GDPR Policy

Version:	Detail:	Approved by:	Date:
1.0 to 1.1	First Issue following policy introduction	Paul Prisgrove	May 2019
1.2	Annual review and staff contact changes	Blake Prisgrove	2022
1.3	Implementation of refreshed policy, featuring new responsibilities	Richard Luke	November 2023
1.4	Reviewed and updated to new template	Paul Ollivere	October 2025

1.1 Purpose:
We are committed to forging continued trust, starting with helping our stakeholders understand our privacy practices.

SMI's 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.

The UK GDPR sets out seven key principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

SMI embodies these principles; they are at the heart of our approach towards processing and protecting personal data.

1.2 Statement of Intent:
Our commitment ensues 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 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.
- Ensuring that everyone handling personal data knows where to find further guidance.
- Ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly.
- Regularly reviewing data protection procedures and guidelines within the organisation.

1.3 Principles of the Policy:

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 should 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

1.4 Further information:

Data Protection Act 1988
https://www.legislation.gov.uk/ukpga/1998/29/contents
• Data Protection 2018:
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted