TeeTors

DRAFT

Data Protection Policy

1. **REFERENCE.** Currently this Policy is being updated to reflect requirements for the California Consumer Privacy Act https://oag.ca.gov/privacy/ccpa and the European Union General Data Protection Regulationshttps://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en . This initial phase is based on compliance with the New York State Information Security Breach and Notification Act of 2005 https://ag.ny.gov/internet/data-breach . A comprehensive update is targeted for 11/30/20. The intent of www.teetors.org, an "S Corporation" organized in the State of Virginia and physically headquartered at [insert address], is to employ regulatory compliance standards that meet the best practice for supporting its mentees, mentors, and user community.

2. **OVERVIEW.** Misuse, unauthorized disclosure, or compromised Personal and Private Information can post many legal, privacy and security risks; thus, it is important for users to understand the appropriate collection, use, storage, and disposal of Personal and Private Information.

3. **DEFINITIONS.**

3.1. **Personal Information.** shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

3.2. **Internal Information.** To include contact lists, correspondence, meeting minutes, procedural documentation, and trade secrets.

3.3. **Confidential Information.** To include educational information, employment information, legally privileged information, or subject to a confidentiality agreement.

3.4. **Private Information.** shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

3.4.1. social security number;

3.4.2. driver's license number or non-driver identification card number; or

3.4.3. account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

3.4.4. criminal background data, electronic credentials, medical information, and information of individuals under 13 years of age;

3.4.5. "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

4. **PURPOSE.** The purpose of this Data Protection Policy is to ensure the proper use of the Personal and Private Information that www.teetors.org collects and retains; and make users aware of what www.teetors.org deems as acceptable and unacceptable classification, collection, access, use, storage, retention, and disposal of such information.

5. **SCOPE.** This policy covers appropriate classification, collection, and usage of information and applies to all employees, vendors, and agents operating on behalf of www.teetors.org.

6. **POLICY.**

6.1. **Classification.**

6.1.1. **Public.** Public data is information that may be disclosed to any person regardless of affiliation with the company. Examples of Public data include company contact information, service offerings, and company certifications and affiliations.

6.1.2. **Internal.** Internal data is information that is potentially sensitive and is not intended to be shared with the public. Examples of Internal data include correspondence, meeting minutes, contact lists that contain information that is not publicly available, and procedural documentation that should remain internal.

6.1.3. **Confidential.** Confidential data is information that if made available to unauthorized parties, may adversely affect individuals or the company. This may include data that is required to be keep confidential, either by law or under a confidentiality agreement with a third party. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. Examples of Confidential data include legally privileged information, information subject to a confidentiality agreement, and personal information that is not otherwise publicly available.

6.1.4. **Restricted Use.** Restricted Use data includes any information that the company has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In certain cases, unauthorized disclosure or loss of this data would require the company to notify the affected individual and state or federal authorities. Restricted Use data should be used only as necessary and carefully protected. It should be encrypted both in transit and when stored. Examples of Restricted Use data include private information, criminal background data, electronic credentials used to authenticate individuals, protected health information, and financial account numbers.

6.2. **Labeling.**

6.2.1. Review what is currently stored for accuracy, relevancy, and completeness.

6.2.2. 'Title' will develop schedule to appropriately label information in accordance with 6.1 Classification.

6.3. **Retention.**

6.3.1. Review what is currently stored for accuracy, relevancy, and completeness.

6.3.2. 'Title' will develop schedule for periodic review of Personal and Private Information.

6.3.3. Personal Information will be maintained for XX years after individual leaves company.

6.3.4. Private Information will be maintained for XX months after individual leaves company.

6.3.5. Public information will be maintained for XX months.

6.3.6. Internal information will be maintained for XX years.

6.3.7. Confidential information will be maintained for XX years.

6.3.8. Restricted Use information will be maintained for XX years.

6.4. The below table identifies the appropriate method of collection, access, sharing, reproduction, sending, storing, auditing, incident reporting, and destruction for various classifications of data.

CLASSIFICATION	**PUBLIC**	**INTERNAL**	**CONFIDENTIAL**	**RESTRICTED USE**
COLLECTION	No restriction	No restriction	Reduce or eliminate data collection where not required for business function.	
ACCESS		Access should be provided as required to execute business functions.	Adhere to protocols to grant access to information on a need to know basis or a policy of least privilege; and revoke access upon change in employment status.	
SHARING		Share with employees as needed. Share with third parties as approved by supervisor.	If uncertain about who to share information with request clarification from supervisor. Some information may require a non-disclosure or confidentiality agreement.	
PRINT, COPY, SCAN		No restriction	Printer often store the printed document on a local hard drive potentially allowing unauthorized access to the information. Avoid printing data unnecessarily.	
SENDING		Send in a manner that protects it from incidental	Should be encrypted during transmission using secure email service if available.	

		or casual reading. Using some form of authentication to verify recipient.	Accessing data using smart phone/tablets through email puts that data at higher risk of unauthorized disclosure.
STORING		Stored in non-public location or meet a minimum standard of password protection i.e. requiring computer log in.	Information should be physically secured or encrypted. If using cloud services for storage, ensure access is restricted accordingly and that the cloud provider has proper credentials to store that information.
AUDITING		Conduct periodic reviews of where data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols. Verify procedures from granting and revoking access are accurate.	
INCIDENT REPORTING		Report any unauthorized disclosure or loss of this information to supervisor.	
DESTRUCTION		Physically destroy (i.e. shredder) or securely delete data using a secure erase tool. Do not destroy records subject to litigation hold, regulatory requirement, or company retention policy. Certain Confidential or Restricted Use records may require documentation of destruction.	

7. POLICY COMPLIANCE.

7.1. **Compliance Measurement.** The management team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

7.2. **Exceptions.** Any exception to the policy must be approved by the management team in advance.

7.3. **Non-Compliance.** An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Date: ____________________

Signature: ________________________________

Printed Name: ________________________________