Sunrise Diversity

Data Protection Policy

Policy Statement

Sunrise Diversity is committed to a policy of protecting the rights and privacy of individuals, voluntary and community group members in accordance with The Data Protection Act 1998 and General Data Protection Regulation (GDPR) 2018 . Any breach of The Data Protection Policy is considered to be an offence and in that event, disciplinary procedures apply.

Introduction

The Data Protection Act 1998 establishes 8 principles which state that personal information shall be:

- Processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose(s).
- Adequate, relevant and not excessive.
- Accurate and where necessary up to date.
- Kept for no longer than necessary.
- Processed in accordance with the individual's rights.
- Protected by the appropriate security.
- Not transferred to countries outside the European Economic Area without adequate protection.

The use of personal data is also governed by other statutory and common law requirements, including the law of confidence and defamation. Sunrise is committed to ensuring that its use of personal data is fully complaint with the law and best practice including the General Data Protection Regulation (GDPR) May 2018.

Sunrise is the data controller and has the responsibility for legally determining the purposes for which, and the manner in which, any personal data is or will be processed.

1. Aim

The aim of the Data Protection Policy is to ensure that staff, volunteers, service users and others who may use personal information in the course of their duties to enable Sunrise to carry out its functions, understand their responsibilities with regard to Data Protection. Some of the requirements are complex and detailed, particularly for those members of staff who are responsible for deciding what personal information is kept and how it is used. For this reason the Policy does not attempt to give

detailed guidance. Instead its purpose is to identify how Data Protection issues will be managed by describing rights and responsibilities.

2. Procedures

Sunrise holds three types of information which are covered by this policy.

- **Organisational** information – publicly available information about organisations and some confidential information. Whilst information about organisations is not covered by the Data Protection Act, there is sometimes ambiguity about whether certain information is personal or organisational. For instance the contact details for ensuring service user support may be someone's name, home address, telephone number or email address. As Sunrise strives for best practice with regard to organisational information it is covered by this policy.
- **Personal** information – information about individuals such as names, addresses, job titles, telephone number, email address. This information is essentially factual but may also be an opinion.
- **Sensitive** information – information about staff and service users such as health, race, ethnicity, politics, membership of a trade union, religion, sexuality, and criminal convictions. This can also include any recording of dietary requirements which might allow a person's religion to be deduced. Membership of certain network/political groups can also be seen as sensitive data. Processing this data requires the individual's consent.

Data Subject

The data subject is the individual who is the subject of personal data. This will include staff, volunteers, service users, suppliers of goods, visitors, contractors, etc.

Data

Data is information which is processed by a computer or manually held on a paper file which identifies individuals, or where specific criteria can be used to identify individuals. Also covered are emails, recorded telephone calls and answering machines, CCTV footage, photographs or information like fingerprints and notepads, such as telephone jotters which can be used to identify an individual.

Sunrise will not hold information about individuals without their knowledge and consent. The information held will be for specific purposes and the data subject will be informed of what those purposes are. Sunrise will also inform individuals if the purposes for holding information change.

Information about data subjects will not be disclosed to other organisations or to individuals who are not members of Sunrise staff or Board of Trustees except in circumstances where there is a legal requirement, where there is explicit or implied consent or where the information is publicly available elsewhere.

Information will not be retained once it is no longer required for its stated purpose. Cross reference to Recruitment and Selection Policy, Supervision and Support Policy and Appraisal Policy for retention of information for staff and volunteers.

Sunrise will seek to maintain accurate information by creating ways in which data subjects can update the information held. Data subjects are entitled to have access to information held about them by Sunrise.

Data subject's personal information will not be released by Sunrise for the purposes of direct marketing.

Processing

Processing is any action involving data – i.e. obtaining, storing, sorting, updating or deleting it. If people working or volunteering for Sunrise have access to personal data they should assume they are processing it, and are responsible for data in this capacity.

3. Practice

How Sunrise Manages Data Protection

This part of the Policy identifies the Data Protection responsibilities of the Board, staff and volunteers.

Board of Trustees

The Board of Trustees are responsible for ensuring that Sunrise is fully compliant with the law and best practice for handling personal information. They will:

- Approve and review policies and procedures for handling personal information.
- Allocate resources to enable the Data Protection Policy to be practically and proactively applied.

Sunrise CEO (Data Protection Officer)

- Provide general guidance, advice and dissemination of information regarding Data Protection.
- Provide Data Protection awareness training to all staff and volunteers as part of induction.
- Ensure there is a regular cycle of checking, updating or discarding old data.
- Deal with data subject access requests and co-ordinate responses to complaints.
- Co-ordinate and advise on all requests for disclosure of personal information.
- Monitor and report to the Board on compliance and recommendations for improving good practice.

Staff and Volunteers

- Ensure they are satisfied with the legality of holding and using personal information.
- Ensure that the use of personal data complies with all Sunrise policies.

- Refer any requests for disclosure, requests for data subject access and requests to cease processing to the Sunrise CEO immediately.

Confidentiality

Access to personal data is on a "need to know" basis only. Access to information is monitored by the CEO. Personal data is regularly reviewed, updated and deleted in a confidential manner when it is no longer required. Sunrise will only retain records, if it considers it necessary, for a maximum of 5 years.

Data which is kept on Sunrise premises will always be locked in a filing cabinet.

Where personal data needs to be taken away from Sunrise premises for business purposes, the member of staff must be authorised to do so by the CEO. Any member of staff who takes personal data from Sunrise premises is under a legal responsibility to keep it secure, making sure it is never left unattended in a car or in a public place.

Information held electronically

All users of personal information have a responsibility for the security of that data when held electronically. Passwords used to access data will be kept confidential (not written down or kept near the electronic device) and changed on a regular basis. All data will be scanned for computer viruses on a regular basis.

Any breaches of IT security will be investigated by the CEO supported by a nominated Board member.

Personal data not transferred to countries outside the UK, unless the country has adequate protection for the individual.

Data must not be transferred to countries outside the UK without the explicit consent of the individual. Sunrise takes particular care to be aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the European Economic Area.

Access to information

Staff, volunteers and service users have the right to view any information relating to them that is held by Sunrise. Any request to view this information must be in writing and forwarded to Sunrise CEO. The CEO will check the identity of the data subject before handing over any information. The request will be responded to, in writing, within one month of the request being made and by way of a one to one meeting. The CEO will make any decisions where there is a request for personal information to be corrected or deleted.

Policy reviewed	March 2021
Ratified by:	Board of Trustees