Community HeARTs Data Protection and Security Policy

1. **Introduction**
   1.1. Community HeARTs is committed to protecting the privacy and security of personal data. This policy outlines our procedures for data protection and security in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. **Purpose**
   2.1. The purpose of this policy is to ensure that all personal data is handled securely, responsibly, and in compliance with applicable laws and regulations. It provides guidelines for the collection, storage, processing, and disposal of personal data.

3. **Scope**
   3.1. This policy applies to all employees, volunteers, contractors, and partners who handle personal data on behalf of Community HeARTS. It covers all personal data processed by Community HeARTS, including data related to employees, volunteers, service users, and partners.

4. **Policy Statement**
   4.1. Community HeARTS is committed to:
   - 4.1.1. **Lawful Processing**: Ensuring that personal data is processed lawfully, fairly, and transparently.
   - 4.1.2. **Data Minimisation**: Collecting only the personal data that is necessary for specific, legitimate purposes.
   - 4.1.3. **Accuracy**: Keeping personal data accurate and up to date.
   - 4.1.4. **Storage Limitation**: Keeping personal data only for as long as necessary for the purposes for which it was collected.
   - 4.1.5. **Integrity and Confidentiality**: Ensuring proper security measures are in place to protect personal data.
   - 4.1.6. **Accountability**: Demonstrating compliance with data protection principles and maintaining records of processing activities.

5. **Data Collection and Processing**
   5.1. Lawful Basis for Processing
   - 5.1.1. Community HeARTS will ensure that personal data is processed based on one or more of the lawful bases outlined in the UK GDPR:
   - 5.1.2. **Consent:** The individual has given clear consent for the processing of their personal data.
   - 5.1.3. **Contract:** The processing is necessary for the performance of a contract with the individual.
   - 5.1.4. **Legal Obligation:** The processing is necessary for compliance with a legal obligation.
   - 5.1.5. **Vital Interests:** The processing is necessary to protect someone's life.
   - 5.1.6. **Public Task:** The processing is necessary to perform a task in the public interest or for official functions.
   - 5.1.7. **Legitimate Interests:** The processing is necessary for legitimate interests pursued by Community HeARTS a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

   5.2. Data Collection
   - 5.2.1. Inform individuals about the purpose of data collection, how it will be used, and their rights regarding their data.
   - 5.2.2. Obtain explicit consent from individuals when required.
   - 5.2.3. Collect only the data necessary for the specified purpose.

6. Data Processing

6.1. Process personal data in a manner that ensures security and confidentiality.
6.2. Use personal data only for the purposes for which it was collected.
6.3. Regularly review and update personal data to ensure its accuracy.

7. Data Security

7.1. Physical Security

7.1.1. Store physical records containing personal data in locked, secure areas.
7.1.2. Restrict access to physical records to authorised personnel only.

7.2. Digital Security

7.2.1. Use strong passwords and two-factor authentication for accessing digital systems.
7.2.2. Encrypt sensitive data to protect it from unauthorised access.
7.2.3. Regularly update software and systems to protect against security vulnerabilities.
7.2.4. Implement firewalls and antivirus software to protect against cyber threats.
7.2.5. Conduct regular security audits and risk assessments.

7.3. Access Control

7.3.1. Restrict access to personal data to individuals who need it for their work.
7.3.2. Implement role-based access controls to ensure employees can only access data relevant to their role.
7.3.3. Use access logs to monitor and review access to personal data.

8. Data Breach Management

8.1. Identifying and Reporting Breaches

8.1.1. Ensure all employees and volunteers are trained to recognise potential data breaches.
8.1.2. Report any suspected data breaches immediately to the Data Protection Officer (DPO).

8.2. Responding to Breaches

8.2.1. Investigate reported breaches promptly.
8.2.2. Assess the impact of the breach and take appropriate action to mitigate harm.
8.2.3. Notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of a breach, if required.
8.2.4. Inform affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

9. Data Subject Rights

9.1. Right to Access

9.1.1. Individuals have the right to access their personal data held by Community HeARTS.
9.1.2. Respond to access requests within one month.

9.2. Right to Rectification

9.2.1. Individuals have the right to request correction of inaccurate personal data.
9.2.2. Respond to rectification requests within one month.

9.3. Right to Erase

9.3.1. Individuals have the right to request deletion of their personal data under certain circumstances.
9.3.2. Evaluate and respond to erasure requests within one month.

9.4. Right to Restrict Processing

9.4.1. Individuals have the right to request restriction of processing under certain circumstances.
9.4.2. Evaluate and respond to restriction requests within one month.

9.5. Right to Data Portability

9.5.1. Individuals have the right to request transfer of their personal data to another organisation.
9.5.2. Provide data in a structured, commonly used, and machine-readable format within one month.

9.6. Right to Object

9.6.1. Individuals have the right to object to processing based on legitimate interests or for direct marketing purposes.
9.6.2. Evaluate and respond to objections within one month.

9.7. Rights Related to Automated Decision Making and Profiling

9.7.1. Individuals have the right to not be subject to decisions based solely on automated processing, including profiling.
9.7.2. Inform individuals about the logic involved and the significance and consequences of such processing.

10. Training and Awareness

10.1. Provide regular training on data protection and security to all employees, volunteers, and contractors.
10.2. Ensure staff are aware of their responsibilities under this policy and the UK GDPR.
10.3. Keep staff updated on any changes to data protection legislation or internal policies.

11. Monitoring and Review

11.1. Regularly review data protection and security practices to ensure ongoing compliance.
11.2. Conduct periodic audits to assess the effectiveness of data protection measures.
11.3. Update this policy as necessary to reflect changes in legislation or organisational practices.

Conclusion

Community HeARTS is committed to safeguarding personal data and ensuring compliance with data protection laws. By adhering to this policy, we aim to protect the privacy and security of all individuals whose data we handle.