Data Protection Policy

1. Purpose and scope

1.1 The Rift Valley Institute ("RVI", "the Institute") processes personal information (also called personal data) about individuals. Individuals include, but are not limited to, consultants, employees, fellows, partners, donors, event and course participants, contractors, suppliers, and others who are in contact with RVI for a variety of reasons.

1.2 This document sets out the RVI data protection policy. It provides some basic information about data protection, including the 7 data protection principles, information regarding special categories of personal data, how RVI processes personal information (including the legal bases for processing), how RVI keeps it secure and where appropriate shares it, and how RVI would deal with any data security breach. It also provides information on the rights of "data subjects" (individuals about whom RVI holds personal information). It applies to all those involved in processing personal information on our behalf, who must comply with this policy in all respects.

1.3 **Personal data** is any information from which a person can be identified, directly or indirectly. In addition to basic personal information, such as names and contact details, it includes opinions expressed about a person and information regarding the intentions of the data controller and third parties about a person. It does not include information that has been appropriately anonymised.

1.4 **Processing** means anything RVI does with personal information—for example, collecting, editing, storing, holding, disclosing, sharing, viewing, recording, listening, erasing, or deleting. RVI is committed to processing personal information appropriately and lawfully, in terms of the Data Protection Act 2018 (the "2018 Act") and the General Data Protection Regulation ("GDPR").

1.5 RVI has a separate **Privacy Policy,** which outlines the way in which RVI processes personal information provided, and a **Data Retention Policy,** which outlines how long various categories of personal information are retained by RVI. In general terms, personal information should only be retained for as long as is necessary for the purposes for which it was obtained.

1.6 This policy does not form part of any contract of employment or contract to provide services. It will be reviewed from time to time to ensure compliance with data protection laws and will be updated as required.

1.7 RVI takes compliance with this policy very seriously. Any deliberate or negligent breach of this policy by an employee may result in disciplinary action being taken and may result in dismissal for gross misconduct.

2. Protection Principles

2.1 Personal information will be processed in accordance with the 7 GDPR Data Protection Principles, which stipulate that personal information must be:

- processed lawfully, fairly and in a transparent manner: data is stored with one of GDPR's legal bases as outlined in this policy, the Data Retention Policy and the Privacy Policy, which are publically available;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes: when RVI collects data, it will explain as clearly as possible what the data is intended for and not use it for any other purpose;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed: which data RVI collects, how long it retains it and why are outlined in the Data Retention Policy;
- accurate and, where necessary, kept up to date: RVI's Data Retention Policy includes when and how data are updated and, otherwise, deleted;
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which it is processed: if data is kept for statistical, analytical or reporting purposes, RVI will ensure it is anonymized;
- processed securely, with protection against unauthorised or unlawful processing and against accidental loss or damage, using appropriate technical or organisational measures: an Information Management Manual ensures staff all minimize the risks to the personal data RVI keeps;

and, in accordance with the seventh principle, RVI is responsible for, and must be able to demonstrate compliance with, the first 6 principles as listed above.

3. Special categories of personal data

3.1 These are categories of personal information that are deemed to be more sensitive than others. Additional rules (see under paragraph 4 below) apply to the processing of personal information which falls under any of these categories, which are defined in the GDPR as being "*Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*"

3.2 RVI may hold significant amount of personal information classed as *special category personal data* in the form of interview transcripts with research subjects. All research transcripts are anonymised and encrypted according to the sensitive documents protocol as outlined in the RVI Information Management manual.

3.3 RVI may also hold significant amount of personal information classed as special category personal data in databases designed to lanalyse social and political processes relevant to RVI's research. Whilst such information is not de-identified within the database itself, project managers are required to ensure access to such database is highly restricted, password protected (using two-factor authentication where possible), and regularly reviewed and re-assessed.

4. Legal Bases for processing personal information and special categories of personal information

4.1 RVI processes personal information on one or more of the following legal bases, which are also set out in the Privacy Policy, where:

4.1.1 an individual has given consent to the processing for one or more specific purpose;

4.1.2 processing is necessary for the performance of a contract with an individual; or

4.1.3 processing or sharing is believed to be necessary to protect an individual's life in line with RVI Travel and Security Policy; or

4.1.4 processing is necessary for compliance with a legal obligation.

4.1.5 processing is necessary for the legitimate interests of the organisation, or the legitimate interests of a third party; if data is processed based on legitimate interest, a legitimate interest assessment will be conducted for the data in question.

4.2 Where RVI processes special category data (and this will be in exceptional cases) RVI will, **in addition** to meeting a minimum of one of the legal bases listed in paragraph 4.1, hereof ensure that one or more of the following applies:

4.2.1 processing is carried out in the course of RVI's legitimate activities with appropriate safeguards by RVI as a not-for-profit body and on condition that the processing relates solely to RVI staff and consultants, or to former staff and consultants, or to people who have regular contact with RVI in connection with RVI's institutional aims, and that the personal information is not disclosed outside RVI without your consent; or

4.2.2 a person has given explicit consent to the processing of their personal information for one or more specified purposes.

5. Access to personal information and keeping it secure

5.1 Everyone who processes personal information on RVI's behalf (including, but not limited to, employees, consultants, interns and service providers) must ensure that they do so in line with this policy, our Data Retention Policy and our Privacy Policy, and all in accordance with data protection law.

5.2 Personal information should only be accessed by those who need it in connection with the work they do for RVI.

5.3 Personal information should be processed only for the purposes for which it was obtained.

5.4 Personal information should be accurate and, where necessary, updated.

5.5 Personal information should not be shared with persons who are not authorised to receive it. Care should be taken when dealing with any request for personal information, whether by letter, email communication, over the telephone, or otherwise. Identity checks should be carried out if giving out information to ensure that the person requesting the information is either the individual concerned, or someone properly authorized to act on their behalf.

5.6 Hard copy personal information should be avoided where possible, otherwise stored securely (in lockable storage, where appropriate) and not visible when not in use, or disposed when no longer needed.

5.7 Confidential paper waste should be disposed of securely by shredding.

5.8 Staff computers should be locked (or shut) when leaving them unattended, and should be password protected. Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

5.9 Group or non-personal email addresses (e.g. finance@riftvalley.net) should not be used for processing personal information.

5.10 Emails containing personal information should not be sent to or received at a work email address (other than an @riftvalley.net address) as this might be accessed by third parties.

5.11 If personal devices have an @riftvalley.net account linked to them these should not be accessed on a shared device for which someone else has the pin code.

5.12 Personal data stored electronically should not be kept outside of RVI's information management architecture (i.e. it must be kept within RVI email, file sharing system or contact database).

5.13 As an international organization RVI will transfer personal data outside the European Economic Area, but will do so in compliance with the GDPR as set out in this policy, as well as the Data Retention Policy and the Privacy Policy.

6. Sharing personal data

6.1 RVI will only share personal information where the Institute has a legal basis to do so. This may require information relating to travel insurance, in line with RVI Travel and Security Policies; personal and contact information relating to project teams in order to execute contracts; or to comply with tax legislation in countries where RVI has staff and offices.

6.2 Information is only sent outside the European Economic Area in line with the requirements of the GDPR.

7. If there is a data security breach

7.1 A data breach is where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This can happen in many different ways, for example:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information by a member of staff, volunteer or third party;
- Loss of data resulting from an equipment or systems failure;
- Human error, such as accidental deletion, alteration or transfer of data;
- Unforeseen circumstances, such as fire or flooding;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams;

7.2 Should a data security breach occur, and if the breach is likely to result in a risk to the rights and freedoms of individuals, RVI will notify the Information Commissioner's Office without undue delay and, where possible, within 72 hours of the time we become aware of the breach. Notification will be made or coordinated by the Head of Operations.

8. Subject access requests

8.1 Individuals who are data subjects may ask for copies of the personal information RVI holds about them. This request must be made in writing. Any such request received by the Institute should be forwarded immediately to data@riftvalley.net who will coordinate a response within the necessary time limit (maximum 30 days).

8.2 It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

9. Rights of Data subjects

9.1 Data subjects have certain other rights under the GDPR and the 2018 Act, including the right to know what personal data the Institute is processing, the purposes of such processing, and the legal basis or bases for the processing.

9.2 Data subjects have the right to request that RVI rectifies any inaccurate or incomplete personal information, and to erase personal data if RVI is not entitled by law to process it or it is no longer necessary for RVI to process it for the purpose for which it was collected. In situations where consent is the only legal basis RVI has for processing data, the personal information should be erased if and when the individual revokes that consent.

9.3 All requests to have personal data corrected or erased should be passed to the Head of Operations who will be responsible for responding to them.

10. Training

10.1 RVI will ensure that all those engaged in processing personal information for the Institute receive adequate training in their data protection responsibilities.

11. Contracts

11.1 If any processing of personal information is outsourced to an external data processor RVI will enter into a contract with them to ensure compliance with data protection law.

12. Data Protection Policy Review

12.1 This policy will be reviewed and updated annually.

This Data Protection Policy was adopted on June 2021. The charity and trustees will be responsible for the implementation of this Policy.