Data Protection Policy

Date of Review: **November 2018**

Date of Next Review: **November 2019**

Chief Executive Officer's Signature: ….....

DATA PROTECTION POLICY

Purpose Of This Policy

To ensure that all staff, volunteers and trustees comply with the EU General Data Protection Regulation and any subsequent revisions of this Act.

General Principles

Accuro (Care Services) as a data controller must comply with the Data Protection Principles: -

1. Personal data must be fairly and lawfully obtained. We must be transparent as to how the data will be used.

2. Personal data must only be obtained for a specific lawful purpose.

3. Personal data must be adequate, relevant and not excessive in relation to the purposes for which it is processed.

4. Personal data must be accurate and, where necessary, kept up-to-date.

5. Personal data processed for any purpose(s) shall not be kept longer than is necessary for that purpose.

6. Personal data must be kept safe and secure.

7. Personal data must be processed in accordance with the rights of data subjects under the Act.

8. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

9. We do not process or store data outside of the EU, but data may reside or pass outside the EU during transmission e.g. via email, the routing of which is outside our control.

What Is Personal Data?

Data which relates to a living individual who can be identified from that data (or from that data together with other information in the possession of the Data Controller, i.e. Accuro (Care Services)). It includes any expression of opinion about the individual and any indication of the intentions of the data controller. The legislation covers manually held data as well as that held on computers. It includes visual images and sound recordings, information about sole traders and partnerships but not companies.

Personal data we gather may include: individuals name, date of birth, email address, postal address, telephone number, health care professionals, social workers, carers and schools.

What Does Processing Mean?

Processing is very widely defined and includes: obtaining, recording, using, disclosing and holding data. The legislation requires certain conditions to be met before personal data may be processed and care must be taken with what the Act defines as "sensitive data".

What Is "Sensitive Data"?

Sensitive Data includes:

- The racial or ethnic origin of the data subject.
- Political opinions.
- Religious beliefs.
- Membership of a Trade Union.
- Physical or mental health.
- Information around individual's medical health and disabilities.
- Sexual orientation.
- The commission or alleged commission by the data subject of any offence.
- Or any proceedings for any offence committed or alleged to have been committed by them, or the sentence of any court in such proceedings.

This list is not comprehensive – if in doubt about any data, seek advice from the CEO.

Who Are Data Subjects And What Are Their Rights?

Data subject means an individual about whom Accuro (Care Services) holds personal data. Their rights are:

- To ask what information we hold.
- To be given a copy of the information (except where legal exemptions apply).
- To be given details about the purpose for which we use the information and about other organisations or people to whom it is disclosed.
- To ask for incorrect data to be corrected.
- To ask us not to use their personal information for direct marketing which is likely to cause damage or distress or to make decisions based on the automatic processing of the information.
- To require the Information Commissioner to assess whether there has been a contravention of the Act.

- To be compensated for any damage or distress should these be caused by failure to comply with the Act.

How Accuro (Care Services) Store Your Data

Personal data in our databases is only accessible by appropriately trained staff and volunteers who need to access your personal data as an essential part of their role. All access is tracked through individual login credentials. We take the security of personal data seriously. We employ security technology, including firewalls, and encryption to safeguard personal data and have procedures in place to ensure that our paper and computer systems and databases are protected against unauthorised disclosure, use, loss and damage.

We only use third party service providers where we are satisfied that the security they provide for your personal data is at least as stringent as we use ourselves.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, and include computer records as well as manual files.

Many records will be kept whilst the person is a:

- Service User, Trustee, Employee or Volunteer

Many records are kept for up to seven years including, but not limited to:

- Records relating to contractual matters
- Financial records to support HMRC audits or provide tax information
- Ex-employee records
- Minutes of meetings

Some records are kept for up to two years, including those where consent appropriate to circumstances has been requested and obtained. These include records of:

- Ex-Service Users
- Ex-Volunteers
- Ex-Trustees
- Attendees at events
- Personal information in responses to questionnaires

Records related to unsuccessful applicants for a job or a Trustee or Volunteer role will be kept for up to 6 months. In all cases the times given are measured from the date of the latest interaction with the data subject in relation to that data.

Our Responsibilities Under The Regulation.

- Files/confidential information must not be left in unlocked cabinets (this includes computer storage devices, e.g. discs).
- Access to personal information must be on a strict need to know basis. Information must contain the minimum identifiable information necessary.
- When transporting files around, store in lockable box or briefcase in locked boot of car. On no account should files be left on display.
- Take great care when e-mailing confidential information.
- Records of service users and staff must always be stored in lockable cupboards/systems when an office is unattended.
- Documents on screen must be shut down when pc is unattended.
- All computers and storage devices on which data is stored must be password protected.

Consent

Informed consent must be obtained from individuals regarding the possibility of information being passed to other agencies. Refusal to consent must be respected unless exceptional circumstances exist.

These are:

- Information required by statute or court order.
- Where a serious public health risk exits.
- Where a serious risk of harm to the individual or other individuals exists.
- Where information is required for the prevention, detection of prosecution of serious crime.
- To safeguard national security.

Disclosures

Information on a need to know basis can be given to clients, families, carers/befrienders and volunteers in order that the services offered can function effectively and safely for all concerned.

However, there is an overriding duty under child protection procedures to report any concern that has to do with a child or children who may be at risk of significant harm.

There also may be other strictly limited expectations where the law or the public interest will override the person's right to confidentiality and thus consent is not required. Legal

advice should then be obtained, and no more information disclosed than is strictly required.

Record of Consent

EU General Data Protection Regulation

To provide you with a service we may need to record sensitive personal data about you. The law says that we must get your consent to do this. Everything you tell us will be treated as confidentially, save in exceptional circumstances (please see attached policies on Confidentiality and Data Protection).

Sensitive personal data is defined as information relating to any of the following: racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexuality or sex life, offences and/or convictions.

The Data Controller is Accuro (Care Services) for the purpose of the Act.

I have read, understand and agree to abide with the contents of the Data Protection Policy.

Name: .....

Signature: .....

Date: .....