Share with a Counsellor Data Protection Policy

1.0: Key details

Policy prepared by:	Share with a Counselor
Approved by board / management on:	1st December 2021
Policy became operational on:	1st December 2021
Next review date:	1st December 2022

2.0: Brief Introduction

Your privacy is imperative to our service provision; thus, we provide this privacy statement explaining our online activities and the alternatives you have on the way your information is collected and used through our websites into the mobile applications. The Platform is linking the public to the mobile phone app, website and Social Media platforms serving as the marketing tools. The systems are all information and data driven, hence the need to protect the Users with the Data Privacy and Protection Policy. This policy document describes how the personal data will be collected, handled, stored and archived to meet the company data protection standards and comply with the law. The essence of the data protection policy is to ensure the agency does the following:

- Complies with the Data Protection Act and other Data Protection Laws and follow good practice;
- Protects the rights of customers, staff, and partners;
- Ensures transparency on how it stores and processes individuals' data;
- Protects itself from the risks of data breach;

3.0: Definition of Terms

- **You/ Client/Customer-** Will refer to the User of any '*Share with a Counsellor'* platforms (social media & Website) through the mobile application services.
- **We or Agency**- Will refer to '*Share with a Counsellor'*, which is the business name through which mental wellness services are offered.
- **Partners**- Will refer to Institutions, Organizations, Companies, Donors and Groups of people contracting '*Share with a Counsellor'* to provide mental wellness services to their beneficiaries, clients or/and target groups.
- **Service Providers-** Will refers to professional individuals and companies/ business entities contractually engaged by the agency to offer specific services at an agreed fee.
- **Data Collectors and Processors-** These are companies or business entities contracted by the agency to support the administrative systems that receive, process, store, analyze data and generate reports using customer's data, during their interaction with the platform. These are also categorized as service providers who have the relevant licenses to offer the intended services.
- **Platform-** Will refer to the invisible system alignment coordinated through administration software and solutions to cause effective running of the intended functions through the Mobile Application.
- **Mobile Apps**- This makes reference to a software application to be used by both Android and iPhone mobile Users.
- **Data Protection Policy**- This a customized policy document by '*Share with a Counsellor'* to cushion the customers, partners and the agency and all rights are reserved to the Agency.
- **A Privacy Policy and Data Protection**- It is a statement or a legal document that states how a company or website collects, handles and processes data of its customers and visitors. It explicitly describes whether that information is kept confidentially or is shared with or sold to third parties.
- **Commissioners/Commission**- The assenting of the data protection act 2019, led to the establishment of the office of the Data Protection Commissioners, hence they form the commission that will be providing License to the data collectors and processors.

4.0: Data Privacy and Protection Policy

The Privacy and Data Protection Policy 2018 Kenya describes how organizations must collect, handle and store personal information whether electronically or physically. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed unlawfully**.** The Data Protection Act 2018 underpinned important principles, which we will adhere to the letter. The agency endeavors to ensure personal data is:

- Processed fairly and lawfully;
- Obtained only for specific and lawful purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Not be held for any longer period than necessary;
- Processed in accordance with the rights of data subjects;
- Protected in appropriate ways;
- Adheres to data privacy policy of target countries or blocks;

5.0: Use of Information

The agency may use and analyze customer's information for following purposes:

- Gain access to the Mobile Phone Application by using personal information to generate 'User Id' for future access to services.
- Enable Users to process and access required services and products offered in the platform.
- Facilitate billing processes and payment for services provided;
- Personal information like email addresses and phone numbers will provide the platform systems a medium to communicate with the Users via Chats, Short Messages, and/or email; and to respond to any customer's queries or concerns.
- Registration to required services centers and appropriate allocation of service providers.
- Verification of User identification information through publicly available and/ or restricted government database in order to comply with any legal, government or applicable regulatory requirements or use by lawyers in connection with any legal proceedings.
- In business best practices such as quality control, training, and ensuring effective system operation.
- To protect the Share Center which include managing the high volume of Calls, Chats and Texts Messages.
- To provide information to customers and guide their understanding of how to use the Agency network, products, and services for the purpose of developing or improving delivery.
- To communicate with customers or notify them on when there are upcoming events, new products, send notifications and to collect feedback about the Agency's products or services.
- Preventing and detecting fraud or other crimes and for debt recovery.
- For research, statistical survey, and other scientific business purposes.
- Provide aggregated data (it does not contain any information that may identify the customer as an individual) to third parties for research and scientific purposes.
- Administrate any of the Agency online platforms (Websites and Mobile App) where necessary.

6.0: Registration of Data Controllers and Data Processors

- Our website links customers to a mobile phone app service and online operations that are managed by service providers, who have all the required licenses and certifications from the Communication Authority of Kenya, the manufacturers of specific products and other online licenses. This is in adherence to the requirement by Data Protection Commission, to have all data controllers and data processors registered.

7.0: Safeguarding and Data Protection

- The Agency's Website and Mobile Applications have put in place technical and operational measures through service providers, to protect your information from unauthorized access, accidental loss, or destruction.
- The App Website and Mobile applications are operating on other agencies that are registered in Kenya, as business entities with all required certification/licenses. This is to ensure personal data is processed lawfully, fairly, and in a transparent manner in relation to any data subject.
- To ensure that data is collected, used and processed with care, every service provided to the public through the Mobile Applications have indicated a clear description of the data required, the importance of the data, access limits, privacy, storage, and liberty to edit and delete.
- The Website and Mobile Applications provide Users with General Terms and Conditions (T&C) governing the Website and all platforms, and simpler targeted T&Cs at account portals. Users are provided with free will and liberty to sign (Accept to adhere to the T&Cs) and proceed with access to services or terminate the process (by not Accepting the T&Cs).
- Accepting the T&Cs is consent by the User to provide the required data at different levels of the Mobile Application Service Centers; and it also allows the administrator free hand to use the data provided for the professionally intended purpose; remaining cognizant of the Data Privacy and Protection Policy guidelines.

8.0: Storage of Data/ Retention of Information

- There are no prescribed durations for the retention of personal data. Data controllers and processors are required to apply a reasonableness test in assessing retention durations.
- In the case of *'Share with a Counsellor,'* the Website and Mobile Phone Applications will be interacting with huge data that is stored in different virtual servers, owned by data controllers and processors. The Agency may not dictate the duration of retention of data in their server.
- However, the Agency in adherence to the American Psychologies Association (APA) guidelines that states "In the absence of a superseding requirement, psychologists may consider retaining full records until seven years after the last date of service delivery for adults or until three years after a minor reaches the age of majority. Therefore *'Share with a Counsellor'*, will keep client's data for 7 years for adults, in archives, after which it will be destroyed.
- Apparently, the Users have the liberty to delete personal accounts that contain their data and uninstall the Mobile Application, unconditionally, even after consenting and voluntarily providing the data to the Agency. This will erase their personal data from the local server accessible by the Agency solution.
- The voice over the internet either as video or audio will not be recorded by the Agency. The User personal data is only available to service providers at the specific interaction time, after which it is erased.
- The agency systems will retain customer's personal information for as long as is reasonably necessary to fulfill the purpose for which it was collected, including for the purpose of satisfying any legal, regulatory, tax, accounting or reporting requirement.
- Customer's personal data will be retained for a longer period in the event of a complaint or if there is a reason to believe that there is a prospect of litigation, in respect to the relationship between the involved entities.
- To determine the appropriate retention period for personal data, the Agency will consider the potential risk of harm from unauthorized use or disclosure of customer's personal data, the purposes for which the Agency processes the data, and whether the intended purpose is achieved through other means; the need to comply with the Agency internal policy and applicable legal, regulatory, accounting or another requirement.

- The public visible data is very minimal, because the Users will set account and the system will automatically generate a 'User id', these are the two identifiers that the User will interact with while in the platform. The identifier is geared towards protecting the identity of the Users.
- Except in the structured 'Therapy Service Centers', where the User will be required to complete an intake form that is visible to the professional providing the services to the client and the administrator; all other services are confidential.
- The Agency operations are executed virtually and therefore the platform relies on electronic mediums, concurring with the American Psychological Association (APA) in their website; "the advent of electronic health records has radically altered the documentation landscape. At a minimum, electronic records are subject to similar concerns and requirements as paper records".
- *'Share with a Counsellor'* operations will therefore, follows the provided guidelines by APA on managing information and electronic health records, such as using appropriate levels of encryption and passwords to protect digital information.
- Therefore, the User will set their own password to protect their account and a Pin to manage their e-wallet accounts and transactions, this keeps their data protected from external interference. They are also provided with the opportunity to reset those secret encryptions, with several levels of verifications in the processes.
- The system is also secure with different levels of firewall and protective measures to ensure Users' data is protected.
- The User is also limited in terms of the number of gargets they can be logged at a time to one, this will protect them from involuntary personal exposure of their personal data.
- Revealing of personal sensitive data is the last option in the process of lawful demand to disclose (Lawful Basis for processing your information).

9.0: Personal identifiable Information

- The mobile application services will require different data, some of which touch on the category of sensitive data, especially when completing the service intake form that allows Users to reveal a little more personal information to the professionals.
- This data is only accessed by professional practitioners, who are vetted, recruited and contracted to serve in the Agency.
- Each practitioner will only access the data of their specific clients with the coded identity, only the administrator has access to all the data in the system.
- During referral or linkage to other service providers, only the data clients provide voluntarily will be shared with the 3rd party, data in the platform will not be revealed to any other entity.
- The intake form for clients that serves as a consenting point, allows the agency to provide basic information during service linkage to different professionals within the agency.

10: Sensitive Data (Special Categories) Data

- The agency may collect special category of personal data about the User (this includes details about the customer's bio; home country, ethnic social origin/mother language; health/mental health status; conscience/ belief/religious faith; family history/genetic data; biometric /mental assessment data; criminal records/ offenses/ convictions; suicidal ideations; gender/sexual orientation; marital status; and family details that could include names of children, parents, spouse(s) are deemed sensitive data).
- This data will be handling with caution and the sensitivity it deserves, following mental health protocols available; for example, personal data relating to the health of a client will only be processed by or under the responsibility of a health care provider.
- The agency will rely on any legal basis provided to collect any more sensitive data, adhering to the professional code of conduct provided.

- Mental health services are a little intrusive and utilize a lot of sensitive data to understand the underlying issues, to offer appropriate intervention and identify appropriate linkage, referral and support system more data is required including a contact of one's support system.

11: Non-Personally identifiable Information

- The agency, advertisers, advertising networks and third-party service providers may collect information that is anonymous and not intended to personally identify the User, when you visit our website or use our Mobile Applications.
- Non- personally identifiable information likely to be obtained include: network or internet protocol address and type of browser you are using, the type of operating system you are using, the web pages you have visited, and the type of mobile device used to view our site, general location information etc.

12: Information from Social Networks

- Through our third-party social media plugins, we may request you to allow our website or mobile applications to gain access to your social media accounts, to allow you to access some services within the site/apps for example, request to make a comment, share articles and/ or engage with other Users, etc.
- Such a request will enable such services to have access to certain personally identifiable information and non-personally identifiable information from your social media profile (e.g., name, e-mail address, photo, gender, birthday, location, User files like photos and videos, your list of friends, people you follow and/or who follow you, the posts or the 'likes' you make, etc.).

13: Geo-location Information

- While using the Mobile Applications, you will be requested to share your Geo- Location information, this will enable the agency can customize your experience on our Apps.
- The future of the Agency is to link service providers and customers within the same geographical location for physical interaction.
- Referral services will be guided by physical location of the service providers and clients, hence the need for geo-location information of both.
- The Agency intends to use Geo-location information for services that benefit the User and to generate need-assessment data for future improvement of mental health accessibility and service provision.

14: Transfer of Personal Data outside Kenya

- The *Share with a Counsellor* website and mobile applications are utilizing service providers whose servers are in Kenya and others outside the country. Therefore, from time to time the Agency may need to transfer customer's personal information outside the Republic of Kenya.
- Wherever information is sent outside Kenya, the agency will ensure that personal information is properly protected in accordance with the applicable Data Protection Laws.

15: Exemptions

- On general exemption, the website and mobile applications will use data analytics in the platform to document best practices and emerging trends in mental health for purposes like lobbying, advocacy, and creation of awareness. This could be done through Journals, Study literature, Newsletters, Articles, or/and Blogs.
- Some of the data could be age, geo-location, gender, seeking services, web visits, Apps downloads, social media likes, sharing and subscription.
- The generated statistics will be documented and shared in public spaces to promote Evidence-Based Interventions (EBI's) that are scalable, cost-effective, and high impact; generate Social Behavior Change Communication (SBCC) campaigns messages.

- The consumers for these data include the Government, Policymakers, Donors, Local Non-Governmental Organizations (NGO's), Media, and Stakeholders in the specific areas of interest.

16: Lawful basis for processing your information

- The agency will process your personal information based on any of the lawful basis provided for, under the Data Protection Law:
    - The service agreement with the customer;
    - Legitimate business interest;
    - Compliance with a mandatory legal obligation;
    - Consent provided;
    - Public interest;
    - Customer vital interest;
- Access to such data outside the administration is limited to legal litigation, upon production of a court order, specifying the type of information required.
- In case of breach of confidentiality necessitated by 'life in danger' (suicide or homicide ideation) or criminal activities, the administrator will engage the required processes to address the matter, which may involve breaching the confidentiality but protecting the client.

17: Enforcement

- The Agency will be offering mental wellness services through the Mobile Applications, hence interacting with a lot of data; thus *'Share with a Counsellor'* is working with a legal advisor to ensure compliance with all the regulations and policy guidelines.
- The most important compliance document is a service agreement with all service providers, this Data Privacy and Protection Policy Document; Terms & Conditions.
- The security of data in the system is guaranteed by the service providers and therefore a breach of the User's data is a delegated liability to the service providers.
- However, the initial data between the Users, Professionals, and Agency system administrator, is a shared responsibility between the solution service provider and the agency.
- This allows the two parties to address imminent security concerns and possible system gaps that could compromise crucial data.
- The professionals serving in the agency must all sign the Privacy and Protection Policy Document; Terms & Conditions; Service Agreement Contract that stipulates consequences of breaching the contract.
- Therefore, the Agency will endeavor to protect the User's data at all levels and adhere to Government regulations and the Professional Code of Conducts.

18: Accountability

- In order to ensure accountability, the Website and Mobile Application management Agency has put together all the necessary mechanisms to promote and ensure accountability in the platform especially on policies, procedures, practices; and trade documents such as contracts with customers, partners and suppliers.
- The agency as well will monitor the implementation and maintenance of compliance with the Data Privacy and Protection Act at all levels.
- All service providers must sign a service agreement documents before rendering any services, and the policy document.
- All departments will have a System Operation Manual (SOP) document to guide their operations and implementers will be trained on their operation.
- The Mobile Application will ensure 95% of communication, services, payments, and documentation is done within the systems, this allows monitoring of activities, tracking of important trails especially in case of complaints by any party all in the spirit of accountability.

- The 5% will allow referral procedures where customers will be linked to service providers within their geographical location for physical interactions and service access.
- Within the same allowance, services can also, be offered by the Agency professionals outside the platform but with prior planning by the Agency system administrator.
- The Agency offers services through the Website and Mobile Phone Apps, hence working with legal advisors to ensure compliance with all the regulations and policy guidelines. The most important compliance documents are service agreements with all service providers; and Terms & Conditions for services offered under all platforms, for Users to read and accept.
- The User **Must** also read, understands, and accepts all terms and conditions set in the platform. Upon acceptance of the Terms and Conditions, the system will auto populate your name, phone number, date and time.
- The security of data in the system is guaranteed by the service providers (those operating as administrators of the operating systems), therefore a breach of User's data is delegated liability to the service providers, hence they are held liable.
- However, the initial data captured between the Users, Professionals, and Agency system administrator is a shared responsibility between the service providers of systems & solutions and the Agency.
- Thus, the two parties have a responsibility to secure their systems and protect User's data at all interaction points. Hence, the two parties have a duty to address imminent security concerns and possible system gaps that could leak out crucial data.
- The professionals serving in the Agency must all sign the data protection policy, and service agreement contract that stipulates consequences of breaching the contract prior to offering any services to the customers.
- Therefore, the Agency will endeavor to protect the User's data at all levels and adhere to government regulations.

19: The use of Hyperlinks

- The Agency Websites may provide hyperlinks to other locations or websites on the internet.
- These hyperlinks lead to websites published or operated by their parties who are not our affiliates or in any way related to us and have been included in our website to enhance Users experience with information only.
- The Agency does not endorse, recommend, approve or guarantee any third-party products and services by providing hyperlinks to an external website or webpage and does not have any collaboration with such third parties unless otherwise disclosed.
- We will not in any way be responsible for the content of any externally linked website or webpage.
- By clicking on a hyperlink, you will leave the *'Share with a Counselor'* webpage and accordingly, you shall be subject to the terms of use, privacy, and cookie policies of the other website that you choose to visit.

20: The Use of Cookies

- The Agency may store some information using ("cookies") on your computer when you visit our websites. This enables us to recognize you during subsequent visits.
- The type of information gathered is non-personal (such as the Internet Protocol (IP) address of your computer, the date and time of your visit, which pages you browsed and whether the pages have been delivered successfully.
- The Agency may also use this data in aggregate form to develop customized services-tailored to your individual interest and needs.
- Should any customer choose to allow the cookies, it is possible depending on the browser, to be prompted before accepting any cookies, or to prevent the browser from accepting any cookies at all. This however causes certain features of the website not to be accessible.

21: Customers Right

Subject to legal and contractual exceptions, the clients have rights under data protection law in relation to personal data. These are listed below:

- The right to be informed that we are collecting personal data about you.
- Right to access personal data that we hold about you and request information about how we process.
- Right to request that we correct your personal data where it is inaccurate or incomplete.
- Right to request that we erase your personal data noting that we may continue to retain your information if obligated by the law or entitled to do so.
- Right to object and withdraw your consent to the processing of your personal data, although the Agency may continue to process if we have a legitimate or legal reason to do so.
- Right to request restricted processing of your personal data, noting that we may be entitled or legally obligated to continue processing your data and refuse your request.
- Right to request transfer of your personal data in an electronic format.

If you do not agree with any section or/and statement within this Data Privacy and Protection Policy, which govern the operation of the Agency, please do not seek services or consume any product from any platform set within the trade name ***Share with a Counsellor.***

22: Disclaimer

If you wish to exercise any of the rights set out above, please contact us at *info@sharewithacounsellor.com* The agency may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. We try to respond to all legitimate requests within a reasonable time. Occasionally it could take us longer if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

23: How to Contact Us

If you would like to contact us on any topic in this Data Privacy and Protection Policy Document governing *'Share with a Counsellor'* Agency, you can email us at *info@sharewithacounsellor.com* or submit a request via our digital platform, or telephony.

Our contact details

Share with a Counsellor
P.O. Box 23952-00100
Nairobi, Kenya.

- Safaricom: 0707764498 (Call, Text and Telegram)
- Airtel: 0739 340004 (Call, Text and WhatsApp)
- Telcom: 0777543858 (Call and Text)

Email Address:
info@sharewithacounsellor.com

Consent

Name:..... Accept:..... Reject.....

Date: ..... Signature.....