The Religious of St Andrew

THE ST ANDREW'S DATA PROTECTION POLICY

The EU General Data Protection Regulation – Implementation date 25 May 2018

The Trustees are aware of their responsibility for ensuring that the charity complies with the General Data Protection Regulation [GDPR] and they follow advice from the Office of the Information Commissioner.

One of the most important aspects of the GDPR is data security. Examples of serious breaches include:

- lost, unencrypted memory sticks and back-up hard drives containing sensitive information;
- used computers that have been sold on without first destroying personal data;
- laptops and briefcases stolen from vehicles;
- documents left on the outside of cars that have then been driven away;
- confidential reports missing after being left unattended;
- correspondence sent to the wrong people, and emails sent in error

Compliance with the General Data Protection Regulation

By law, all of St Andrew's sisters, volunteers and employees with access to personal data must be familiar with and adhere to the eight principles of the GDPR. The eight principles specify that personal data must be:

1. Processed fairly and lawfully.

2. Obtained for limited, lawful, specifically stated purposes, and not further processed in any manner incompatible with those purposes.

3. Used in a way that is adequate, relevant and not excessive in relation to the purpose(s) for which it is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept for no longer than is absolutely necessary for the purpose(s) for which it is processed.

6. Processed in accordance with the rights of data subjects under this Act.

7. Kept safe and secure; with appropriate technical and organisational measures taken against unauthorised or unlawful processing, accidental loss, destruction or damage. Note: this means that volunteers and employees must actively take technical measures to ensure any personal information processed on behalf of St Andrews is held securely, especially on mobile devices. The term 'mobile devices' includes laptops, tablets such as iPads, smartphones and any other electronic means by which data can be stored.

8. Personal data must not be transferred to a country or territory outside the European Economic Area (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. Note: the EEA comprises all countries in the European Union plus Iceland, Liechtenstein and Norway.

The rights of the individual

Requests by data subjects with regard to the following must be actioned. Under the terms of the GDPR, all data subjects have the right to:

- obtain a copy of the information held about them;
- withdraw consent for their data to be processed;
- have inaccurate information about them corrected;
- opt out of direct marketing; and
- claim compensation where they have suffered damage or distress as a result of a breach of the DPA.

Dealing with data subject access requests

The Trust will as obliged, on written request to provide the data subject with a description

of the data held, the purpose(s) for which it is held, the source of the data and a list of those to whom it has been or will be disclosed, as well as a copy of the data.

All information held at the time the application was made must be supplied within 40 days unless the provision of information would involve disproportionate effort.

Keeping data safe and secure

Necessary precautions include the Hard copies of sensitive personal data, including contemporaneous notes, which must be stored in such a way that unauthorised access is prevented (a locked filing cabinet, for example), and, together with computers or mobile devices, kept in a room that can be locked when unattended.

GDPR Notice for Visitors

At annex A is a notice relating to St Andrew's use of personal information which is intended for display on the Visitors' Notice Board.

Trustees Policy No 20

Reviewed 29th March 2024