

Policy: Data Protection

In accordance with the Data Protection Act 2018

and General Data Protection Regulation (GDPR) 2018

Trustees have overall responsibility for ensuring The Rural Coffee Caravan (RCC) complies with all legal obligations regarding data protection.

Purpose of Policy: The RCC does not process personal data, but data is held within the charity. This policy is to comply with all legal requirements regarding data protection and to follow good practice in this area. It is to protect visitors, staff and other individuals that we have contact with.
The policy will demonstrate RCC's commitment to respect the rights of individuals, and to be transparent and honest. It will also provide guidance to employees, Trustees and Committee Members.

Scope of Policy: applies to all locations, employees, volunteers, Trustees and Committee members of the RCC.

Data Protection Officer (DPO): Michael Osborn. Appointed by Trustees at their meeting dated 28th Sept 2018

This official will be responsible to The Treasurer for all day-to-day matters regarding the charity's adherence to this policy and for ensuring that data protection matters are an agenda item for Trustees & Committee Meetings whenever appropriate. This person will be responsible for ensuring the Data Protection Policy forms part of RCC's policies portfolio and carries out reviews as necessary and at the policy review date. The role will ensure that the policy is available to existing employees, volunteers, Trustees and Committee Members; provide advice on training; and ensure it is covered in any future inductions.

Right of Access requests: The Chair of Trustees will be responsible for processing all Rights of Access requests, taking legal advice if necessary. Such requests must be in writing and generally free of charge except where they are manifestly unfounded, excessive or

repetitive when a charge can be made. Response will normally be made within 1 month of the request.

Overall data security policy: Data stored within RCC will be limited to that which is adequate, relevant and not excessive. It will be kept accurate and held for no longer than is necessary and stored securely. Employee IT will use password protected software and locations will be locked when unattended.

Trustees may, from time to time, take responsibility for data. An example would be the listing of nominated drivers and their details. Data captures of this nature, and the associated update processes, are necessary to ensure we operate responsibly. Such data falls within that which is covered by this policy and the Trustees must abide by the policy.

Hard data that contains personal data of any description held in any location must be kept securely in a locked cupboard or cabinet. Hard data containing personal data held at Head Office will be stored in a locked cupboard accessed only by the Chief Executive Officer (CEO) and the Administrator within the office which is locked when unattended.

Any issue raised to an RCC Volunteer that requires the recording of personal details, must be referred by the volunteer to the attendant RCC member of staff.

Any request received for personal data referring to any person employed by, or associated with, the RCC must be referred to that person before any information or data is discussed with the enquirer.

Personal data held as hard copy will be shredded when disposal is required. This will apply to the Trustee's details when they step down.

The taking of photographs to be retained by RCC at visits and events is under the control of the CEO, the Community Engagement Officers, the Marketing & Communications Manager or a Trustee. Specific agreement to the photo must be obtained from those individuals included prior to the taking of the photo and its potential use explained. Such agreement can be verbal.

The RCC's use of social media is strictly controlled and restricted to the CEO and two designated employees only. It is not permissible for Trustees, Committee Members, volunteers or any other employee, to post on any social media platforms anything relating to the RCC, associated agencies, events, or activities. Should any such requirement become known or wanted it must be highlighted to the CEO who will vet the proposed post to ensure compliance with our data protection policy and undertake the posting.

Dealing with a Data Breach: Any data breach (or suspected breach) must be reported to the DPO immediately who will take responsibility for dealing with the matter. All breaches must be investigated immediately and reported to the Chair of Trustees. Action agreed as necessary to resolve the situation must be implemented immediately. The DPO will report on all data matters, including breaches, at Trustee and Committee meetings where a record of the breach and the actions taken will be documented. The effectiveness of the corrective action will be measured, and appropriate changes made to policies and operations.

Information held, and Policy on, Data held by RCC:

Data	Why held?	Retention and Disposal
Personnel files.	To comply with legal requirements regarding employment. Record of employment history, and compliance, where required, of employees. Records include address, contact details, bank details, application form, licences held, DBS check.	Held as printed documents in Head Office in individual personnel files. Stored in a locked cupboard accessed only by the CEO and the Administrator within the office which is locked when unattended. If employees leave, their record will be archived for three years and then shredded.
Volunteer records.	The charity relies on volunteers to be available for visits and events. Records include contact details, driving licence and DBS check.	When required, held as printed documents in Head Office in individual volunteer files. Stored in a locked cupboard accessed only by the CEO and the Administrator within the office which is locked when unattended. If a volunteer no longer wishes to be involved their record will be shredded immediately.
Emails	Normal course of business.	If email contains personal information it should be deleted as soon as the content matter is concluded.
Contacts	Generally email addresses to facilitate easy contact. Personal details of Trustees.	Email addresses retained on office system and phones – both password protected. Policy is to keep these secure, updated and deleted when no longer relevant. Internal contact details are maintained for contact and Charity Commission reasons. These are held on password protected office systems in locations locked when unattended.
Feedback forms	To evaluate the effectiveness and attraction of events for both attendees and agencies.	No personal data is requested on the forms, but if individuals do give details this should be anonymized during the evaluation process and the form shredded.

Location and contact details of villages visited and GAF venues	To maximize impact of our work, record activities and facilitate communications	Policy is to keep these secure, updated and deleted when no longer relevant. Data is held on password protected office systems in locations locked when unattended.
Agencies we work with and their contact details, including their associated representatives.	To ensure forthcoming events are known to agencies so they can plan attendance which ensures visitors have maximum access to them. To maintain contact with organisations to whom we signpost	Only details that are essential to normal business will be kept. Email addresses of contacts retained on office system and phones – both password protected. Policy is to keep these secure, updated and deleted when no longer relevant. We will respect agencies formal or implied policies on data protection.
Photographs	For publicity, website, social media, promotion of our work.	Catalogued and held within the CEO's or Community Engagement Officer's password protected IT system. Held for as long as they are appropriate to our work and afterwards deleted.
Expense claim forms	For processing and payment, then as record for independent assessment of accounts.	Held as current documents until the year end independent assessment of the charity's accounts. Archived for seven years. All expense claims are held as printed documents in Head Office which is locked when unattended.

Policy Date: June 2018: Last review date: Aug 2024 Next review: Aug 2027

This policy is displayed on RCC website and review dates should also be updated on the on-live version.