WEB/RISC
Data Protection policy 2019

Review Date, 3 years from adoption date, due: 2022

WEB/RISC
Registered Charity no. 293799
35 – 39 London Street
Reading
RG1 4PS

t. 0118 9586692
f. 0118 9594357
e. admin@risc.org.uk

WEB/RISC Data Protection policy 2019

This policy applies to everyone at WEB/RISC. This includes paid employees and all volunteers, and in this way also applies to trustees. For convenience, the word staff has been used throughout this policy to apply to everyone.

In this policy the following terms are used based on their definitions in the Data Protection Act 2018 (which incorporates the General Data Protection Regulations (GDPR) 2018)

Personal Data: This is any information from which a living individual can be identified, either directly or from other information held by or likely to be held by WEB/RISC. The Data Protection Act 2018 (DPA 2018) applies only to such personal data.

Sensitive Data: The DPA 2018 recognises two types of sensitive data which require more protection because it could create more risks to a person's fundamental rights and freedoms, such as unlawful discrimination:

- Special Category Data: this is any personal data consisting of information relating to an individual's racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, genetics, biometrics (when used for ID purposes, such as fingerprints) physical, mental health or sexual life. This may only be processed under special conditions such as employment purposes or for monitoring equality of opportunity or treatment.
- Criminal Offence Data: this is a list of criminal convictions or offences. This is now heavily restricted and can only be processed in limited circumstances such as where there is express consent, to protect an individual's vital interests, or if there are legal proceedings.

WEB/RISC normally requires the explicit consent of a data subject to process special category data or criminal offence data.

Data Subjects: This is an individual who is the subject of Personal Data held by WEB/RISC.

Data Controller: This is the person who is legally responsible for processing personal data.

Data Processor: Is any person who collects or processes the data on behalf of the Data Controller: eg staff and trustees, volunteers, external agencies.

Introduction: The Data Protection Principles

RISC recognises the importance of safeguarding personal privacy when dealing with information about Data Subjects. We need to obtain, store, process and sometimes disclose personal data in order to carry out the legitimate activities of the organisation. WEB/RISC also needs to keep certain information about its staff and other users.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, WEB/RISC must comply with the Data Protection Principles, which are set out in the DPA 2018 which are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

All staff that collect, process or disclose any personal information must ensure that they follow these principles at all times. In order to achieve this, this policy sets out WEB/RISC's procedures and the responsibilities of staff in implementing them.

RISC is committed to providing information and training on Data Protection to all staff who require it. This policy will be included in the induction for all new staff and volunteers. If any staff are unsure about any aspect of this policy or its implementation, they should take the matter up with their manager or the nominated member of staff.

Any staff who has concerns that WEB/RISC may be in breach of this data protection policy should raise the matter with the nominated member of staff.

Obtaining Personal Data

We obtain Personal Data from people who, in our reasonable opinion, are reliable sources. Such sources include: employees, volunteer workers, trustees course/conferences organised by RISC and members of the public requesting information or services.

- RISC will only collect data that is relevant to the carrying out of the legitimate purposes and functions of the charity in a way that is not prejudicial to the interests of individuals.
- All data on individual subjects will be treated in a consistent way.
- Subjects will be informed about how WEB/RISC will store and use the data at the time of collection. This will require a ***data protection statement*** to be sent in all written requests for data, including web and email communications, that should include at least the following:

  "If you complete this form WEB/RISC will store and process your data in accordance with the requirements of its Data Protection Policy and in keeping with the Data Protection Act 2018
- When ***sensitive data*** (this includes special category data or criminal offence data) is collected a statement must also be included in all written forms which explains why the data is being collected, how it is to be processed, and whether anyone external to WEB/RISC will have access to it. **Explicit consent** for the collection and processing of sensitive data must be obtained from the data subject, usually by means of a tick-box or a signature stating agreement. For special category data this consent is not necessary if the ***only*** purpose of the data is for equal opportunities monitoring, though the statement must make this fact explicit.
- Where WEB/RISC intends to use data for its main purposes, such as providing advice or placing volunteers, subjects will be deemed to have given their data for this purpose.
- RISC will strive to ensure that data collection is as accurate as is possible, given the methods used in collection.
- RISC will strive to ensure that sensitive data is accurately identified on collection so that the proper procedures for processing the information can be observed.

When collecting personal subject data, WEB/RISC staff has the following responsibilities:

- Staff are responsible for ensuring that data collected is accurate and complete.
- When collecting personal data in writing, staff should ensure that an appropriate data protection statement is included, such as the one above.
- Staff are also responsible for identifying sensitive data when collected. Staff must ensure when collecting sensitive data that the rules outlined above are followed; namely that an appropriate statement is included on any written material and that the data subject has given explicit consent in writing, unless it is not required.
- Staff are also responsible for ensuring that the information about them that is held by WEB/RISC is accurate.
- All personal information should be dated at the time of collection so that records can be archived at an appropriate time.

Data Storage and Processing

The DPA 2018 applies to personal data stored in both electronic databases and ordered manual filing systems. Processing is the term used to mean any action that is performed on the data, and includes such processes as filing, transferring, and also destroying. Any data processing will only be allowed where there is a clear rationale for the activity, which meets the DPA 2018 criteria. As such:

- RISC only holds data that is relevant to the carrying out of the legitimate purposes and functions of the charity in a way not prejudicial to the interests of individuals.
- RISC also holds information about each member of staff, volunteer and trustee which is both necessary and adequate for the particular engagement.
- RISC may also occasionally process Personal Data on behalf of other, independent, Data Controllers. When it is operating as a Data Processor, WEB/RISC applies the same technical and organisational security measures to the data processing function, as it would use in its capacity as Data Controller.
- RISC will endeavour to ensure that any information held is both accurate and timely, and is held in an environment as secure as possible.
- A list of data stores will be maintained, and forms an appendix to this document.
- All databases and ordered manual files containing personal data will be kept up to date and will have an agreed archiving policy. This will be that inactive records will be destroyed after five years, unless there is an internal procedure or an overriding legal obligation that requires otherwise. Exceptions to this 5-year policy due to internal procedures will be listed in the appendix to this policy.
- RISC does not transfer personal data outside of the European Economic Area (which is the area the Information Commissioner considers safe). The only possible exception to this is the WEB/RISC web site. Consent must be obtained from the individual concerned for personal data to be included on the web site. WEB/RISC staff will be deemed to have given their consent for the use of personal data that is relevant to their work. For anyone else explicit consent must be obtained from the data subject in writing.

Any staff that process personal data must understand the following points:

- RISC staff will be responsible for ensuring that all regular data care procedures are fully and conscientiously followed. They are also responsible for any records they keep in any ordered filing systems.
- Staff must ensure when processing sensitive data that the explicit consent, in writing, of the individual concerned to the processing of such data has been received.
- Staff has a responsibility to check that data no longer required for the legitimate purposes of WEB/RISC is regularly purged. In the absence of any archiving policies stating otherwise, and as a general rule, personal data should not be kept for longer than five years without a legitimate reason.
- All individual data will be kept secure, by regular office security procedures or through the controls over the computer network. All personal data will be stored in a secure location and precautions will be taken to avoid letting data become accidentally disclosed.

- If any member of staff has any concerns about the security of personal data at WEB/RISC, the issue should be raised with the line manager and/or nominated person.

Disclosing personal data

Sometimes it is necessary for WEB/RISC to disclose personal data to third parties in order for the organisation to operate on a day-to-day basis. WEB/RISC will not allow data collected from subjects to be disclosed to third parties except in circumstances, which meet the requirements of the DPA 2018.

RISC will only disclose personal data to third parties for the following reasons:

- Data disclosed as part of the usual operations of WEB/RISC, for instance in the placement of volunteers by the Voluntary Action Centre, or providing an external trainer who is running a training course with details of the participants. Where such legitimate transfers take place, the Data Subject will be deemed to have given consent.
- Data disclosed to persons legally entitled to the information e.g. Companies House and Charity Commission for England and Wales.

Data disclosed to individuals or companies who provide WEB/RISC with electronic data processing services or other professional or management services such as payroll administration, pensions, insurance, health or legal services. Where data are passed to a third party for processing, WEB/RISC will ensure control of the data will not be allowed to move to the third party, and that the third party complies with the principles laid out in the DPA 2018.

All staff should be aware of the following points:

- Where sensitive data is involved, staff should not disclose this data to outside agents except in cases agreed by the HR Administrator.
- All staff have a duty to protect personal data from accidental disclosure. This involves abiding by any confidentiality or security arrangements that are in place. It also involves staff using some common sense, such as: not give out passwords to other people, reporting any potential risks to the nominated person, and in particular taking due care to ensure that data is not left about in places accessible to the public or by other people who are not WEB/RISC staff.
- If staff receive any request for data based on a legal requirement, eg. from Police, Inland Revenue or other body, it must be put in writing. The nominated member of staff must be informed and the request checked against the advice of the Office of the Information Commissioner before data are disclosed.

Subject Access to Personal Data – "The Right of Access"

Any person has the right to know what personal data WEB/RISC is keeping about them, in order to verify it and correct any inaccuracies, and a right to obtain a copy of this personal data and any supplementary information. As such WEB/RISC will provide information in response to any reasonable such request. This only applies to personal data and not about data relating to someone else (unless they are acting on someone's behalf).

RISC will operate the following practices regarding subject access to personal data:

- Anyone wishing to exercise this right should contact WEB/RISC in writing, and this request should be forwarded to the nominated staff member.
- If any volunteer or staff member believes that someone has asked them for access to their personal data, this volunteer or staff member should let their supervisor or the HR Administrator know as soon as possible including the date of the request and contact details for the individual. The Supervisor or HR Administrator will then contact the individual to clarify their request.
- The HR Administrator will keep a record of subject access requests, which includes date of initial request, any clarification sought and date by which the request must be completed. RISC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 days. If due to the size or detail of the request it is anticipated that we cannot reasonably respond fully to you in this time, we will write to you and let you know a date by which we can gather the full data of your request.
- Staff will make every effort to ensure that immediate action is taken when subject data access is requested.
- A letter will be sent to the subject stating WEB/RISC's policy on subject access. This will include the above statement about complying to a request within 28 days or identifying a further period if this is not reasonably practical due to the size or complexity of the request.
- A search will be set up of all data stores to ensure that all relevant data will be collected and collated ready to present to the subject. The search will include all electronic data and ordered manual files if required. Information on data collection, storage, processing and transfer may be required.
- The data will be offered to the subject on WEB/RISC premises with a staff member on hand to help with any queries or interpretations. If the subject is unable to visit WEB/RISC premises, alternative arrangements can be negotiated.
- WEB/RISC will not charge you to access your personal data however if the request is excessive or repetitive we may charge a fee to cover our reasonable administrative costs for processing your request. In such cases we will let you know what this will be before processing.

Complaints and Queries:
RISC will respond to any complaints as quickly and responsively as possible. Any letter we receive in relation to the Data Protection Act, that questions our policy and/or procedure will be dealt with immediately. Records will be kept of all correspondence for 5 years.

Breaches of this policy:
It is possible that any deliberate breach of the data protection policy by WEB/RISC staff may lead to such action as: disciplinary action, suspension from duties, or in extreme circumstances even a criminal prosecution.

Updating this policy:
This policy will be updated from time to time in order to incorporate any new or revised codes of practice or future amendments to national/international legislation and Data Subjects will be notified of the changes wherever possible.