St Andrew's Community Network
Data Protection Procedure

---

1. Introduction

St Andrew's Community Network needs to collect and use certain types of information about individuals who come into contact with St Andrew's Community Network in order to carry on our work.

Due to the nature of the work undertaken by St. Andrew's Community Network (mainly involving vulnerable adults), much of the data processed is defined as sensitive, and handling such data well is a priority for the organisation.

This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under General Data Protection Regulations (GDPR) 2018.

2. Data Controller

St Andrew's Community Network is the Data Controller under the Act, which means that it determines what purposes personal information is held for, how it will be processed and what it will be used for. It is responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used. It is also responsible for reporting and responding appropriately to a breach of data.

3. Disclosure

St Andrew's Community Network may share data with other agencies such as the local authority, funding bodies, evaluation partners and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances of how and with whom their information will be shared. We do this through published Privacy Notices.

There are circumstances where the law allows St Andrew's Community Network to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State
b) Protecting vital interests of an Individual/Service User or another person
c) The Individual/Service User has already made the information public
d) Conducting any legal proceedings, obtaining legal advice, or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e., race, disability, or religion
f) Providing a confidential service where the Individual/Service User'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 Individuals/Service Users to provide consent signatures.

St Andrew's Community Network 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. Therefore, any ad-hoc requests to share information should be authorised by the Data Protection Lead.

4. Data Protection Act Adherence

St Andrew's Community Network will ensure that personal information is treated lawfully and correctly. St Andrew's Community Network will adhere to the 6 Principles of Data Protection, as detailed in the Regulations.

Specifically, the Principles require that personal information shall be:

1) processed lawfully, fairly and in a transparent manner in relation to individuals
2) 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.
3) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5) 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.
6) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

St Andrew's Community Network will, through appropriate management and strict application of these procedures ensure the quality of information used.

5. Responding to requests for information

The data subjects have specific rights under the data protection act. SACN ensures that the rights of people about whom information is held can be fully exercised under the Act.

Staff and volunteers will treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for information.

These data subject rights 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)

All requests for information shall be directed to the Data Protection Lead. The Data Protection Lead will:

- Seek written confirmation from the individual/service user
- Inform the individual/service user of the time scale for processing (normally 4 weeks but in some cases, this may take longer)
- Process the request within the time scale

Detailed procedures for dealing with a requestion for information are in the Data Subject Access request procedures.

6. Assessment of Data Mapping

St Andrew's has undertaken the mapping of data processes and is committed to reviewing this regularly. This information is available to view as a separate data processing document for each subject area. SACN will review the following aspects annually:

- The nature of the data we collect
- The basis on which we hold the data
- Any changes to how we handle this data

7. Data Collection

A lot of the data we collect is personal information and therefore classed as sensitive data. This means it can be used to identify people we support.

GDPR 2018 identifies 6 different lawful bases for collecting and processing data:

- Contract
- Legitimate interest
- Legal Obligation
- Vital Interest
- Public task
- Consent

When collecting data, we will ensure that the Individual / Service User has access to the privacy notice that explains:

- why the information is needed.
- what it will be used for and what the lawful bases are for processing the data.
- when explicit consent, is required and why is the process of special category data necessary.

When consent is collected, as far as reasonably practicable, we will ensure that the data subject is competent enough to give consent and has given so freely without any duress.

SACN maintains a data processing document for each area of its work that explains the lawful bases for the collection, processing and storage of data. These are updated annually.

8. Data Storage and Security

SACN takes the security of the data we collect very seriously. We have taken appropriate technical and organisational security measures to safeguard personal information.

Most of the data is stored electronically in a secure database and can only be accessed by authorised people who hold the relevant password and login details (supported with multi-factor authentication).

All users of the system are required to complete a "data protection statement" which means that they know they must keep this data safe. All our staff and volunteers should also sign a confidentiality agreement.

Where we keep paper records (e.g., foodbank vouchers and/or volunteer application forms) these are always kept in a locked drawer, before staff leave the office. No paper records are to be left on the desk at night.

All our trustees and staff have work-specific email addresses.

In the unlikely event that there is a personal data breach, the Data Protection Lead will action the following procedure without hesitation:

- Contain the breach
- Assess any adverse consequences for individuals
- Assess whether to inform individuals involved
- Assess whether to inform the Information Commissioner's Office
- Keep an accurate record of the breach

Details of procedures for what to do when a breach occurs and whom to contact are explained in the Data Breach Procedures.

9. Data Retention

The length of time SACN will keep data depends on the area of work under which the data has been collected. This information is detailed in a Process flow document for each of the subject areas.
At the appropriate time, electronic data will be deleted, and paper records will be shredded.

When any computer system previously used within SCAN, has been passed on / sold to a third party, it is the staff's responsibility to ensure all personal and company data is non-recoverable. If in doubt, contact your line manager or Data Protection Lead.

10. Data access and accuracy

All Individuals / Service Users have the right to access the information St Andrew's Community Network holds about them. St Andrew's Community Network will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

When processing personal information, the organisation:

- Will ensure that staff follow the directions given by the Data Protection Lead who will have specific responsibility for ensuring compliance with the Data Protection Act
- Understands that staff are contractually responsible for following good data protection practices as set out in these procedures.
- Will ensure that staff have received training and guidance before processing personal information, contact your line manager or the Data Protection Lead if in doubt.
- Will deal promptly and courteously with any enquiries about handling personal information, if in doubt contact your line manager or the Data Protection Lead.
- Will assist the Data Protection Lead as they undertake audits of the ways we hold, manage and use personal information.
- Understand that any breach by any member of staff of the rules and procedures identified in these procedures may lead to disciplinary action being taken against that staff member.

11. Other Networks

We are part of some wider networks of note, especially Community Money Advice, which oversees our debt services and Trussell Trust, which oversees our Foodbanks.

We operate under their guidance, and they have had significant input into our policies and procedures. We have agreements with both of these organisations that cover data, but we will justify our own actions where necessary. In process terms there may also be a delay in changes being implemented as guidance is received and revised.

12. Sending personal data abroad.

Currently, no personal information should be transferred abroad. Contact the Data Protection Lead if you believe personal data is going abroad. If data needs to go abroad the Data Protection Lead ensures suitable safeguards are in place before the information is sent.

13. Question about these Procedures

In case of any queries or questions in relation to these procedures please contact the St Andrew's Community Network Data Protection Lead.

Policy approved by: The Trustees
Date of Approval: August 2024
Date for Review: August 2025

14. Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information St Andrew's Community Network will hold and how it will be held or used.
General Data Protection Regulations 2018 - The GDPR significantly changes the rights of Data Subjects and the obligations of those processing data. It also significantly increases the penalty for non-compliance.
Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.
Date Protection Lead – The person(s) responsible for ensuring that St Andrew's Community Network follows its data protection policy and complies with the Data Protection Act 2018.
Individual/Service User – The person whose personal information is being held or processed by St Andrew's Community Network for example: a client, an employee, or supporter.
Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.
Notification – Notifying the Information Commissioner about the data processing activities of St Andrew's Community Network, as certain activities may be exempt from notification.
Information Commissioner – The UK Information Commissioner is responsible for implementing and overseeing the Data Protection Act 2018.
Processing – means collecting, amending, handling, storing or disclosing personal information.
Personal Data – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within the organisation.

Special Category data – also referred to as Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

St Andrew's Community Network

16 Larkhill Lane, Clubmoor, Liverpool, L13 9BR
0151 226 3406 www.standrewslive.org.uk

Reg. Charity No. 1105307 | Reg. Ltd. Company No. 4918017
Regulated and authorised by the FCA No. 692452