



# Data Protection Policy

May 2018

## Personal Data and the GDPR 2018

---

The government has created a new Data Protection Act (2018) which replaces the 1998 Data Protection Act. General Data Protection Regulation (GDPR) came into force on May 25, 2018, and was designed to modernise laws that protect the personal information of individuals.

This policy explains how this data is collected, processed, stored, accessed, and reviewed in order to meet Reaching People Data Protection standards and comply with the General Data Protection Regulations (GDPR) and Data protection Act 2018.

In order to operate, Reaching People (RP) needs to gather, store and use certain forms of information about individuals. \*Personal Data means any data which, together with other information held or likely to be held by the Company, identifies a living individual. This includes any opinion about the individual and any indication of how Reaching People intends to treat the individual.

This policy ensures that Reaching People

- Protects the rights of individuals including our members, staff, service users and volunteers
- Complies with data protection law and follows good practice
- Protects RP from the risks of a data breach

The Data Protection Act 1998 (the Act) gives individuals certain rights. It also provides that those who record and use personal data must follow the eight enforceable data protection principles.

The GDPR principles provide (in summary) that personal data must be:

- Fairly and lawfully processed
- Obtained or processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than necessary
- Processed in accordance with individuals' rights
- Secure
- Not transferred to countries outside the EEA without adequate protection

Some personal data is defined as 'sensitive' in the Act and can only be processed under strict conditions. Sensitive personal data is data falling into the following seven categories:

- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs;
- Trade union membership;
- Health;

- Sex life;
- Criminal proceedings or convictions.

Reaching People differentiates between the data controller and data processors, as defined in the Data Protection Act, and ensures that, as a data controller, it has in place the appropriate monitor, review and audit procedures to ensure that any processing of personal data, for which Reaching People is responsible, complies with the Act.

**Data processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Processing** in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

A Data Sharing Protocol will be agreed and signed between Reaching People, as data controller, and any member required to process data.

If a member of staff of either Reaching People or a Reaching People member is in breach of this policy, they may be subject to disciplinary action which could lead to dismissal. A breach of the Act means that the individual, their organisation and/or Reaching People may be prosecuted.

Related policies and procedures included, Equality, IT, Confidentiality.

### [Subject Access Request](#)

All subjects are made aware of the process to view their personal data in line with GDPR. This policy is readily available to all on the Reaching People website and on request.

## [PROCEDURES:](#)

### [Right to Data Access/Deletion request Procedure](#)

The overriding majority of personal data held by Reaching People (RP) will fall into one of the four following categories:

1. All individuals are informed, at point of data collection, that they have a right to request access to see their data and how to start this process should they wish.
2. All individuals are informed, at point of data collection, that they have a right to have corrections made to any identified errors in their collected data.
3. All individuals are informed, at point of data collection, that they have the right to request deletion of their data and the steps they will need to take enable this.
4. RP office collates and processes data relating to staff (current and previous – in line with project requirements), Trustees (in line with Companies House and Charities Commission requirements) and will record and process individual's data given by RP members/staff members who use their own personal email address(es), telephone number(s) and social media details in relation to their work.
5. Beneficiary data relating to specified RP projects. Each project will have its own sub-set of procedures, however overall responsibility for data access/deletion requests will be held by RP CEO or recorded designated individual (for RP held projects).

## Right to Data Access (Subject Access Request)

6. Anyone who has personal information recorded and stored by RP is able to request access to view the data held. To do so, they will need to submit the request in writing to CEO of RP, Third Floor, 15 Wellington Street, Leicester, LE1 6HH.
7. RP will respond to this request within one calendar month of receipt of the letter.  
There will usually be no charge\* for the subject being given access to their own data.
8. All requests received will be recorded on the central **Subject Requests log**, along with dated actions taken.
9. \*a nominal charge may be made, or RP may refuse access to data held, should there be numerous/repeated requests from one individual, particularly where it is clear to both RP and the individual that there has been no cause for data held to be amended in any way since last access request. Refused requests must also be logged on the central **Subject Requests log**.
10. RP can withhold personal data where disclosing such data may adversely affect the rights and freedoms of others.
11. Where a request is refused, the subject must be informed in writing within one calendar month of the reason(s) for such refusal and that they have the right to complain to the Chair of RP at the above address and also to the ICO (information Commissioners Office) and will be directed to the appropriate website.

## Data Correction/Data Deletion Request Procedure

12. Where a subject has viewed their data and seen inaccuracies/inconsistencies in the data held, the subject has a right to have this data corrected. RP will liaise with the subject to gather evidence to ensure that any inaccuracies/inconsistencies are corrected. The **Data Protection correction form\*** must be completed and signed by both RP and the data subject.
13. Should the subject choose they can, at any time, submit a Data Deletion request in writing stating the reasons they wish all of their personal data/named parts of their personal data to be deleted.
14. RP will review the related data concerned to confirm that this is “lawfully required”\* in order for the data subject and RP to work together effectively. The Data Deletion request must be recorded on the central **Subject Requests log** along with whether the request has been confirmed or denied.
15. **If request successful:**  
RP will write to the individual and confirm that the specified data deletion will take place immediately. The letter actions to take place within one calendar month of the subject deletion request being received.  
  
**If request denied:**  
RP will write to the individual detailing the lawful reasons for continuing to hold the data. This letter to be sent within one calendar month of the subject deletion request being received.

16. If, following request denied and explanation given by RP, the subject still wishes the data to be deleted, RP CEO should write to the individual and agree to delete the data and confirm any repercussions this will have on the continuing relationship. A second copy of the letter must be enclosed for signature and return by the subject. Once this has been signed and returned, the relevant data must be deleted within one calendar month. A letter must be sent to the subject confirming when this action has been carried out.
17. The CEO should take the ongoing Subject Request to each LVSRA Board meeting where actions will be reviewed by the chair and countersigned when satisfied.

## Reaching People Data Capture and Processing Procedure

All staff involved in collecting, collating and/or processing data will receive training input on data protection and GDPR requirements. Signed confirmation of this will be held on their HR file.

### Data Capture

1. All personal data\*(see page 1) must be obtained with the individual's consent (evidenced).
2. The individual must be informed of the following:
  - How the information will be held (paper/online/database/telephone record etc)
  - Who it will be shared with and for what purpose
  - The lawful basis on which it is being collected
  - How long it will be held and why
  - How an individual can request access to their data that RP holds
  - That they have the right to request that any inaccuracies found be corrected (see separate Data Access procedure)
  - That they have a right to request that their data be deleted
3. Physical (paper) data must be stored securely in locked filing cabinets and marked with an expiry date. Expiry dates will vary dependant upon the data held (see separate Data Review & Retention procedure).

### Data Processing

4. The Data processor will ensure that the data captured/held is in line with the data retention policy before proceeding to process the data.
5. Only the data captured that is required for its stated purpose will be processed. Any unwanted data at this stage must be destroyed (see data retention process).
6. Only RP approved methods/systems will be used for processing data and accessible only to those requiring to view such information (see Data Access procedure).

7. Staff member must raise any data concerns e.g. regarding inappropriate data capture/unnecessary processing with the CEO who will investigate the concerns at the earliest opportunity.
8. Where non-RP staff are used to process data, all such individuals must be familiarised with RP GDPR procedures, or equivalent procedures relating to a specific RP project. This includes any contractor(s) retained to undertake bespoke pieces of work/research on behalf of RP.
9. All persons undertaking data capture or processing for or on behalf of RP will sign to confirm that appropriate training/induction to data procedures has taken place, along with signature of privacy/non-disclosure agreements

## Reaching People Data Review and Retention Procedure

### Data Procedure Review

1. All Data Protection procedures will be reviewed annually to confirm that they remain appropriate for the types and levels of data collected by RP.
2. Any required changes to procedures should be drafted and discussed with the CEO and other relevant staff.
3. Agreed changes should be made to the procedure and subsequent version number given. The original procedure should be kept but archived to retain a data procedure trail. This will assist in showing that appropriate action has been taken in a timely manner to eradicate extraneous data which is no longer purposeful.

### Date Review, Retention and Expiry

#### Review

4. At the same time, all strands of data collected will be reviewed to ensure that no characteristics continue to be captured unnecessarily. Any strands that are identified as no longer relevant or having lawful purpose should be raised with the CEO and a decision taken as to whether it is therefore appropriate to delete such data and data strands.
5. Data must be retained for the minimum period possible and data held should be reviewed annually as a minimum to confirm that data held is still being held purposefully.
6. In determining the length of time to retain records, attention must be made to any current legal requirement relating to data retention in respect of:
  - Employment law
  - HMRC/Tax purposes
  - Other financial/company accounting purposes

- Requirements of any funders (under whose specific project the data was captured)
7. Once it has been decided on action to be taken with reviewed data, the outcome should be recorded on the **Data Review Decisions log**.

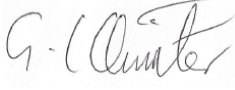
### **Retention**

8. If data is to be retained, the end retention date (i.e. expiry date) must be entered onto the **Data Review Decisions log**.
9. Where paper records exist for this data, these shall be boxed up, sealed and stored securely; a label being secured to the outside of the box detailing the date for disposal. If full paper records exist, it will be necessary to consider whether the same data is still required to be held on computer. Where it is considered appropriate to only retain paper records, all related computer records should be deleted as below (*expiry and disposal section*).
10. Once the due disposal date is reached for the paper records, all documentation held must be disposed of through secure document disposal waste management.
11. Any residual computer records that were kept (see 9 above) must also be thoroughly deleted at this point.
12. **Date Review Decisions log** should be completed thus showing a full audit trail of the data set.

### **Expiry and disposal**

13. If reviewed data is to be disposed of, this must be confirmed with the CEO.
14. Data held on computer must be deleted fully from the system where it is held. Full subject data should only be stored in one place, however all related email addresses/old emails, phone numbers must be deleted at the same time, unless ongoing contact remains.
15. Any related paper records must also be disposed of in a secure manner (e.g. either shredded or by approved secure document waste management).
16. **Data Review Decisions log** must be completed thus showing a full audit trail.
17. If the latest contact seems to be necessary to continue after the original lawful purpose has passed (see 14 above), ***fresh written permissions need to be obtained*** from the individual to allow the appropriate pieces of data to continue in place. This will constitute new data and should be treated as such.

## Document Control

Approved by:	<b>G Quilter</b>	
Signature:		
Board Responsibility:	<b>Chair</b>	
Review Date:	May 2019	
Summary of changes	Document is current and in line with GDPR for annual review in the first instance as this is new legislation	