GDPR and Confidentiality POLICY

Written	February 2023
Review Date	February 2024

Introduction

Safe Soulmates as part of its business activities needs to gather and use certain information about individuals. These can include people we support and their families, employees, volunteers, board members, contractors, partners and other people the organisation has a relationship with or may need to contact.

Safe Soulmates takes the security and privacy of your data seriously. We need to gather and use information or data about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** and the **General Data Protection Regulation** in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

The organisation will therefore follow procedures that aim to ensure that all employees, students, contractors, and volunteers who have access to any personal data (held about employees, board members, volunteers, or people we support and their families) are fully aware of and abide by their duties and responsibilities under the Act.

Purpose and Scope

This data protection policy ensures Safe Soulmates:
• Complies with data protection law and follows good practice;
• Protects the rights of clients, their families, staff and partners;
• Is open about how it stores and processes individuals' data;
• Protects itself from the risks of data breach.

Data protection risks

This policy helps to protect Safe Soulmates from some very real data security risks, including:

• Breaches of confidentiality – for instance, information being given out inappropriately;
• Failing to offer choice – For instance, all individuals should be free to choose how the organisation uses data relating to them;
• Reputational damage – For instance, the company could suffer if hackers successfully gained access to sensitive data.

Everyone who works for or with Safe Soulmates (both staff, volunteers and contractors) has responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

4. Definitions Terms

GDPR: means the General Data Protection Regulation.

Data Protection Act 2018: The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Subject/Service User : The individual whose personal information is being held or processed by Safe Soulmates (for example: a service user or a supporter).

Explicit consent is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him. Explicit consent is needed for processing sensitive data this includes the following: racial or ethnic origin of the data subject; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual orientation; criminal record; proceedings for any offence committed or alleged to have been committed

Information Commissioner: The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

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 Group.

5. Data protection principles

The organisation is committed to processing data in accordance with its responsibilities under the GDPR.
GDPR requires that personal data shall be:
a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step
must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. General provisions

a. This policy applies to all personal data held and processed by the Safe Soulmates;
b. This policy shall be reviewed at least annually;
c. The organisation shall register with the Information Commissioner's Office as an organisation that processes personal data.

7. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent;
b. Individuals have the right to access their personal data and any such requests made to the organisation shall be dealt with in a timely manner.

8. Lawful purposes

a. All data processed by the organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information);
b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data;
c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the organisation's systems.

9. Data minimization

a. The organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
b. Any other considerations relevant to the organisation's particular systems.
c, Data is used to identify members and ensure we have health information to put in place the relevant measures to keep people safe and can respond appropriately in an emergency situation.

10. Accuracy

a. The organisation shall take reasonable steps to ensure personal data is accurate.

11. Security

a. The organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date;
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information;
c. When personal data is deleted this should be done safely such that the data is irrecoverable;
d. Passwords are stored on a secure Citrix password manager;
e. All personal information is on Cognito forms which is encrypted;
f. Appropriate back-up and disaster recovery solutions shall be in place.

12. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Safe Soulmates is registered as such. The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. It is the Director's responsibility to ensure the timely renewal.

13. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the organisation shall promptly assess the risk to people's right sand freedoms and if appropriate report this breach to the ICO (more information on the ICO website) and to Named Data Controller Glenn Jobson glennsafesoulmate@gmail.com