Data Protection

Statement of Scope and Purpose

This policy applies to everyone linked with Pillar Kincardine, whether service users, advisers, volunteers or staff. Its aim is to ensure that all those involved are aware of:

- what, if any, personal data is held by Pillar Kincardine – the 'data controller' – regarding them – the 'data subjects'
- what measures are in place to protect them from any misuse of such data
- their right to confidentiality within the organisation
- their responsibilities regarding the security of their own and others' personal data.

Commitment

All personal details held by Pillar Kincardine both manually and in computer records are subject to the Data Protection Act 1998 (DPA) – as amended by the European Union's General Data Protection Regulation 2018 (GDPR) – and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). We are committed to complying fully with these regulations and with the DPA's eight Data Protection principles. Pillar Kincardine will, accordingly, ensure that:

1. *We have legitimate grounds for collecting and using personal data*

We'll not only tell people why we want to collect their details, and only do so if we have their clear and informed consent, but also make sure that everything we do with the information is in the individual's best interests.

2. *We are completely open and transparent about how we intend to use the data*

If we wish to use or disclose the data we have collected for any purpose other than that originally specified, we'll make that new use or disclosure absolutely clear to those affected. *However, see note on Disclosure below.*

3. Any personal data we hold are adequate, relevant and not excessive

We'll identify the minimum amount of personal data we need about each individual to be able to deliver our services in a professional manner, and to fulfil our responsibilities in respect of any contract or service level agreement we may have with funding bodies. And we'll hold only that much information – nothing more.

4. *The data are accurate and up to date*

We'll do everything we can to ensure that the personal data we hold about each individual has been checked with them and as far as possible is kept up to date.

5. *The data are kept no longer than necessary*
In particular we'll review the personal data we hold annually and destroy any information held on any person who has had no contact with Pillar in the preceding year, in accordance with an agreed Retention Schedule.

6. The rights of our data subjects are respected at all times
Thus any member or person connected with Pillar Kincardine can ask to see the details held about them on our systems at any time and we'll do our very best to comply in a reasonable timeframe and at no cost to them.

7. We take all reasonable steps to protect personal data from accidental disclosure or theft
We'll make sure our systems have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; this includes making it clear who within Pillar Kincardine is responsible for ensuring information security.

8. No personal data is transferred to another country unless we are legally required to do so.

In addition,

- Pillar Kincardine will carry out an annual audit of its data protection practice to ensure that it remains in compliance with the eight Data Protection principles.
- Members of and advisors to the Board of Directors, volunteers, and members of staff will be required to make a written, personal commitment to uphold the aims of this policy.

A Note on Disclosure

Pillar Kincardine will not in normal circumstances pass on personal data to a third party without the express permission of the person involved. However, we have a common law duty of care, and where we believe that there is a risk of serious harm to a person or to others, then, and only in these exceptional circumstances, information may be passed to the appropriate authorities.

If practicable, Pillar Kincardine will inform the person in advance of any such disclosure to a third party.

Signed:

(Chair) (Service Manager)

Date:

Adopted 11"' April 2018 Date of review April 2021