Solutions for the Planet

Data Protection Policy and Procedures

Introduction

Solutions for the Planet (S4TP) is committed to a policy of protecting the rights and privacy of individuals, S4TP needs to collect and use certain types of Data to carry on our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act (DPA) 1998 and General Data Protection Regulations (GDPR) 2018 govern the use of information about living people (personal data). Personal data can be held on computer or in a manual file, and includes email, telephone numbers, minutes of meetings, and photographs. S4TP will remain the data controller for the information held. S4TP will be responsible for processing and using personal information in accordance with the Data Protection Act.

All board and staff members who have access to personal information, will be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out S4TP's commitment and procedures for protecting personal data. S4TP regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The General Data Protection Regulations

This contains 8 principles for processing personal data with which S4TP will comply. Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s)

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area 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 information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller –The person who (either alone or with others) decides what personal information S4TP will hold and how it will be held or used.

General Data Protection Regulations – The UK legislation that provides a framework for responsible behaviour by those using personal information. As of May 2018, this replaces the 1998 Data Protection Act.

Senior information rights owner –Board member who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998 and GDPR 2018.

Information asset owner – Any member of staff who process personal information.

Data Subject/Service User – The individual whose personal information is being held or processed by S4TP.

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see GDPR definition) to the processing of personal information about her/him.

Explicit consent is needed for processing all personal data and sensitive data this includes the following:

(a) racial or ethnic origin of the data subject
(b) political opinions
(c) religious beliefs or other beliefs of a similar nature
(d) trade union membership
(e) physical or mental health or condition
(f) sexual orientation
(g) criminal record
(h) proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioners Office (ICO) about the data processing activities of S4TP.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing, or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the S4TP.

Applying the Data Protection Act within S4TP

Collection, storage, and access to personal data is limited to the staff members of S4TP.

Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them. As of May 2018, individuals also have the right to be forgotten and have all their data removed from S4TP systems.

Responsibilities

S4TP is the Data Controller, and is legally responsible for complying with GDPR as of May 2018. This means S4TP determines what purposes personal information held will be used for.

The Board will consider legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information,

- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information

The senior information rights owner on the board is

Name: Jen Baughan

Contact Details: Jen@solutionsfortheplanet.co.uk

The lead data protection person is

Name: Jess Mitchell

Contact Details: Jess@solutionsfortheplanet.co.uk

The Senior information rights owner will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- Dealing promptly and courteously with any enquiries about handling personal information
- Describe clearly how it handles personal information
- Will regularly review and audit the ways it holds, manages and uses personal information
- Will regularly assess and evaluate its methods and performance in relation to handling personal information
- All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

Solutions for the Planet

Data Protection Policy and Procedures

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and General Data Protection Regulations 2018.

In case of any queries or questions in relation to this policy please contact Jess Mitchell, Data Protection Lead, jess@solutionsfrotheplanet.co.uk.

Data collection

Informed consent

In line with the 2018 General Data Protection Regulations (GDPR) informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

S4TP will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, S4TP will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit written consent for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Legitimate interest

In certain cases, S4TP may store and process data without the demonstrable consent of the data subject. In doing so S4TP cites legitimate interest for holding and processing said data. Each individual case for legitimate interest is reviewed and documented within a legitimate interest assessment or LIA. Data subjects or any personas wishing to see details of the LIAs may do so by contacting S4TP directly.

Data Storage

Solutions for the Planet

Data Protection Policy and Procedures

Information and records relating to service users will be stored securely and will only be accessible to S4TP staff. Information will be stored for only if it is needed or required and will be disposed of appropriately.

It is S4TP's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party. This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and General Data Protection Regulations 2018.

Data Subject Access Requests

Members of the public may request their information from S4TP at any point. S4TP will have seven working days to respond to the request.

Disclosure

On some occasions S4TP will need to share data with certain other agencies. The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows S4TP to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

S4TP regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. S4TP intends to ensure that personal information is treated lawfully and correctly.

Risk Management

Solutions for the Planet

Data Protection Policy and Procedures

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released without their knowledge. S4TP staff should be aware that they can be personally liable if they use personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of S4TP is not damaged through inappropriate or unauthorised access and sharing.

Electronic copies of personal data

Files containing personal data are to be stored within the S4TP online system or on encrypted memory sticks. Files contain personal data are not stored on personal desktops, laptops, or memory sticks or as paper copies (see below).

Paper copies of personal data

Paper files containing personal data are uploaded to the S4TP online system upon receipt and then destroyed by shredding or burning. No paper copies of personal data are printed without prior consent of the SIAO. Any postage of files containing personal data is done so by recorded delivery post.

Destroying personal data.

Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of a programme cycle and its evaluative stage. S4TP review their data every two years and will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to S4TP please contact the Data Controller: Jessica Mitchell

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

All organisational staff are required to sign and date this form at the beginning of their employment.