



SCRP 8a

Policy Title: GDPR

1. Introduction

This policy sets out how SCRP Ltd applies the provisions of the General Data Protection Regulation. It applies to all who handle or have access to information about individuals including the board of directors, all paid staff, volunteers, partners, and anyone working on behalf of SCRP, henceforth referred to as “staff”. Significant breaches of this policy will be handled under SCRP’s disciplinary procedure (Policy 16). If any party concerned has a sensory or physical impairment, efforts should be made to ensure that all aspects of this policy and exchanges between parties are understood.

This policy should be read in conjunction with Policy 13 “Confidential Information” and Policy 20 “Safeguarding”.

2. Terminology

The following definitions are used in this policy document.

The Act

The General Data Protection Regulations 2016 (effective May 2018)

Data

Data is recorded information, whether stored electronically on a computer, in paper-based filing systems, on the internet or on other material.

Personal Data

Information about an identifiable living individual. It includes personal, family, lifestyle, education, training, medical, employment, financial and contractual details, and can be an opinion, such as how a manager thinks an employee has performed at an appraisal.

Data Subjects

Anyone who SCRP might hold personal information about including current, past, and prospective directors, partners, employees, and volunteers.

Data Controllers

A person and/or organisation who holds and uses personal information. They decide how and why the information is used. In this case SCRP is the Data Controller.



Data Processing

Any activity involving the data, including collecting, recording, or retrieving the data, or doing work on the data such as organising, adapting, changing, erasing, or destroying it.

Data Processors

Organisations and individuals who process data on behalf of data controllers.

3.0 SCRP Data Protection Policies

SCRP uses and collects Personal Data about people with whom it deals to carry out its legitimate business purposes. SCRP collects, processes, and uses this data by following the Principles of Good Practice as identified by the Act. SCRP is a Data Controller. The Board appoints and supports a designated individual for the establishment and implementation of workplace practices and policies that are in line with the Act. The current Data Controller is shown in Appendix A and is supported by the Board.

SCRP ensures that contracts with third parties for the processing and use of data will specify the requirement that the organisation can demonstrate that it handles SCRP data in accordance with the Act. Current third-party organisations are shown in Appendix A

SCRP ensures that staff managing and processing personal data understand that they are responsible for following good data protection practice, are appropriately trained and appropriately supervised. Data protection will be an integral part of the performance review process and an agenda item on all "one to one" sessions.

3.1 Process data fairly, lawfully, and transparently.

SCRP will:

- advise the Data Subject at the time the information is requested the lawful basis for processing their data, how it will be used, our data retention periods, their rights under the Act and how and to whom to complain along with the name of our Data Controller. This will be in the form of a "Privacy Notice", a copy of which will be available on the SCRP website.
- only collect and process data for which the Data Subject has given their positive, written, opt-in consent. A record of this permission will be kept by the company.
- maintain a directory of data lists. The current directory is shown in Appendix A and is updated annually.
- regularly assess and evaluate methods and policy of processing Personal Data and their performance.



SCRCP recognises that the Act identifies Special Categories of Personal Data as more sensitive, for example race, religion and sexual orientation and more explicit conditions of use and safeguarding will be applied for these categories.

SCRCP collects and processes data relating to people under the age of 16 in very limited circumstances, for example, photos of Go-Learn sessions. The ages of Data Subjects will be verified and for those under 16 positive written consent received from their parent or guardian.

3.2 Collect data only for specified, explicit and legitimate purposes.

Data will only be collected for specific and valid reasons. Data collected for one reason will not be used for any other unrelated purpose.

Our current list of reasons for the collection of data are shown in Appendix A. Should a new reason be added, the Data Controller will arrange for affected Data Users to be advised and their written permission sought. This list will be reviewed by the Board on an *annual* basis.

3.3 Collect and store data only to the extent it is adequate, relevant, and not excessive.

SCRCP will only ask for the type of data needed for the specific purpose. Appendix A sets out the current range of data type collected and is reviewed annually by the Board.

3.4 Ensure data is accurate, up to date and not kept longer than is necessary to fulfil the purpose.

-Data users and Processors will record data accurately and take reasonable steps to check the accuracy of information received from Data Subjects or anybody else.

-The Data Controller will arrange for an annual clean of all storage systems to destroy out of date information, correct inaccurate records and destroy data not relevant for future purposes.

-A record of when these updates take place will be kept.

Data will be destroyed following the guidelines set out by the Information Commissioners Office. If a request for destruction has come from a Data Subject, the default position will be to delete the data as requested, unless there is a specific lawful reason for keeping it. SCRCP will inform the Data Subject of the action taken.

Data will only be archived where there is a legal requirement such as data on current and past employees for responding to enquiries from a new employer or the Inland Revenue.



3.5 Data will be processed in line with the Data Subject's rights.

SCRP recognises that Data Subjects rights include:

- asking for access at reasonable intervals to the information held about them
- preventing processing that is likely to cause damage to themselves or anyone else.
- not having their data used for direct marketing purposes
- acting to correct, block, erase or destroy data that is inaccurate or contains opinions that are based on inaccurate data.

Requests for information will be handled courteously and the following process applied:

- Requests in writing may be made through the website or through contact with members of staff. SCRП will verify the identity of the person making the request.
- Requests will be handled by the Data Controller and responses made within one month of receipt.
- If a request is refused, the Data Subject will be told why and that they have the right to complain to the supervisory authority and to a judicial remedy.

The data protection privacy notice will advise how to contact the company and to whom.

3.6 Appropriate security measures will be employed to protect against unauthorised or illegal data processing.

3.6.1 SCRП staff will undertake the following action in their workplace with respect to Personal Data:

- Lock paper-based records away when not in use, in desks, filing cabinets or cupboards and keep keys in a safe place.
- Position computer equipment such that no one else can see an operator's computer
- Remove documents from photocopiers after they have been used.
- Clear computer screens and password protect and lock documents away when vacating desks.
- Protect offices from unauthorised visitors and lock when not in use.
- Choose a secure computer password, change it monthly and never give anyone their password or use another person's password.



-Only use authorised software

-Always use BCC when emailing to lists unless previous agreement from all participants.

-Use appropriate security measures when using portable equipment such as laptops and mobile phones away from the workplace.

3.6.2 Data Breaches

SCRIP will set up procedures to detect, report and investigate a personal data breach. When the data breach may result in a high-risk to the rights and freedoms of the individual(s), SCRIP will inform the people affected and the Information Commissioner's Office within 72 hours of becoming aware of the breach. If a member of staff becomes aware of a data breach this should be reported immediately to the Data Controller who in turn should make the Board aware.

3.7 Transferring data outside the European Economic Area (EEA)

SCRIP will ensure that data is not transferred outside the EEA without suitable safeguards.

4 Review and Audit

The Board will undertake an audit at least once a year to include:

- A review and update of all information contained in Appendix A
- Identification of any data breaches that have occurred and the action taken.
- Address any issues outstanding that have arisen, including those from staff performance reviews and "one to ones".
-

Additionally, members of the Board may undertake sample spot checks of the contents of individual data lists during the year.



Appendix A

SCRP Data Information

Update May 2018

Data Controllers

SCRP CIC is a Data Controller and Fiona Morton is the designated individual for the establishment and implementation of workplace practices and policies that are in line with the Act supported by the Board of SCRП CIC.

Data Processors

Current SCRП Data Processors are:

| | |
|------------------|---|
| Payroll SCRП | Trevor Field, Finance & Fundraising Officer |
| Pension Provider | Legal & General |
| IT support | PS Technology |

Directory of Lists: Internal

| |
|---|
| The Stakeholder Advisory Board |
| The Marshlink Steering Group |
| The Redhill/Reigate Steering Group |
| The Uckfield-Oxted and East Grinstead Line Steering Group |
| The Arun Valley Line Steering Group |
| The Seaford to Brighton Line Steering Group |
| The North Downs Line Steering Group |



Southeast Communities Rail Partnership CIC



| |
|---|
| The Sussex Coast Line Steering Group |
| Hastings to Tonbridge Line Steering Group |
| Volunteer Directors |
| SCRP CIC Employees |
| Newsletter distribution list |

Directory of Lists: External

| | |
|------------|-----------------|
| Details | Company |
| Pensions | Legal & General |
| IT Support | PS Technology |

Purposes for Using Data

| |
|--|
| Circulation of Newsletters |
| Details of Meetings including agendas and minutes |
| Forwarding of relevant information from partners and volunteers. |
| Staff information for payroll |
| Staff information for pensions |
| Writing up case studies (Active Access for Growth programme) |
| Press releases and posts on SCRП website and Twitter, including photos |
| Staff personal details kept for Personnel and Appraisal purposes. |

Type of Data Collected

| | |
|-----------------------|--|
| Name | |
| Company/ Organisation | |
| Email address | |
| Phone numbers | |



Southeast Communities Rail Partnership CIC



| | |
|--------|--|
| Photos | |
|--------|--|