RCS

# Rural Community Services (West Cheshire)
# Data Protection Policy

## 1. Introduction

Rural Community Services (West Cheshire) (RCS) regards the lawful and correct treatment of personal data as very important for the successful management and delivery of services and the continuing confidence of the people with whom we deal.

RCS collects and uses personal data about its staff, service users, volunteers, applicants and Trustees. It has a legal obligation to comply with all appropriate legislation in respect of Data Protection, including the General Data Protection Regulations (GDPR) from May 2018. This Data Protection Policy shows how RCS will meet its legal obligations in respect of the GDPR.

## 2. The purpose of this Policy

The purpose of this policy is to ensure that RCS staff, Trustees and volunteers who handle personal data are clear about RCS responsibilities and commitments in respect of data protection and the principles of the General Data Protection Regulation. Failure to adhere to the legislation could result in reputational damage and action being taken against RCS, its staff, trustees and volunteers.

## 3. Scope of this Policy

Information falls within the definition of the Directive if the information in question is 'data' (either processed by automatic means or non-automated processing within a filing system) and the 'data' is 'personal data' if it relates to an identifiable individual.

This Data Protection Policy applies to all personal information obtained and processed by RCS employees, trustees and volunteers, whether processed electronically or as manual records.

## 4. The rights of individuals under GDPR

The General Data Protection Regulation provides the following rights to individuals with regard to data held about them from which they can be identified:

- The right to be informed
- The right to access
- The right to clarification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making.

## 5. Principles

RCS will uphold the principles of GDPR as stated in article 5 of the regulation. These principles are:

- Data will be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Data will be for explicit and legitimate purposes and will not be further processed any way that is incompatible with those purposes.
- Data will be relevant and limited to what is necessary for the purpose(s) for which they are processed.
- Data will be accurate and kept up to date. Every reasonable step should be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

- Data will be 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.
- Data will be 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.

## 6. Data Protection Responsibilities

### 6.1 Board of Trustees

- The Board of Trustees is responsible for ensuring the implementation and monitoring of RCS policy and procedures for data protection.
- RCS is registered with the Information Commissioners Office as a Data Controller. The Board is responsible for ensuring the RCS Data Protection notification is reviewed and renewed annually for all use of personal data.
- The RCS Board will put into place comprehensive but proportionate measures to ensure the protection of the personal data it holds.
- RCS Trustees are responsible for ensuring that they, their staff and volunteers have access to suitable Data Protection training and refresher training.
- RCS Trustees are responsible for ensuring that the appropriate procedures and practices are in place and are adopted by RCS personnel.
- RCS Trustees are responsible for initiating a privacy impact assessment whenever it initiates a new service that requires significant changes in the processing of person identifiable data by RCS.

### 6.2 Data Protection Officer's (DPO) Responsibilities

The RCS Board assigns responsibility for Data Protection compliance to the nominated Data Protection Officer who reports to the Board through the Information Governance Committee.

The Data Protection Officer is responsible for:

- Annually notifying the Information Commissioner about RCS's uses of personal data.
- Ensuring that an appropriate Data Protection policy for RCS is up to date.
- Acting as a central point of contact on Data Protection within RCS.
- Providing the appropriate guidance and direction on matters of data protection to the RCS Board of Trustees.
- Ensuring compliance with individual's rights, including subject access.
- Ensuring any infringement or unlawful disclosure of personal data is investigated and appropriately dealt with.
- Ensuring any data breach that risks damage to the rights of individuals is reported to the appropriate authority within the required time period.

### 6.3 General Responsibilities

- RCS employees (including volunteers, temporary staff and contract staff) are subject to Data Protection compliance and are responsible for compliance with this policy and its associated procedures. They are accountable via personal liability.
- RCS employees (including volunteers, temporary staff and contract staff) will ensure that all personal information obtained by RCS will be held and processed in a professional manner in accordance with the GDPR.
- RCS Trustees, employees, volunteers, temporary staff and contract staff have a responsibility to inform the Data Protection Officer of any new use of Personal Data as soon as possible after it has been identified.

- RCS Trustees, employees, volunteers, temporary staff and contract staff have a responsibility to inform the Data Protection Officer of any subject access request received within 48 hours.
- RCS Trustees, employees, volunteers, temporary staff and contract staff will respond promptly and helpfully to any data subject access request. RCS will ensure that subject access requests are reported and responded as soon as possible, within no more than one month of receipt.
- RCS Trustees, employees, volunteers, temporary staff and contract staff will ensure that all personal information is obtained, held and disclosed in a secure manner and not disclosed to unauthorised persons.
- They are responsible for ensuring personal information held electronically on laptops and other portable devices are transferred securely in accordance with the requirements of this policy and its associated procedures.
- RCS Trustees, employees, volunteers, temporary staff and contract staff are responsible for reporting any breaches of the General Data Protection regulations without delay.
- RCS Trustees, employees, volunteers, temporary staff and contract staff are responsible for responding promptly to requests from data subjects for personal data to be amended or deleted and for recording their actions.

**7. Confidentiality**

RCS will treat the personal data it collects as confidential and will ensure processes are in place so that data it collects is accessible only to those staff and volunteers with a need to know.

RCS will not share the personal data it collects about members or volunteers without the consent of the data subject, except in the event of an emergency or where there are strong concerns about the safety or wellbeing of the data subject.

**8. Consent**

RCS will establish and record the legal basis of all categories of the personal data it processes.

Where consent is used as the legal basis for processing personal information, RCS will ensure that its consent procedures meet the requirements of the GDPR. RCS will ensure there is full transparency around what personal data it holds and how it processes that personal data. This includes circumstances where RCS is under a contractual obligation to share personal data for monitoring and other purposes.

**9. Special categories of data**

RCS will process ‘special category’ data (previously referred to under the Data Protection Act as ‘sensitive personal data’) only in limited circumstances.
Special category data is defined in the GDPR as:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life;
- sexual orientation.

RCS staff will work with the RCS DPO to ensure they process data that falls under the special categories only in accordance with the conditions listed under the GDPR.

**10. Data security**

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss or release of data, destruction or damage.

RCS will take appropriate and proportionate technical and organisational measures to ensure the protection of the personal data it processes.

**11. Data Breaches**

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

RCS will ensure that staff and volunteers know what a data breach is and what to do if they become aware of a data breach.

Any data breach will be notified via the DPO and the trustees to the relevant supervisory authorities within 72 hours of RCS becoming aware of it.

**12. Subject Access Requests**

Individuals will have the right to obtain confirmation that their data is being processed and will have the right of access to their personal data.

Upon request, RCS will ensure it responds to subject access requests as soon as possible and within one month of the request being received. In exceptional circumstances where it is not possible to provide a response within a month, RCS will inform the individual and explain why an extension of no more than one month is necessary.

RCS will provide a copy of the requested information free of charge.

**13. Inspection and Audit**

Subject to reasonable and appropriate confidentiality undertakings, RCS will permit its commissioners or the Council or the Authorised Officer to inspect and audit its data processing activities related to a current contract, in order to verify that RCS is in full compliance with the Data Protection Act and the GDPR.

Date ratified by the RCS Board: 31st January 2018
Effective from: 18th May 2018
Review date: January 2021
Policy owner: RCS Data Protection Officer

**Board of Trustees** **January 2018**