# Data Protection Statement

| | |
|---|---|
| **Reviewed by:** | Board of Trustees |
| **Date Approved:** | **16 July 2024** |
| **Next review due:** | July 2026 |

This policy sets out how we will protect personal data, special category data and criminal convictions personal data.

It meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

**Principle 1** – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

*We ensure that processing is fair by providing detailed privacy notices to individuals whose personal data is being processed. All individuals are advised of their right to contact the Data Protection Officer with any queries regarding the processing of their personal data. We will only process personal data fairly, and will not mislead individuals about how their data may be used.*

**Principle 2** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

*We meet this obligation by explaining through our privacy notices which legal basis we are relying on when processing personal data. We will only use the data for the purposes for which it was collected unless we advise individuals, prior to any additional use, of our intentions and the rights they have in relation to any further use.*

**Principle 3** – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

*We meet this obligation by only collecting what is required for a particular purpose, and ensuring that we have sufficient relevant information for that purpose.*

**Principle 4** – Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

*We meet this obligation by ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.*

**Principle 5** – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

*We meet this obligation by ensuring that personal data is managed in line with our retention schedule, and either deleted or completely anonymised when it is no longer necessary for us to use it. The period for which we retain personal data is explained in each privacy notice relevant to that service.*

**Principle 6** – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

*We meet this obligation by ensuring that our technical and organisational controls. Our organisational controls include:*

- Appropriate roles and responsibilities including a Data Protection Officer and Senior Information Risk Owner
- Robust policies and procedures which are regularly reviewed
- Regularly training our staff in their data protection responsibilities
- Ensuring our processing activities are transparent and secure, including
    - o Records of Processing Activities
    - o Data Protection Impact Assessments
- Contractual Controls to govern the use of personal data by our suppliers
- Physical security controls including
    - o Restricted access to physical storage of sensitive personal data
    - o Visitor management
- Security breach management

**Our Technical Controls include:**

- Firewalls, anti-malware and patching
- Disaster Recovery and Business Continuity arrangements
- Role based access controls to personal data
- Password management
- Sending email securely

**Principle 7** - The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

*We meet this obligation by maintaining Records of Processing Activities which are available on demand to the Information Commissioner. We routinely carry out Data Protection Impact Assessments for any processing of special categories of data or where there is a high risk to individuals' privacy. We have appointed a Data Protection Officer and have defined policy and process to manage the exercising of data subjects' rights.*

For further information about how we process personal data please see our online privacy notices on our website or contact our Data Protection Officer, Jordan Aldridge: jaldridge@epsilonstar.co.uk