DATA PROTECTION POLICY

1. Introduction

1.1. This Policy sets out the obligations of Rise regarding data protection and the rights of customers, business contacts, employees etc. (**data subjects**) in respect of their personal data under the UK General Data Protection Regulation (the **Regulation**) and the Data Protection Act 2018.

1.2. The Regulation defines **personal data** as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. By natural person, it means a person who is alive.

1.3. This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by Rise, its employees, agents, contractors, or other parties working on its behalf.

1.4. Rise is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

2.1. This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures

required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) 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, using appropriate technical or organisational measures.

3. Lawful, Fair, and Transparent Data Processing

3.1. The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1. Rise collects and processes the personal data set out in the Register of Processing Activity (ROPA). This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties.

4.2. Rise only processes personal data for the specific purposes set out in the ROPA or this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

4.3. We will share your personal information with third parties only where required by law, where it is necessary to administer the working relationship with you or

where we have another legitimate interest in doing so.

5. Adequate, Relevant and Limited Data Processing

5.1. Rise will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up To Date

6.1. Rise shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

7.1. Rise shall not keep personal data for any longer than is necessary considering the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay. Rise operates a Data Retention Policy to support this process.

8. Secure Processing

8.1. Rise shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

8.2. Rise will limit access to personal data to those employees, agents, contractors, and other third parties who have a business need to know. They will only process personal data on our instructions and they are subject to a duty of confidentiality. Rise has put in place procedures to deal with any suspected data security breach and will notify affected data subjects and any applicable regulator of a suspected breach where it is legally required to do so.

9. Accountability

9.1. Rise's Data Protection Lead is the Business & Strategy Director.

9.2. Rise shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the company, its data protection lead, and any applicable third-party data processors;

b) The purposes for which it processes personal data;

c) Details of the categories of personal data collected, held, and processed by Rise; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data

from Rise;

e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f) Details of how long personal data will be retained by the company; and

g) Detailed descriptions of all technical and organisational measures taken by Rise to ensure the security of personal data.

10. Data Protection Impact Assessments

10.1. Rise shall carry out Data Protection Impact Assessments (DPIAs) when and as required under the Regulation and record these in the relevant project/programme storage areas. DPIAs shall be overseen by the Charity's CEO and shall address the following areas of importance:

a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

b) Details of the legitimate interests being pursued by Rise;

c) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

d) An assessment of the risks posed to individual data subjects; and

e) Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

10.2 Rise uses a template DPIA which is the recommended template from the ICO. This is stored on Rise's internal IT systems.

11. The Rights of Data Subjects

11.1. The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

d) The right to erasure (also known as the 'right to be forgotten');

e) The right to restrict processing;

f) The right to data portability;

g) The right to object; and

h) Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1. Rise shall ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the company including, but not limited to, the identity of its Data Protection Lead;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in the ROPA) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which Rise is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the **EEA**), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);

g) Details of the length of time the personal data will be held by the company (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the data subject's rights under the Regulation;

i) Details of the data subject's right to withdraw their consent to the company's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2. The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

a) Where the personal data is obtained from the data subject directly, at the time of collection;

b) Where the personal data is not obtained from the data subject directly (i.e. from another party):

   a. If the personal data is used to communicate with the data subject, at the time of the first communication; or

   b. If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c. In any event, not more than one month after the time at which Rise obtains the personal data.

13. Data Subject Access

13.1. A data subject may make a data subject access request (**SAR**) at any time to find out more about the personal data which Rise holds about them. The company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2. All SARs received will be handled by Rise's Data Protection Lead.

13.3. Rise does not charge a fee for the handling of normal SARs. The company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1. Please see our Data Rectification Policy & Procedure.

15. Erasure of Personal Data

15.1. Please see our Data Erasure Policy & Procedure.

16. Restriction of Personal Data Processing

16.1. Please see our Data Restriction Policy & Procedure.

17. Data Portability

17.1. Please see our Data Portability Policy & Procedure.

18. Objections to Personal Data Processing

18.1. Please see our Data Objection Policy & Procedure.

19. Automated Decision-Making

19.1. In the event that Rise uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from Rise.

19.2. The right described in Part 19.1 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between Rise and the data subject;

b) The decision is authorised by law; or

c) The data subject has given their explicit consent.

20. Profiling

20.1. Where Rise uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. Personal Data & Purposes for Which it will be Used

21.1. Examples of the personal data which may be collected, held, and processed by Rise include, but are not limited to: name; date of birth; postcode; ethnicity; gender; medical conditions; bank account details; pension information.

21.2. The purposes for which Rise may process personal data include, but are not limited to:

21.2.1. To register participants;

21.2.2. To perform a contract or service;

21.2.3. To manage a relationship, including notifications about changes to a contract or service, or asking for feedback;

21.2.4. To administer and protect the business and the Rise website; and

21.2.5. To make suggestions or recommendations about similar goods or services that may be of interest to the data subject.

22. Data Protection Measures

22.1. Rise shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All emails containing personal data must be encrypted and sent via Microsoft Outlook

b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hard copies should be shredded, and electronic copies should be deleted securely using proprietary software.

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

f) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a recorded delivery service;

g) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of Rise requires access to any personal data that they do not already have access to, such access should be formally requested from Rise's Data Protection Lead;

h) All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of Rise or not, without the authorisation of Rise's Data Protection Lead;

j) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

k) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

l) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Rise or otherwise, without the formal written approval of Rise's Data Protection Lead and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

m) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Rise where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulations (which may include demonstrating to Rise that all suitable technical and organisational measures have been taken);

n) All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted proprietary software;

o) All electronic copies of personal data should be stored securely using passwords and proprietary data encryption;

p) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by Rise is designed to require such passwords under our IT & Email Policy.

q) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Rise, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

r) Where personal data held by Rise is used for marketing purposes, it shall be the responsibility of Rise's Data Protection Lead to ensure that no data subjects have added their details to any marketing preference databases.

23. Organisational Measures

23.1. Rise shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the company shall be made fully aware of both their individual responsibilities and Rise's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy if working with personal data;

b) Only employees, agents, sub-contractors, or other parties working on behalf of Rise that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the company;

c) All employees, agents, contractors, or other parties working on behalf of Rise handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of Rise handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other parties working on behalf of Rise handling personal data shall be regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of Rise handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of Rise handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the company arising out of this Policy and the Regulation;

i) Where any agent, contractor or other party working on behalf of Rise handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring Personal Data to a Country Outside the EEA

24.1. Rise may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA, however, this is an unlikely and infrequent action.

24.2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and Rise (or for pre-contractual steps taken at the request of the data subject);

e) The transfer is necessary for important public interest reasons;

f) The transfer is necessary for the conduct of legal claims;

g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data Breach Notification

a) Rise has an internal Data Breach Policy and Procedure which details how it handles potential data breaches.

This Policy has been most recently approved and authorised by:

Name:	Clare Morley
Position:	Chief Executive Officer
Date:	05/06/2024
Due for Review by:	30/11/2025