Information Security.

Policy.

1. Introduction

1.1. This Policy should be read in conjunction with the accompanying Information Security Procedures.

1.1.1. All staff and volunteers with access to the charity's business should sign the Confidentiality Policy statement.

1.1.2. All staff and volunteers should be aware of and abide by the Data Protection policy.

1.1.3. All stand-alone computers and laptops should be virus protected at all times.

1.1.4. The Worldpay Point of Sale card payment reader (reference iCT250 / serial number TID 16909130) should be kept out of site other than when being used and checked for signs of tampering on a monthly basis.

2. Responsibility

2.1. The Business Development Manager is responsible for managing information security, and he/she will also ensure that all employees are trained to understand, implement and maintain the security objectives set out in this Security Policy and as detailed in the company's security related Work Instructions.

3. These Procedures and accompanying Policy document are set out to in the knowledge that the security of our charity, its employees, volunteers and services, and our on-going good security reputation, depend upon the every-day security awareness and actions of all our personnel, both on-site and off-site.

4. We are wholly committed to the principles of Information Security and hereby state that it is the responsibility of every individual employee of the company to ensure that all security plans, standards, procedures, work instructions and actions fully meet with agreed company and customer requirements.

Signed on behalf of the Board _____

Position _____

Dated _____

Review date: November 2023

A current version of this document is available to all members of staff in the Policies and Procedures file.