Calderdale Valley of Sanctuary

**Data Protection Policy**

**Calderdale Valley Of Sanctuary**

**Review Date Dec 2022**

## 1. Purpose of the policy

1.1 Calderdale Valley Of Sanctuary is committed to complying with privacy and data protection laws including the Data Protection Act ("**the DPA**"). This policy sets out what we do to protect individuals' personal information.

1.2 Anyone who handles personal data in any way on behalf of Calderdale Valley Of Sanctuary must ensure that they comply with this policy. Section 3 of this policy describes what comes within the definition of "personal information". Any breach of this policy will be dealt with seriously and may result in disciplinary action or more serious sanctions.

1.3 This policy may be amended to reflect changes in legislation, regulatory guidance or internal policy decisions. You may not necessarily be notified of these changes so you should review this policy from time to time.

## 2. About this policy

2.1 The types of personal information we may deal with include details of members, (potential) drivers and asylum seekers & refugees mobile phone numbers.

2.2 The Chair of Calderdale Valley of Sanctuary is responsible for ensuring compliance with the DPA and this policy. Any concerns or questions in connection with this policy should be referred in the first instance to the Chair of Management Committee by emailing togetherwegrow2@yahoo.com

## 3. Definition of data protection terms

The following terms will be used in this policy and are defined below:

3.1 **Data subjects** include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.2 **Personal data** means information relating to a living person who can be identified from that information (or from that information when combined with other information in our

possession). Personal data can be factual (such as a name, address or date of birth) or can be an opinion (such as a performance appraisal).

3.3 **Data controllers** are people who, or organisation which, decide the purposes for which, and the way any personal data is processed. They have a responsibility to process personal data in compliance with the DPA. **Calderdale Valley Of Sanctuary is the data controller for all personal data that we manage in connection with our work and activities.**

3.4 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include other organisations such as website or server hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.5 **EEA** is the European Economic Area which includes all countries in the European Union, as well as Norway, Iceland and Liechtenstein.

3.6 **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.7 **Processing** is any activity that involves use of personal data. It includes obtaining, recording, holding, organising, amending, using, disclosing or destroying personal data.

3.8 **Sensitive personal information** 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;
- Sexual life or orientation; or
- Criminal record (including any allegation that they have committed an offence).

**4. Data protection principles**

Anyone processing personal data must comply with the eight data protection principles. We are required to comply with these principles (summarised in paragraphs 5-11 below) in respect of any personal data that we deal with as a data controller.

Personal data should be:

4.1 Processed fairly and lawfully;

4.2 Processed for purposes which the individual has been told about, and not in any way that is incompatible with those purposes;

4.3 Adequate, relevant and not excessive in relation to the purpose for which it is held;

4.4 Accurate, and where necessary, kept up to date;

4.5 Not kept longer than necessary;

4.6 Processed in accordance with individuals' rights;

4.7 Secure; and

4.8 Not transferred to people outside the EEA without adequate safeguards.

**5. Processed fairly and lawfully**

5.1 The first data protection principle requires that personal data be obtained fairly and lawfully and processed for purposes that the data subject has been told about.

5.2 To do this, every time we receive personal data about a person, which we intend to keep, we need to provide that person with **"the fair processing information"**. In other words, we need to tell them promptly:

5.2.1 Who will be holding their information i.e., Calderdale Valley Of Sanctuary;

5.2.2 Why we are collecting their information and what we intend to do with it, for instance to notify them of annual general meetings or send them mailing updates about our activities; and

5.2.3 Anything else necessary to make sure that we are using their information fairly, for example, if we intend to share their information with another organisation.

5.3 This fair processing information can be provided in several places including on web pages, in mailings or on application forms.

5.4 Obtaining an individual's consent can help ensure we process their data fairly but in most cases is not required. Exceptions to this are covered in paragraphs 12 and 15 below.

**6. Processing data for the original purpose**

6.1 The second data protection principle requires that personal data be only processed for the specific purposes that the individual was told about when we first obtained their information.

6.2 This means that we should not collect personal data for one purpose and use it for another, unless the second purpose is implicit.

**7. Personal data should be accurate**

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Inaccurate or out-of-date data should be archived if necessary or otherwise destroyed securely.

**8. Not retaining data longer than necessary**

8.1 The fifth data protection principle requires that we should not keep personal data for longer than we need it for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think we are holding out-of-date or inaccurate personal information, please speak to Xx.

8.2 For guidance on how long particular types of personal information that we collect should be kept before being destroyed or erased, please consult Xx or seek legal advice.

**9. Rights of individuals under the DPA**

The DPA gives people rights in relation to how organisations process their personal data. They include (but is not limited to) the right:

9.1 to request a copy of any personal data that we hold about them (as data controller) as well as a description of the type of information that we are processing, the uses that are

being made of the information and details of anyone to whom their personal data has been disclosed (known as subject access rights);

9.2 to have inaccurate information amended or destroyed;

9.3 to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else; and

9.4 to ask us to cease processing for direct marketing purposes.

**10. Data security**

10.1 The seventh data protection principle requires us to keep secure any personal data that we hold.

10.2 We are required to put in place procedures to keep the personal data that we hold secure.

10.3 When we are dealing with sensitive personal information (as defined in paragraph 3.8 above), more rigorous security procedures are likely to be needed, for instance, if sensitive personal information is held on a memory stick or other portable device it should be encrypted.

10.4 When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures must be followed in relation to all personal data processed by us:

- Equipment: Users should ensure that individual monitors do not show confidential information to others who are unauthorised and that they log off from their PC when it is left unattended;
- Methods of disposal: Paper documents should be shredded. Memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer needed;
- Secure exchange of data: Personal data must always be exchanged in a secure manner. The degree of security will depend on the nature of the data; how sensitive the data; the more sensitive and confidential the data, the more stringent the security measures should be. The following precautions should be taken:
    - use registered post or courier. Never send a CD or stick containing personal data by ordinary post;
    - use password protection (on files) if sending by e-mail – but recognise that this is not very secure and should only be used for small quantities of information;
    - never send sensitive data by e-mail unless it has been encrypted (speak to xx for more details);
    - if you wish to process personal data on your personal device (such as a smartphone or tablet) you need to be satisfied that it is being processed securely. Please discuss this with Xx before doing so.

**11. Transferring data outside the EEA**

11.1 The eighth data protection principle requires that when organisations transfer personal data outside the EEA they take steps to ensure that the data is properly protected.

11.2 Not used

11.3 Not used

11.4 If a transfer outside the EEA is necessary, speak to Xx or seek further legal advice before doing so.

**12. Processing sensitive personal data**

12.1 On some occasions we may collect information about individuals that is defined by the DPA as **sensitive,** and special rules will apply to the processing of it. The categories of sensitive personal data are set out in the definition in paragraph 3.

12.2 In most cases, to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be clear with people about how we are going to use their information.

12.3 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the DPA permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal information and are not able to obtain explicit consent for the processing, please speak to Xx.

**13. Consent**

Whilst consent is not required to process most data, it is usually required to process sensitive personal data (see paragraph 12 above) and is normally required to send direct marketing by e-mail or SMS. Please speak to xx if you plan to do this.

**14. Monitoring and review of the policy**

This policy is reviewed once every two years by our Management Committee to ensure that it is achieving its objectives.

**Agreed December 4th, 2020**

**Review date December 4th, 2022**