Confidentiality and Data Protection Policy – Appendix 1

1.0 The six privacy principles

1.1 Under the GDPR, there are six privacy principles which are key conditions that we must follow when processing personal information:

1. **Lawfulness, fairness and transparency**

   Lawfulness – the Group must have, and record, a legal basis for processing personal data.

   Fairness – we must only process personal data in ways which is fair to the data subject.

   Transparency – we must tell people what personal data we collect and how we process it. This is done via the Privacy Notice on the website. There is a separate Privacy Notice for employees, volunteers and Board Members in the Employees' Handbook.

2. **Purpose Limitations**

   We must only use personal data we collect for specific purposes, as set out in the Privacy Notices.

3. **Data Minimisation**

   We must only collect personal information which is adequate, relevant and necessary for specific processing purposes.

4. **Accuracy**

   Personal data collected by the Group must be accurate and up to date.

5. **Storage limitations**

   We must not store the personal data that we collect for longer than necessary.

6. **Integrity and Confidentiality**

   We must ensure that there are adequate technological and organisational measures in place to keep personal data secure.

1.2 It is a criminal offence to:

- Unlawfully obtain or disclose personal data;
- Sell, or offer to sell, personal data without the consent of the data subject

- Fail to comply with any enforcement notice issued by the Information Commissioners Office (ICO).

2.0 Lawful bases for processing data

2.1 We must establish and record a valid lawful basis to process personal data, special category personal data and information relating to criminal convictions. When processing personal data, there are six lawful bases:

- Consent – where a data subject has given clear consent for their personal data to be processed for a specific purpose;
- Contract – where the processing is necessary in the performance of a contract, or where specific steps need to be taken before entering into a contract;
- Legal Obligation – where the processing is necessary in order to comply with the law;
- Vital Interests – where the processing is necessary to protect someone's vital interests;
- Public Task – where the processing is necessary to perform a task in the public interest, or for an official function;
- Legitimate Interests the processing is necessary for the legitimate interests of the data processor and those interests outweigh the rights and freedoms of the data subject.

2.2 Where we process 'special category data' (sensitive personal data, including genetic and biometric data) an additional special category basis must also be identified in addition to one of the above lawful bases. The ones which are relevant to the Group are:

- The data subject has given explicit consent to the processing of their personal data for one or more specified purposes;
- Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment or social security and social protection law.
- Processing is necessary to protect the vital interests of the data subject or of another individual where they are incapable of giving consent;
- Processing relates to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims;
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.