GDPR/DATA PROTECTION POLICY

Data Protection Policy

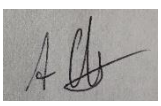
In line with the General Data Protection Regulations (GDPR) our data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

We are committed to:
Ensuring that we comply with the eight data protection principles, as listed below. Meeting our legal obligations as laid down by the Data Protection Act 1998. Ensuring that data is collected and used fairly and lawfully. Processing personal data only in order to meet our operational needs or fulfil legal requirements. Taking steps to ensure that personal data is up to date and accurate. Establishing appropriate retention periods for personal data. Ensuring that data subjects' rights can be appropriately exercised. Providing adequate security measures to protect personal data. Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues. Ensuring that all staff are made aware of good practice in data protection. Providing adequate training for all staff responsible for personal data. Regularly reviewing data protection procedures and guidelines within the organisation.

Data protection principles

1. Personal data shall be processed fairly and lawfully. 2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998. 7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal Data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is to be reviewed annually. Next review 25/8/2027.

Signed: 

Adam Clements

Data Protection officer (DPO):