**Standard Operating Procedure (SOP)**

**Data and Privacy**

**DAP-006-01**

**Purpose**

The purpose of these Standing Operating Procedures (SOPs) is to establish a framework for Out There Exeter (the “charity”), to effectively manage its privacy obligations and protect the personal data of its staff, volunteers, beneficiaries, and other stakeholders. This SOP aims to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and promote good privacy practices within the charity.

**Scope**

ThisSOP applies to all aspects of Out There Exeter's operations that involve the collection, use, storage, disclosure, and disposal of personal data. This includes, but is not limited to, the following activities:

* **Collecting personal data:** Obtaining personal data from individuals through forms, surveys, online interactions, or other means.
* **Using personal data:** Processing personal data for legitimate charitable purposes, such as providing services, managing programs, and communicating with stakeholders.
* **Storing personal data:** Storing personal data securely and confidentially in appropriate formats and locations.
* **Disclosing personal data:** Sharing personal data with third parties only when authorised and in accordance with the UK GDPR.
* **Disposing of personal data:** Destroying or securely erasing personal data when it is no longer required.

**Responsibilities**

The following are the key responsibilities for privacy at Out There Exeter:

* **Trustees:** Ultimately responsible for the charity's privacy compliance and ensuring adherence to these SOPs.
* **Data Protection Officer (DPO):** Oversees the implementation of the charity's privacy framework and coordinates privacy-related activities. In the absence of a DPO, these responsibilities fall to the Trustees.
* **Staff and Members:** Responsible for complying with privacy policies and procedures when handling personal data.

**Procedures**

1. **Data Collection and Processing** 
   1. Collect personal data only for legitimate charitable purposes, such as providing services, managing programs and events, and communicating with stakeholders.
   2. This SOP applies to all personal data collected, processed, and stored by Out There Exeter, including but not limited to:

* Employee data
* Volunteer data
* Beneficiary data
* Donor data
* Supplier data
  1. Obtain informed consent from individuals before collecting their personal data.
  2. Provide clear and transparent privacy notices to individuals about how their personal data will be used.
  3. Use personal data only for the purposes for which it was collected and in accordance with the UK GDPR.

1. **Data Security**
   1. Implement appropriate technical and organisational measures to protect personal data from unauthorised access, use, disclosure, alteration, or destruction.
   2. Use secure storage methods for personal data, both electronically and physically.
   3. Limit access to personal data to authorised personnel only.
   4. Train staff on data security awareness and best practices.
2. **Data Sharing and Disclosure**
   1. Share personal data with third parties only when necessary for legitimate charitable purposes and in accordance with the UK GDPR.
   2. Implement data sharing protocols with third parties to ensure secure and compliant data transfers.
   3. Obtain written agreements with third parties who handle personal data on the charity's behalf, ensuring they are compliant with the UK GDPR.
   4. Do not disclose personal data to third parties for marketing purposes without the individual's consent.
   5. Regularly review and monitor third-party service providers to ensure their ongoing compliance with data protection obligations.
3. **Data Retention**
   1. Retain personal data only for the minimum period necessary for the purpose for which it was collected.
   2. Out There Exeter will retain personal data for the minimum period necessary for the purpose for which it was collected. The following data retention periods apply to different types of personal data:

* **Employee data:** Retain for a period of seven years after the employment relationship ends, or longer if required by law.
* **Volunteer data:** Retain for a period of three years after the volunteer relationship ends, or longer if required by law.
* **Beneficiary data:** Retain for a period of five years after the last interaction with the beneficiary, or longer if required by law.
* **Donor data:** Retain for a period of seven years after the last donation, or longer if required by law.
* **Supplier data:** Retain for a period of five years after the last transaction with the supplier, or longer if required by law.
  1. Establish clear data retention procedures, to ensure the proper retention and disposal of personal data, including:
* **Data classification:** Classify personal data based on its sensitivity and retention requirements.
* **Data mapping:** Create and maintain a data map to identify the location and categorisation of personal data.
* **Access controls:** Implement appropriate access controls to restrict access to personal data to authorised personnel only.
* **Regular review:** Regularly review personal data holdings to ensure they are accurate, up-to-date, and no longer required.
* **Secure disposal:** Securely destroy or erase personal data that is no longer required in accordance with data retention policies.
  1. Review and update data retention policies regularly to ensure they remain aligned with the charity's legal obligations and needs.
  2. Securely destroy or erase personal data that is no longer required.

1. **Subject Access Requests (SARs)**
   1. Respond to SARs promptly and within the one-month timeframe specified by the UK GDPR.
   2. Provide individuals with access to their personal data and the ability to rectify, erase, or restrict the processing of their data.
   3. Keep records of all subject access requests and responses, to demonstrate compliance with the UK GDPR.
2. **Privacy Breach Reporting**
   1. Establish procedures for identifying, reporting, and investigating privacy breaches promptly, including:

* **Incident identification:** Establish procedures for identifying and reporting potential data breaches, including internal and external reporting channels.
* **Risk assessment:** Assess the severity and potential impact of data breaches to determine the appropriate response.
* **Notification:** Notify the UK Information Commissioner's Office (ICO) of any significant data breaches within 72 hours of becoming aware of them.
* **Communication:** Communicate data breaches to affected individuals in a timely and transparent manner, providing guidance on any necessary protective measures.
* **Investigation:** Conduct a thorough investigation of data breaches to determine the root cause, implement corrective actions, and prevent future occurrences.
  1. Notify the UK Information Commissioner's Office (ICO) of any significant privacy breaches within 72 hours, as required by the UK GDPR.
  2. Document and learn from privacy breaches to prevent future occurrences.

1. **Privacy Awareness and Training** 
   1. Provide regular privacy awareness training to all trustees, staff, members and volunteers.
   2. Incorporate privacy considerations into all relevant policies, procedures, and training materials.
   3. Promote a culture of data privacy within the charity, emphasising the importance of protecting personal data and respecting privacy rights.
2. **Commitment to Data Protection**
   1. Commit to upholding the highest standards of data protection and ensuring the privacy and security of personal data in all its operations.
   2. Strive to continuously improve its data protection practices and adapt to evolving data protection requirements.
   3. Take all necessary steps to resolve data protection breaches promptly and minimise any harm to individuals affected.
   4. Conduct regular audits to assess the charity's data protection compliance and identify areas for improvement.
   5. Seek expert advice from the Data Protection Officer or external consultants as needed to address complex data protection issues.

**Review and Revision**

This SOP will be reviewed and revised annually to ensure that it remains relevant and effective, or as needed to reflect changes in the charity's strategies or the regulatory environment.

**Compliance**

Failure to comply with this SOP may result in investigation and disciplinary action, up to and including dismissal for employees and termination of volunteer appointments and membership of the charity, and a vote on removal of trustee.

**Version Control**

|  |  |
| --- | --- |
| **Version:** | v1.1 FINAL |
| **Date of approval:** | 01/12/2023 |
| **Date of next review is due:** | 01/12/2023 |