SOLAS OXFORD
Community Interest Company

SOLAS Oxford Information Governance and GDPR Policy

1. Introduction

This Information Governance and GDPR Policy outlines the principles and guidelines that SOLAS Oxford Community Interest Company adheres to regarding the handling and protection of personal and sensitive information. The policy applies to all employees, contractors, volunteers, and third parties who have access to the Company's information assets.

2. Scope

This policy applies to all personal data and sensitive information collected, processed, stored, or transmitted by the Company during its operations, including but not limited to the training and supervision of health and social care professionals, research activities, and psychotherapeutic interventions for parents, children and vulnerable adults.

3. Data Protection Principles

The Company is committed to upholding the following data protection principles:

a. Lawfulness, Fairness, and Transparency: Personal data shall be processed lawfully, fairly, and in a transparent manner.

b. Purpose Limitation: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c. Data Minimization: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

d. Accuracy: Personal data shall be accurate and, where necessary, kept up to date. Reasonable steps shall be taken to ensure that inaccurate or incomplete data is rectified or erased without delay.

e. Storage Limitation: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.

f. Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage.

4. **Data Collection and Use**

a. Consent: The Company will obtain clear and informed consent from individuals before collecting their personal data, and the purpose for which it will be used will be explained.

b. Data Minimization: Only necessary personal data required for the Company's operations will be collected, ensuring that it is relevant and limited to the intended purpose.

c. Lawful Basis: Personal data will only be processed when there is a lawful basis for doing so, such as the necessity for the performance of a contract, compliance with legal obligations, or consent.

d. Sensitive Data: Special categories of personal data, such as health-related information, will be handled with additional care and subject to stricter controls. Such data will only be collected and processed when it is essential and lawful.

5. **Data Security**

a. Access Controls: Access to personal data will be restricted to authorized personnel who require it to perform their duties. Access controls, including passwords and user permissions, will be implemented and regularly reviewed.

b. Data Encryption: Personal data stored or transmitted electronically will be encrypted to protect against unauthorized access or interception.

c. Data Storage: Personal data will be stored securely, whether in physical or electronic form, and protected against loss, theft, or damage.

d. Disposal of Data: Personal data will be securely and permanently erased when it is no longer required for the purposes for which it was collected, in accordance with applicable legal and regulatory requirements.

6. **Data Subject Rights**

a. Data Subject Requests: Individuals will be provided with the opportunity to exercise their rights under data protection laws, such as the right to access, rectify, erase, restrict processing, and object to the processing of their personal data.

b. Privacy Notices: Privacy notices will be provided to data subjects, clearly explaining their rights and how their personal data is processed.

7. **Data Sharing and Third Parties**

   a. Third-Party Agreements: Any third parties that process personal data on behalf of the Company will be required to sign data processing agreements that ensure compliance with data protection laws and this policy.

   b. Data Sharing: Personal data will only be shared with third parties when necessary and in compliance with applicable laws and regulations.

8. **Data Breach Management**

   a. Reporting: Any actual or suspected data breaches will be promptly reported to the appropriate data protection authorities and affected individuals, as required by law.

   b. Investigation and Response: The Company will investigate and respond to data breaches in a timely manner, taking appropriate actions to mitigate any potential harm and prevent future incidents.

9. **Staff Training and Awareness**

   a. Training: All employees, contractors, and volunteers will receive regular training on data protection, information governance, and GDPR compliance to ensure their understanding and adherence to this policy.

   b. Awareness: The Company will promote a culture of data protection awareness and encourage staff to report any potential risks, breaches, or non-compliance.

10. **Policy Review**

    This policy will be reviewed and updated periodically to ensure its ongoing effectiveness and compliance with changing legal, regulatory, and organizational requirements.

    By implementing this Information Governance and GDPR Policy, the Company aims to protect the privacy and rights of individuals whose personal data it processes and ensure the secure and responsible handling of information.