequences of a breach of its responsibilities.

WERS will:

- tell individuals the reasons for processing their personal data or criminal records data to perform obligations or exercise rights in employment law;
- obtain explicit informed consent from individuals to hold and process their personal data if there is no other lawful basis for doing so
- update personal data promptly if an individual advises that his/her information has changed or is inaccurate; and
- hold data in the individual's record (in hard copy or electronic format, or both) and on electronic systems. The periods for which WERS holds personal data are contained in the guidelines below

This policy should be read in conjunction with WERS Safeguarding Adults Policy and WERS' Safeguarding Children Policy.

Responsibilities

WERS trustees are responsible overall for setting the Data Protection Policy and ensuring its implementation. However, all employees and volunteers have a duty to do everything they can to ensure that the policy works in practice. The Director is responsible for ensuring that staff know of and adhere to the policy. The Volunteer Co-ordinators are responsible for ensuring that existing and potential volunteers are aware of and adhere to the policy. Individuals who have access to personal data are required:

- to only access data that they have the authority to access and only for authorised purposes;
- not to disclose data except to individuals who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from WERS' premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- Failing to observe these requirements may amount to a disciplinary offence which will be dealt with under WERS' disciplinary procedures. Significant or deliberate breaches of this policy such as accessing personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Guidelines

Client confidentiality is between the client and WERS the organisation and not between the client and individual staff members or volunteers. Treating sensitive client data in strict confidentiality is essential to the way WERS operates in order to gain and maintain the trust of clients.

The following guidelines show how WERS complies with the duties of an organisation under GDPR:

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, they are entitled to the following information:

- a description of the personal data
- the purposes for which it is being processed
- retention period and rights of rectification, erasure, restriction and objections

To make a subject access request, the individual should send the request to info@wers.org.uk or write to WERS.

WERS will respond to a request within a period of one month from the date it is received. If a subject access request is manifestly unfounded or excessive, WERS is not obliged to comply with it.

Other rights:

Individuals have a number of other rights in relation to their personal data. They can require WERS to:

- rectify inaccurate data;
- stop processing or erase data if the individuals' interests override WERS' legitimate grounds for processing data; and
- stop processing or erase data if processing is unlawful

Data security

WERS takes the security of personal data seriously. WERS has procedures and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure data is not accessed, except by staff and designated volunteers. Personal data is stored with password protection and on electronic drives with restricted access and the backups are encrypted. Hard copies are stored in locked filing cabinets and drawers.

Data Breaches

If the charity discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Board will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

How long WERS will keep data

- **Client data.** Files are archived if a client has not come to WERS for 12 months. Files are destroyed after 5 years of non-attendance. This is an extended period of time because, in WERS' experience, there is a significant probability that a client may re-engage with WERS after a long period of non-attendance.
- **Staff data**. If a person ceases to be a member of staff, their personal data will be kept for 6 years and then destroyed.
- **Volunteer data**. WERS will keep the data for 2 years after the volunteer has left.
- **Member data**. WERS will promptly delete the personal data of members who notify WERS that they no longer wish to be members.
- **Supporters data**. WERS will promptly delete the personal data of supporters from mailing lists who notify WERS that they no longer wish to receive communications.
- **Unsuccessful job applicants.** WERS stores job applications for 6 months (in line with ACAS guidance).

This policy will be reviewed every two years or as necessary if there is any change of legislation.

Date: May 2021