RE:ACT DATA PROTECTION AND DATA SECURITY POLICY

1. Introduction

1.1 RE:ACT is committed to ensuring that all personal information handled by us will be processed accordingly to legally compliant standards of data protection and data security.

1.2 The purpose of this policy is to help us achieve our data protection and data security aims by:

(a) ensuring staff understand our rules and the legal standards for handling personal information relating to staff members, volunteers, donors, and others

(b) clarifying the responsibilities and duties of staff in respect of data protection and data security

2. Who is responsible for data protection and data security?

2.1 Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all staff of RE:ACT, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers.

2.2 The Board of Directors of RE:ACT has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed the RE:ACT Head of Tech and Innovation as the Data Protection Officer with day-to-day responsibility for data processing and data security.

2.3 All staff have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance.

2.4 Any breach of this policy will be taken seriously and may result in disciplinary action.

3. What personal information and activities are covered by this policy?

3.1 This policy covers personal information:

(a) which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess;

(b) is stored electronically or on paper in a filing system;

(c) in the form of statements of opinion as well as facts;

(d) which relates to any individual whose personal information we handle or control;

(e) which we obtain, hold or store, organize, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

4. Data protection principles

4.1 Staff or volunteers whose work involves using personal data relating to any individual must comply with this policy and with the six legal data protection principles as set out in The General Data Protection Regulation (GDPR) which require that personal information is:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(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 they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are 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 are 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 GDPR in order to safeguard the rights and freedoms of individuals; and

(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.

4.2 Some personal information needs even more careful handling. This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about criminal offences. Strict conditions apply to processing this sensitive personal information and the subject must normally have given specific and express consent to each way in which the information is used.

5. Data security

5.1 We must all protect personal information in our possession from being accessed, lost, deleted or damaged unlawfully or without proper authorization through the use of data security measures.

5.2 Maintaining data security means making sure that:

(a) only people who are authorised to use the information can access it;

(b) information is accurate and suitable for the purpose for which it is processed; and

(c) authorised persons can access information if they need it for authorised purposes. Personal information therefore should not be stored on individual computers but instead on authorised cloud based systems.

5.3 By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

5.4 Personal information must not be transferred to any person to process (e.g. while performing services for us on our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

5.5 Security procedures include:

(a) **Physically securing information**. Any desk or cupboard containing confidential information must be kept locked. Computers should be locked

with a password or shutdown when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.

(b) **Controlling access to premises.** Staff should be aware of and confront any person they do not recognise in any area of the office.

(c) **Telephone precautions.** Particular care must be taken by staff or volunteers who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

(i) the identity of any telephone caller must be verified before any personal information is disclosed;

(ii) if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;

(iii) do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the RE:ACT Data Protection Officer.

(d) **Methods of disposal.** Copies of personal information, whether on paper or any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

6. Subject access requests

6.1 By law, any subject may make a formal request for information that we hold about them, provided that certain conditions are met. The request must be made in writing. In some circumstances, it may not be possible to release the information about the subject to them e.g. if it contains personal data about another person.

6.2 Any member of staff or volunteer who receives a written request should forward it to the RE:ACT Data Protection Officer immediately.