# Our Data Protection Policy

Splitz Support Service takes its responsibilities with regard to the management of the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) very seriously.

Splitz Support Service obtains, uses, stores and otherwise processes personal data relating to potential staff and volunteers, current staff and volunteers, former staff and volunteers, current and former service users, and contractors, collectively referred to in this policy as data subjects. When processing personal data, the charity is obliged to fulfil individuals' reasonable expectations of privacy by complying with relevant data protection legislation.

Data will be held securely in accordance with the principles of the data protection legislation.

The Senior Management Team is responsible for implementing the policy.

All employees share responsibility for data protection.

This policy therefore seeks to ensure that we:

1. Are clear about how personal data is processed and the charity's expectations for all those who process personal data on its behalf;
2. Comply with the data protection law and with good practice;
3. Protect the charity's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights;
4. Protect the charity from risks of personal data breaches and other breaches of data protection law.

The charity commits to:

1. Ensure staff and volunteers understand their role in ensuring personal data is handled sensitively and safely at all times;
2. Provide training to all staff and volunteers on the data protection principles and how to report security concerns;
3. Ensure strong security systems are in place to protect personal data at all times, including when in transit and when at rest;
4. Monitor security systems and act to ensure they remain effective at all times;
5. Ensure data subjects know their rights and have the means to request the relevant access to their data;
6. Ensuring privacy by design practices are included in all new projects;
7. Act in accordance with the requirements of data custodians when providing services as a data processor;
8. Developing systems for auditing data security, and monitoring these systems.

Ann Cornelius

Chair
March 2020