ZANE: Zimbabwe A National Emergency
Data Protection Policy

Introduction

ZANE maintains certain personal data about living individuals for the purposes of fundraising, service-delivery and other obligations. ZANE recognises that the correct and lawful treatment of personal data maintains confidence in the charity and provides for successful operations.

This personal data, whether it is held on paper, on computer or other media, is subject to the appropriate legal safeguards specified in the Data Protection Act 1998.

ZANE fully endorses and adheres to the eight principles of the Data Protection Act, as they relate to obtaining, handling, processing, transporting, and storing personal data. Employees who obtain, handle, process, transport or store personal data for ZANE must ensure that data will:

1. be processed fairly and lawfully and will not be processed unless certain conditions are met;
2. be obtained for a specified and lawful purpose and will not be processed in any manner incompatible with that purpose;
3. be adequate, relevant and not excessive for those purposes;
4. be accurate and, where necessary, kept up to date;
5. not be kept for longer than is necessary for that purpose;
6. be processed in accordance with the data subject's rights;
7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
8. and not be transferred to a country or territory outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In order to meet the requirements of these principles, ZANE will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- take the appropriate technical and organisational security measures to safeguard personal data;

Data Handling

Information that is already in the public domain is exempt from the 1998 Act.

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- any personal data which they hold is kept securely;
- personal information is not disclosed orally or in writing or otherwise to any unauthorised third party.

Accessing Data

All individuals who are the subject of personal data held by ZANE are entitled to:

- ask what information is held about them and why;
- ask how to gain access to it;
- be informed how to keep it up to date;
- be informed how ZANE complies with its obligations under the 1998 Act.

All subjects of personal data held by ZANE have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act.

Any person who wishes to exercise this right should make the request in writing to the CEO. ZANE reserves the right to charge a fee for each subject access request. If personal details are inaccurate, they can be amended upon request.

ZANE aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a request 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.

Legal Changes

This policy is subject to adherence to any changes in Data Protection legislation.

ZANE has a separate Card Data Policy reflecting its commitment to comply with required standards governing the security of sensitive and confidential information. The purpose of this security policy is to establish rules to insure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of ZANE's information technology resources. The policy assigns responsibility and provides guidelines to protect ZANE’s systems and data against misuse and/or loss. This security policy applies to all users of computer systems,

centrally managed computer systems, or computers that are authorized to connect to ZANE's data network.

Responsibility for ensuring this policy is adhered to rests with the CEO.

Date policy adopted:

Approved by:

Due for review: Autumn 2019