THE FIRST ORDER OF THE SOCIETY OF SAINT FRANCIS
EUROPEAN PROVINCE

GUIDELINES Number 21A

Data Protection Policy

1. **Introduction**

   The Brothers or the First Order of the Society of St Francis (registered charity 236464; SSF) and The Sisters of the Community of St Francis (registered charity 286615; CSF) are committed to ensuring that personal data is protected, in accordance with the General Data Protection Regulation 2016/679 (GDPR).

   The GDPR only covers Personal Data, which can be divided into two sub-categories; General and Sensitive. Any information held regarding a deceased individual or a non-person, such as a business or charity, is not covered by this Act.

   General Personal Data is information which can identify a living individual, either on its own, or when added to other information held by the Data Controller or to any person to whom you are disclosing the information.

   For example, on a guest register, having the name John Smith being there on the 1st to 3rd, is not personal data, as one cannot identify who John Smith is, however, if we were to write John Smith of 1 The Street, London, he can be easily identified and so we would be holding General Personal Data.

   Sensitive Personal Data is information that is always considered personal data. The categories include, but are not limited to: race/ethnic origin, political opinions, religious beliefs, previous offences, membership of a trade union, health of an individual, an individual's sexual life.

   Publicly declared information is not considered sensitive – for example the religious beliefs of brothers/sisters should not be considered sensitive as we have made a public declaration of our beliefs at novicing.

2. **Data Protection Officer**

   Each charity shall appoint a Data Protection Officer, who will be responsible for:

   - annually auditing the personal data held by the charity and how it is processed, to ensure it complies with the GDPR;

- recommending changes to how data is held and processed to houses and individuals;
- ensuring that brothers, sisters, employees and volunteers are aware of this policy and the importance of acting appropriately with personal data;
- ensuring that requests for personal data, for personal data to be altered, removed and appropriately dealt with;
- ensuring that data breaches are acted upon effectively;
- annually reporting to the respective Provincial Chapter/Joint Chapters ~~of~~ any significant aspects of data protection;
- updating this policy and any related paperwork, when necessary.

3. **Annual audit of personal data**
   The Data Protection Officer will be responsible for conducting an annual audit of the personal data held by their respective charity, this will involve:
   - confirming what data is held, how it is held and who has access to the data, and that we have an appropriate reason/permission for doing this;
   - confirming how data is processed, that this is done securely, and that we have an appropriate reason/permission for doing this;
   - confirming that data is not shared with a third party, unless we have an appropriate reason/permission for doing this;
   - confirming that data that should have been destroyed has been securely destroyed.

4. **Holding and Processing Data**
   a) **Principle of holding or processing personal data**
   To hold or process personal data we are required to either have
      - permission from the individual to hold the data;
      - a legitimate reason for holding it (such as the charity would not be able to fulfil its purpose if we did not hold it);
      - a legal reason to hold the data.

   b) **Security**
   Personal data should be held in as secure a manner as practically possible. Paper records, particularly of sensitive personal data, should be held in locked spaces. Electronic records, should be stored either on the computer or within the cloud, within an EEA country. To ensure the security of

the data, computers should be well maintained to prevent hacking or data loss, but also passwords and encryption should be considered in certain circumstances.

c) **Timeframe**
Data should only be held as long as there is a reason to hold it. If the reason is no longer valid, then the data should be securely destroyed.

5. **Sharing of Data**
Personal data should not be shared with individuals within the charity who do not need the information. Personal data should not be shared with third party organisations or individuals unless we have an appropriate reason/permission for doing this.

6. **Request for Data, amendment of data or deletion of data**
Unless subject to an exemption under the GDPR, an individual has the following rights with respect to their personal data: -

- The right to request a copy of the personal data CSF and SSF hold about them;
- The right to request that CSF and SSF correct any personal data if it is found to be inaccurate or out of date;
- The right to request personal data is erased where it is no longer necessary for CSF & SSF to retain such data;
- The right to withdraw consent to the processing at any time;
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller (known as the right to data portability).
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data;
- The right to lodge a complaint with the Information Commissioner's Office.

Upon receiving such a request, if it can be dealt with simply and accurately then this should be dealt with and the individual informed as soon as possible of CSF/SSF's compliance.

If the request is disputed or complex then an initial response should be sent to the individual within one week and the Data Protection Officer advised, with a further response within 28 days.

Should the response not prove acceptable to the complainant, then it should be considered a formal complaint and be dealt with according to the *Procedure for Formal Complaints* (SSF Guidelines 5E). It may be necessary, in severe cases, to involve the Information Commissioner's Office and to lodge a Serious Incident Report with the Charity Commission.

7. **Data Breach**

A data breach is the intentional or unintentional release of personal data to an untrusted environment without appropriate permission or reason. Upon becoming aware of a data breach the Data Protection Officer should be informed as soon as possible.

The Data Protection Officer is responsible for keeping a record of any personal data breaches, regardless of the requirement to notify. Depending on the nature of the data breach the Data Protection Officer, will be responsible for:

- Informing relevant supervisory authorities of the data breach within 72 hours. This may include, but is not limited to, the Minister, Chapter (as trustees of the charity), the Charity Commission (as a Serious Incident Report) and the Information Commissioner's Office.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they must also be informed without undue delay.

Pentecost 2018