S.O.S Needs
(Siblings of Special Needs)

DATA PROTECTION & CONFIDENTIALITY

DATA PROTECTION AND CONFIDENTIALITY

Objective:

To establish comprehensive guidelines for the secure handling of sensitive information, ensuring the protection of the privacy and confidentiality of beneficiaries, donors, and staff.

Policy:

- Data Privacy:
  - Sensitive Information Identification: All sensitive information, including personal data of beneficiaries, financial details of donors, and private staff records, shall be identified and classified according to the level of sensitivity.
  - Data Collection: Data collection processes shall be limited to the minimum amount of information necessary for the organization's operations, and consent shall be obtained from individuals before collecting their personal data.
  - Data Storage: All sensitive information shall be stored securely, using encrypted digital systems and locked physical storage to prevent unauthorized access, loss, or theft.
  - Data Transmission: When transmitting sensitive information, whether digitally or physically, secure methods such as encrypted emails, password-protected files, or secure courier services shall be used to ensure data protection.
  - Data Retention and Disposal: Sensitive information shall be retained only as long as necessary to fulfill its intended purpose, after which it shall be securely disposed of through methods such as data wiping, shredding, or incineration.

- Access Control:
  - Authorized Personnel Only: Access to sensitive information shall be strictly limited to authorized personnel who require it to perform their duties. Access levels shall be defined based on role requirements, ensuring that only necessary data is accessible.
  - User Authentication: All systems containing sensitive information shall require strong user authentication measures, such as multi-factor authentication, to verify the identity of individuals accessing the data.
  - Role-Based Access: A role-based access control (RBAC) system shall be implemented, ensuring that employees and volunteers can access only the specific information necessary for their role, and no more.
  - Audit Trails: An audit trail system shall be maintained to log all access to sensitive information, allowing the organization to track who accessed data, when it was accessed, and what actions were taken with it. Regular reviews of these logs shall be conducted to detect any unauthorized access or suspicious activities.
  - Access Revocation: Access to sensitive information shall be promptly revoked when an employee, volunteer, or contractor leaves the organization or no longer requires access to the data for their role.

- Confidentiality Agreements:
  - Mandatory Signing:
    All employees, volunteers, contractors, and any other individuals who may be exposed to sensitive information are required to sign a confidentiality agreement as a condition of their involvement with the organization.
  - Confidential Information:
    Employees, volunteers, and contractors acknowledge that during the course of their involvement with the Organization, they may have access to confidential information, including but not limited to data related to beneficiaries, donors, financial information, operational strategies, and intellectual property of the Organization.
  - Protection of Confidential Information:
    The Organization requires that all individuals maintain the confidentiality of all information disclosed to them, either directly or indirectly. This includes agreeing not to disclose any confidential information to any third party without prior written consent from the Organization.
  - Use of Confidential Information:
    All confidential information accessed by individuals during their time with the Organization shall be used solely for the purpose of performing their duties. The information must not be used for personal gain or for the benefit of any third party.
  - Agreement Content:
    Confidentiality agreements shall clearly outline the types of sensitive information covered, including but not limited to beneficiary data, donor information, financial details, operational strategies, and intellectual property. The agreement will specify the individual's responsibilities for protecting this information and the consequences of breaching the agreement.
  - Ongoing Obligation:
    The confidentiality obligations stipulated in the agreement extend beyond the individual's tenure with the organization, ensuring that sensitive information remains protected even after their departure.
  - Intellectual Property:
    Any intellectual property created, developed, or contributed to during the course of employment with SOSNEEDS shall be the exclusive property of the organization.

    Individuals are required to promptly disclose and assign any such intellectual property to SOSNEEDS.
  - Non-Solicitation:
    During the term of employment and for a period of 12 months after termination, individuals are prohibited from directly or indirectly soliciting, enticing, or encouraging any employee, contractor, or consultant of the organization to terminate their relationship with SOSNEEDS.
  - Return of Materials:
    Upon termination of employment or at the request of the organization, individuals must promptly return all materials, documents, and information, including copies or reproductions, containing or pertaining to confidential information or intellectual property.
  - Periodic Review:
    Confidentiality agreements shall be reviewed and updated periodically to reflect any changes in the organization's operations, policies, or applicable laws, ensuring continued relevance and effectiveness.
  - Enforcement:
    Strict enforcement measures, including disciplinary actions, termination, and legal recourse, are established for breaches of confidentiality or non-solicitation agreements, ensuring that all parties understand the seriousness of their obligations.
  - Governing Law:
    This policy and the related agreements shall be governed by and construed in accordance with the laws of the Federal Republic of Nigeria.

- Data Protection Training:
  - Regular Training: All staff and volunteers shall receive regular training on data protection and confidentiality policies, ensuring they understand their responsibilities and are equipped to handle sensitive information securely.
  - Awareness Campaigns: Ongoing awareness campaigns, including newsletters, posters, and workshops, shall be conducted to reinforce the importance of data protection and remind everyone of the best practices.
  - Incident Response Training: Employees shall be trained on how to respond to data breaches or incidents involving sensitive information, including how to report the incident, contain the breach, and mitigate potential damage.

- Incident Management:
  - Incident Reporting: A clear and confidential reporting process shall be established for any suspected or actual breaches of data protection or confidentiality, allowing staff to report incidents without fear of retaliation.
  - Investigation Procedures: All reported incidents shall be thoroughly investigated to determine the cause, impact, and necessary actions to prevent future occurrences.
  - Remediation and Notification: In the event of a data breach, affected individuals and relevant authorities shall be notified promptly, and steps shall be taken to remediate the breach and protect against further risks.