OSAAT Educational Charitable Trust
#108, 1st C Main Road, Jayanagar 7th Block, West of Kanakapura Road (Near Dig Vijaya Hospital) Email:info@osaat.org
Website: www.osaat.org Phone: +91-80-42646922

Data Privacy and Security Policy

Publish date : 20-Nov-2024

The OSAAT® organization consists of various resources both in India, USA performing various roles including fundraising, events, project management, accounts, civil engineering, IT program management, and others. Depending on the role they function in and also region/territory they work with, they could come across lots of sensitive and private information. Given that OSAAT® is a non-profit organization, it is not only the stated intent of functioning in a highly transparent, ethics driven manner - but when subject to audits, either internal or through 3rd party agencies, the organization has to demonstrate the practice of implementing such a policy.

Cloud Data Storage

Most of the data of OSAAT® is stored and shared via Google drive and emails. Other than that certain individuals based on their roles, functions, could be storing information on their personal devices and personal cloud storage as well. If the personal devices are issued by OSAAT®, such devices and data, security policies, anti-virus, data protection, backup could be governed by OSAAT® implemented policies. On the other hand, if data is being stored on personal devices owned by volunteers and other contributors, it is expected that such individuals will follow pragmatic approaches and guidelines in protecting such data and such individuals will be individually responsible. At no point in time the OSAAT® data be shared or used for personal gain without prior permission of OSAAT® officers. Any such misuse may result in disciplinary not limited to immediate termination and disciplinary action.

Access to different cloud folders (Google Drive folders) are provided by classifying different personnel to different groups (Google drive groups) and providing access to such marked folders in a restricted manner. The following sections illustrate different types of groups that may be required to set and restrict access to different Google Drive folders based on their role and function.

Classification of different data types and security needs

Data Type	Nature of Data	Roles/Personnel Restrictions
Sponsor /Donor personal information	Individual, company, personnel details, donation amounts, receipts, phone numbers, email addresses, PAN numbers, Aadhar numbers etc.,	Only Marketing, Legal, Accounts personnel, and Communications teams need access. Not for general volunteers and employees. General publications, exporting, and copying for non-organization purposes should be avoided and discouraged.
Project related Information	School data, location, Head master, contact numbers, email Ids, project information, plans, drawings, contractor/service providers details, PAN numbers, Aadhar numbers, GSTIN numbers, bills and invoices etc.,	Project Managers and Champions working with individual schools will need access. In general, all other volunteers may also need read access to understand templates, data samples, and processes.
Personnel Records of Employees, Contractors, Consultants, advisors.	Appointment letter, Terms of employment, PAN, Aadhar, Appraisals, Disciplinary notes, Home Address, email Ids, contact numbers, Family members, Remuneration, etc.	Only concerning reporting managers and directors, chief compliance/HR heads need to have access to such personal and private information. Personnel having access to such information should be aware of do's and don'ts with such data and ensure privacy and confidentiality. Also, bring violations of such practices to due leadership notice.
Financial Records	Financial statements, records, income & expenditure reports, Bank statements, remittances, withdrawals, access credentials, IT Returns. notices etc.,	Only finance and accounting personnel (individually) should have access to such data and records once they are archived (after the submission process). Other than published records for public, individual transactions, bank access credentials should not be accessible and available to personnel who are not performing such roles (unless authorized and required in a certain business context). Reports and statements are made available to general team members after due review and approvals to share the same.
Legal document	MOUs with donors, other legal documents, agreements with contractors, service providers etc.,	This will be with financial and Legal team along with the heads of the verticals (Digital and Physical)

Other documents	Event information, OSAAT® related brochures and other documents	All the members and volunteers will have access.

General guidelines

It is warranted that whosoever get any information relating OSAAT® that may be obtained from any source or may be developed in the course of their engagement with OSAAT®, by any means, during the period of their engagement or otherwise and is related either to the activities of OSAAT®, its donors, patrons, contractors, employees, consultants or other entities with whom they do business, information relating to its employees, or such other information that may be considered confidential by its very nature (**"Confidential information"**).

All such information shall be held as Confidential information in trust and and shall not be disclosed to any person, firm. company or enterprise, or use any confidential information for its own benefit or the benefit of any other party, unless authorized in writing by the competent authority of OSAAT®.

It is further warranted that such Confidential information shall continue to be governed by & in compliance with all applicable personal data protection and privacy laws of India and regulations (including but not limited to Information Technology Act 2000 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information Rules, 2011) including non-disclosure of any Personal Information.

"Personal Information" means information concerning a living person and includes the full name, date of birth, educational qualification, parental information, PAN number, Aadhar number, contact number, email Id, EPIC number and/or any other number, symbol or code, image or sound attributable to an individual that can be used to identify a particular person, and which is obtained in the normal course of their engagement with OSAAT®.