RETAS LEEDS

Data Protection Policy – September 2018

SECTION 1: Purpose

RETAS needs to keep certain information on its employees, volunteers, service users and trustees to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation. This policy covers employed staff, trustees, volunteers

SECTION 2: Principles of Data Protection

This section sets out the key requirements of the Data Protection Act

In line with the Data Protection Act 1998 principles, RETAS will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred to other countries without adequate protection

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. RETAs will seek to abide by this code in relation to all the personal data it processes, i.e.

- Accountability: those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- Visibility: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- Consent: The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be

used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.

- Access: Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.

- Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span.

SECTION 3: Responsibilities

- Overall responsibility rests with the Board of Trustees
- This Board of Trustees delegates specific tasks to specified personnel
- All staff/ trustees/ volunteers have responsibilities to abide by the policy.

All employed staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary proceedings.

To meet our responsibilities staff, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.

SECTION 4: Subject Access Requests

The Data Protection Act 1998 states that people have a right to access any information that we hold about them. This includes employees, volunteers, Trustees and people who use our services. The Act says that we have to respond to requests for access to information within 40 calendar days.

Information about the records or to grant access after receiving a signed written request from the client should be responded to within 40 days. Identification must be checked, including photo ID. It is reasonable to ask further questions of the client before releasing information but this should not be used to extend the 40 day deadline. Refusals to release information should be given in writing.

A fee can be charged to release the information, the maximum fee is £10. It is reasonable not to release any information before the fee is received.

A request for access to records may be denied if granting access is considered likely to cause serious harm to the physical or mental health or condition of the client and that opinion has been endorsed by an appropriate health professional. An appropriate health professional would usually be a doctor involved in the treatment of the person concerned.

Policy approved by:

Signature……
Date……

Chair of Trustees

Name……..

REVIEW

The effectiveness of this policy and associated arrangements will be reviewed annually by the Board of Trustees under the direct supervision of the RETAS Chief of Executive.

Review Date: September 2019