Tech Trek California
Data Privacy and Protection Policy

December 24

Policy Brief and Purpose 3
Policy Scope 3
Terms and Definitions 3
Data Collection 6
Legitimate Purpose 6
Specific Protections for Minors 6
Demographic Information 6
Deidentification (Expert Determination) 6
Anonymization 7
Data Sharing 7
Internal Data Sharing 7
External Data Sharing 7
Data Retention and Destruction 8
Physical Printed Materials 9
Removable Electronic Media 9
Electronic Files 9
The Right to Be Forgotten 9
Categories of Data Classification 10
Personal Data (Personally Identifiable Information) (L1) 10
Highly Confidential Data (L2) 11
Company Confidential (L3) 12
Publicly Available (L4) 13
Reporting a Data Breach Incident 13
Policy Enforcement 13
Further Assistance 13

Policy Brief and Purpose

At AAUW California Tech Trek, we take privacy and security of personal data very seriously in accordance with AAUW's Privacy Policy. We are committed to continuously evaluating data protection as a global program while maintaining the highest levels of adherence to federal, state, and international regulations.

This policy is intended to instruct and establish proper handling standards to ensure the quality, integrity, and appropriate availability of TECH TREK data. This policy defines the responsibilities of TECH TREK, our staff, agents, and volunteers participating in our program in relation to the access, retrieval, transmission, storage, destruction, and retention of data to help ensure the safe, proper, and legal collection and processing of data across the TECH TREK California program.

Policy Scope

This policy applies to all data collected or processed to support the TECH TREK program. This includes data used in the administration, operations and development of the programs and supporting events. The policy covers, but is not limited to, data in any form, including data collected via registration systems, surveys, forms, audio-visual, third party, backup, archived data, or other data collected both electronically and on paper. The policy applies to all individuals who have access to TECH TREK data, including but not limited to employees, volunteers, and vendors and other entities that have a contractual obligation to provide or access data controlled or collected by TECH TREK related to their approved roles and responsibilities.

Terms and Definitions

(Note: **Bolded** words in definitions also have entries in this list.)

Anonymization is a type of data **deidentification** that permanently and completely removes personal identifiers from data through techniques such as suppression, generalization, or noise addition.

Anonymized data are data that can no longer be associated with an individual in any manner and are permanently stripped of personally identifying elements which can never be re-associated with the data or the underlying individual. In contrast to **personal data**, anonymized data are not protected by the GDPR or other privacy frameworks.

Children's Online Privacy Protection Act (COPPA) is a law created to protect the privacy of children under 13. The Act was passed by the U.S. Congress in 1998 and took effect on April 1, 2000. COPPA is managed by the Federal Trade Commission (FTC). Although nonprofits are exempt from COPPA, TECH TREK has elected to comply with COPPA.

Consent means a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of **personal data** relating to themselves or for minors they are lawfully permitted to consent on behalf of.

Data collection happens when a user deliberately offers or shares **personal data** – for example when filling out a registration form on a website.

Data controller refers to an entity that alone or jointly with others determines the purposes and means of processing **personal data**. TECH TREK is the data controller of record for all **personal data** collected from program participants via TECH TREK-managed systems including, but not limited to, CampDoc and third-party platforms controlled by TECH TREK. TECH TREK branch coordinators and Tech Trek alum group advisors may also be data controllers if they collect data outside of any Tech Trek systems for their internal purposes, such as the maintenance of local mailing lists and local consent forms.

Data minimization is the principle that **data controllers** should only collect and retain personal data which is necessary to complete the task for which the data was collected. Data controllers must only collect and process personal data that is relevant, necessary, and adequate to accomplish the purposes for which it is collected and processed.

Data owner describes the persons or departments who exercise operational authority for specified information and hold responsibility for establishing controls for its collection, processing, and dissemination.

Data processors refer to a third party, including vendors and other entities with a business relationship with a **data controller**, that **processes** personal data on behalf of a data controller. **Data Controllers** have a legal requirement in most jurisdictions to engage in **vendor risk management** to ensure that all data processors handle **personal data** securely and only process data according to the policies set forth by the data controller and agreed to by the **data subject**.

Data security refers to protection against unauthorized or unlawful **processing** and accidental loss, destruction, or damage of data. It covers actions taken to maintain the confidentiality, integrity, availability, and resilience of data systems. Data security encompasses the practices and processes that are in place to ensure that data is not being used or accessed by unauthorized individuals or parties. Data security includes aspects of collecting only the required information, keeping it safe, and destroying information that is no longer needed.

Data subject is an identified or identifiable "natural" person. In the context of privacy law and regulation, a data subject is a living human being whose **personal data** is held by a **data controller**.

Data subject rights refers to a person's ability to know how their personal data will be collected, shared, used, disclosed, and kept secure, and for them to exercise choice and control over these uses.

Deidentification refers to an action taken to remove identifying characteristics from **personal data**. Basic deidentification involves stripping out the names and obvious identifiers from data sets – essentially the removal of columns/fields in a dataset – but the rest of the data is left untouched. Basic deidentification doesn't always successfully **anonymize** data because it may be possible to align separate identified data sets with a deidentified ones. Other, more rigorous techniques may be required to fully **anonymize** data.

Expert determination is a process where a person with appropriate knowledge of and experience with generally accepted statistical and scientific **deidentification** principles determines the most appropriate method for rendering information not individually identifiable.

This person, through applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information, and documents the methods and results of the analysis that justify such determination.

Family Educational Rights and Privacy Act (FERPA) is a US federal law that establishes requirements regarding the privacy protection of student educational records. It applies to all academic institutions that receive funds under applicable U.S. Department of Education programs. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are referred to as "eligible students."

Lawful basis for data collection refers to the reasons that legally allow for the collection and processing of **personal data**. In general, TECH TREK relies on the explicit affirmative **consent** of **data subjects** to collect and process **personal data**. TECH TREK and our Program Delivery Organizations should collect only data that is required for the support, performance, or administration of TECH TREK programs, as described and allowed in the **TECH TREK Privacy Policy**.

List request is data requested by any individual working on behalf of TECH TREK, requiring information on youth, mentor/coach, volunteers, schools, etc. List request output is in the form of a list (e.g., rows of data identifying people, or teams or organization etc.) and not a summary of the data (total counts, %, averages, etc.) and may contain personal information. Each row of data is a record.

Personal data (also known as personally identifiable information or PII, or personal information) is information that can be used on its own or with other information to identify, contact or locate a single person or to identify an individual in context. Personal data includes data types such as name, email address, phone number, physical address, and government ID number, but it can also include any other information that is linked or linkable to an individual in context, such as medical, educational, financial, and employment information.

Processing means any operation or set of operations performed upon **personal data** or sets of personal data, that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of the personal data.

Pseudonymization replaces the most identifying fields in a database with artificial identifiers or pseudonyms. For example, a name could be changed to a unique number. The point is to make the data record less identifying, thereby reducing concerns about data sharing and data retention. It's important to know that pseudonymized data is not the same as **anonymized data**. Pseudonymized data retains a certain level of detail that allows tracking back of the data to its original state, whereas in anonymized data the level of detail is reduced so much that rendering a reverse compilation is impossible.

Pseudonymous data includes data or sets of data that have been amended so that no individuals can be directly or indirectly identified from those data without a "key" that allows the data to be re-identified. Pseudonymous data are treated as personal data because it is still possible to identify individuals using the key.

Third-party vendors, in the context of data protection and privacy, are entities external to TECH TREK who may collect, process, or store TECH TREK data. For example, Google drive, Waldo, Survey Monkey, Tableau, etc., may all be considered third party vendors and **data processors** for TECH TREK.

Vendor risk management is an assessment of a **third-party vendor** for the vendor's privacy and information security frameworks and policies, access controls, and other practices related to privacy and IT security. Privacy/security questionnaires, privacy impact assessments and other checklists can be used to assess this risk.

Data Collection

TECH TREK volunteers and entities with a specific contractual obligation working on behalf of TECH TREK may, with the affirmative consent of the data subject, collect data on persons, events, and business transactions. Basic contact information, such as name and email address, may be collected directly from individuals at outreach events; **it is our policy to collect only the minimum amount of contact information required to follow up with the person.**

Legitimate Purpose

The data must only be collected when there is a legitimate business purpose which is aligned with the business operations of TECH TREK. Legitimate business purposes for collecting information include, but are not limited to, the provision of safe and high-quality programs, customer communication, ongoing management of programs, planning financial and human resource activities, travel, state and national reporting, and evaluation.

Data collections must be designed to maximize their usefulness to serve multiple needs, both internal and/or external to TECH TREK. No collection process may generate a body of data which duplicates information already available within another collection.

Specific Protections for Minors

At TECH TREK, we regard anyone under the age of 18 to be a minor for the purposes of this policy. The TECH TREK data privacy program is primarily built upon the regulations set forth in COPPA and US state-level privacy laws for the protection of minors.

This strict adherence to these laws protecting minors requires that no employee, volunteer, vendor, supplier, or agent of TECH TREK collect any personal data (either on paper or electronically) without the affirmative consent of their parent or legal guardian for minors under age 18 beforehand. This includes, but is not limited to, registration data, contact information, and travel documents.

Youth under the age of 13 are not permitted to create accounts or provide their own personal data to TECH TREK under any circumstance; **personal data from youth under 13 may only be collected directly from a parent or legal guardian**.

The collection of personal data directly from minors ages 13-17 requires the affirmative consent of their parent or legal guardian.

It is the policy of TECH TREK that TECH TREK staff and volunteers should collect the personal data of minors only when obtained directly from their parents or guardians or consent is given by parents or guardians for the collection and use of minor's data.

Note: As a general rule, unless you have valid, affirmative parent/guardian consent for the collection and processing of a minor's personal data, you should not be collecting it.

Demographic Information

To protect the privacy of the TECH TREK community, it is our policy that any demographic reports issued to a third party do not contain identifiable information. To do so, we deidentify and aggregate those reports, and only create reports that contain information from ten (10) or more people.

Deidentification (Expert Determination)

It is our policy to deidentify data for demographic reports and archival purposes using the "Expert Determination" as a standard best practice to decide on the appropriate method of deidentification.

Anonymization

In certain cases, TECH TREK may require anonymization of data before it is used in a report or kept for archival purposes. Anonymization is the strictest type of deidentification that results in data that can no longer be associated with an individual in any manner. Both anonymization and other forms of deidentification aim to protect the privacy of data subjects at TECH TREK.

Data Sharing

It is the policy of TECH TREK that personal data can only be shared with persons or entities who have a specific and legitimate role that allows for such access, and have a legitimate business need to have access to such data. A legitimate business role or need may be demonstrated by items including, but not limited to, a memorandum of understanding (MOU) or sponsor agreement, a data processing or data sharing agreement, or a service contract or other business relationship.

To receive or process any personal data controlled by TECH TREK, all TECH TREK staff and volunteers must complete approved TECH TREK Data Protection and Privacy training and have an associated training completion record held by TECH TREK. **Sharing any company personal data with TECH TREK staff or volunteers who have not completed the appropriate training and do not have a legitimate business reason for access to the data is strictly prohibited.**

Requests from TECH TREK key donors and sponsors for TECH TREK personal data, particularly images and video, will be vetted by TECH TREK program. Any personal data shared with key donors and sponsors may only be used for celebration, advertisement, or promotion of TECH TREK programs, events, or scholarships; promotion and celebration of sponsor's work with and support of TECH TREK; or, for journalistic needs. **TECH TREK prohibits the use of any images for any commercial marketing or advertising.**

In special circumstances, TECH TREK may be required to share medical and non-medical incident information, including personal data, with outside entities such as insurers, venues or host sites, or law enforcement.

Internal Data Sharing

Google Drive and Zoom are the applications approved by for daily or ongoing internal data sharing with TECH TREK volunteers. Where appropriate, other applications may be approved by the program.

Personal data shared internally, including file sharing, may not be conducted through un- encrypted email. Unencrypted email is one of the most common ways data is breached from an organization. Applications that utilize encryption such as WhatsApp are preferred for sharing personal data.

External Data Sharing

It is the policy of TECH TREK to utilize Google Drive and Zoom wherever practicable for external data sharing. Encrypted email may be used for external data sharing when no other options exist, however, any files sent via email should be password protected. The passwords of protected files must not be sent together in the same email. Where possible, it is preferred that passwords are sent using text message, voice call or voicemail for added security. If text or voice messages are not feasible, passwords may be sent through email but only as a separate email with explicit instructions for the person to change the password at first use. **Note: Microsoft Excel does not support password protection on .csv files. You must convert the file to an Excel document (.xlsx) before applying the password.**

TECH TREK requires the use of BCC for all communications involving more than one (1) email address for parents, volunteers, and program participants including mentors/coaches **unless there is a legitimate business reason to share email addresses amongst the recipients.**

Data Retention and Destruction

It is the policy of TECH TREK to store and retain data in compliance with local, state, and federal regulations when and if it has a legitimate business reason to do so. Retention periods are defined below.

California Record Retention Schedule

Records shall be retained according to the following time periods:

Camper Information	
Application/Parent Guardian Certificate	2-3 years
Attendance Agreement	7 years
Transportation Plan	2 weeks post camp
Biographical information	2-3 years
Permission (photo and field trip)	In perpetuity
Incident reports	7 years
Early release	7 years
Camper evaluations	Purpose served
Camper contact information	10 years
Tracking campers	Purpose served
Volunteer/Staff Information	

Biographical information	Purpose served
Staff evaluations	Purpose served
Parent evaluations	Purpose served
JC recommendations	4-6 years
Live Scan report	3 years after last activity
Medical releases	7 years
Letter of Agreement	3 years post service
Branch Information	
Branch Reservation	
Camper Tracking Form	Purpose served
Transmittal forms	7 years
Branch Coordinator information	Purpose served

It is also the policy of TECH TREK to delete, remove, and destroy any data which is inaccurate, out of date, or does not have a legitimate business reason to retain. In the case where destruction is required, the following methods of destruction are approved.

- Physical Printed Materials: shall be disposed of by one (or a combination) of the following methods:
  - Shredding - Media shall be shredded using cross-cut shredders.
  - Shredding Bins - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor.
  - Incineration - Materials are physically destroyed using a licensed and bonded information disposal contractor.

Note: Safeguarding physical printed materials can be a unique challenge. No printed materials containing Personal Data (L1), Highly Confidential (L2), or Company Confidential (L3) should be left unattended. Materials should be accounted for and stored in a locked and secured case where possible while in transit or storage.

- Removable Electronic Media: Physical devices shall be disposed of by one of the methods:
  - Overwriting - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization. Overwriting must utilize a solution that makes a minimum of 2 sector overwrites.
  - Degaussing - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state.
  - Physical Destruction – Implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated.
- Electronic Files: Electronic files, including those in clouds, desktops, folders, or in email, shall be disposed of by one of the methods:

- Permanent Deletion – Deleting the file through the operating system or file explorer and permanently emptying the trash or equivalent backup. In the case of email, both the email and any attachment should be deleted as well as permanently emptied from the trash.

Note: Files containing any Personal Data must be destroyed after the completion of their intended use and may not be stored for archival or historical records.

The Right to Be Forgotten

It is the policy of TECH TREK to honor any personal request for erasure from any person it has collected and processed data on in accordance with this Policy. Anyone may request that their personal data at TECH TREK be deleted by emailing techtrek@aauw-ca.org.

To complete this process, the individual may need to provide their name, email address, phone number, and other identifiers. TECH TREK reserves the right to confirm their identity before taking any action to delete personal data. TECH TREK will assess each request to be forgotten on a case-by-case basis to determine the extent to which data can be deleted. In some cases, TECH TREK will remove personal data from requestor's record but may retain deidentified information. In some cases, such as when data has been collected as part of the Consent and Release forms or youth protection screening, personal data cannot be lawfully deleted.

It is critical to understand this "Right to Be Forgotten" process. As a representative of TECH TREK, you may be asked to fulfill this request. Please direct all such requests to techtrek@aauw-ca.org..

Categories of Data Classification

To protect the security, confidentiality, and integrity of TECH TREK data from unauthorized access, modification, disclosure, transmission, or destruction, as well as to comply with applicable international, federal, and state laws and regulations, all TECH TREK data are classified within security levels. To the extent practicable, data, repositories, or file names (both printed and electronic) must be correctly identified and labeled. List request output must be labeled in the title, footer, or cover page, as applicable. TECH TREK legacy systems will be evaluated on a case-by-case basis to determine the feasibility of placing warning notices to advise of sensitive data. As new systems that collect, store, or process L1, L2, and L3 data are adopted, they should be evaluated for compliance with this data classification and labelling requirement.

Note: Unclassified or unlabeled data is assumed to be L3 Company Confidential.

Personal Data (Personally Identifiable Information) (L1)

Personal Data (Personally Identifiable Information or PII) is any information about an individual maintained by TECH TREK, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date, and place of birth, mother's maiden name, or biometric records; or (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

At a minimum, Personal Data must be treated and handled as Company Confidential (L3), and elements of Personal Data may be classified as Highly Confidential.

Examples of Personal Data include, but are not limited to, the following data elements or categorizations:

- List request (e.g., rows of data identifying people, teams, or organizations, etc.) containing personal data.
- Name, such as full name, maiden name, mother's maiden name, or alias.
- Address information, such as a street address or email address.
- Telephone numbers, including mobile, business, and personal numbers.
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number.
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.
- Personal characteristics, including a photographic image (especially of the face or another distinguishing characteristic), fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry).
- Information identifying personally owned property, such as vehicle registration number or title number and related information.
- Linked Personal Data, information about an individual that is linked or linkable to one of the above (e.g., name and date of birth, name and place of birth etc.….., race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Access

Access to Level 1 data will be granted upon approval from the program director and a legitimate business reason to have access to the data. In addition, TECH TREK Staff must complete data protection training prior to accessing level 1 data and only access such data using TECH TREK credentials. Third party entities such as vendors or suppliers who have access to level 1 data must have proper data protection practices in place and have a signed agreement with TECH TREK that includes a confidentiality clause.

Storing

Personal Data will be stored on TECH TREK-supported servers, cloud infrastructure, and databases.

Sharing

Level 1 data can be shared in applications approved by the Data Governance Team. For a complete list of approved applications, to find out if an application has been previously approved, or to get a new application approved, please contact a member of the Data Governance Team to receive clarification or instruction.

Note: Personal Data may only be stored and transferred in encrypted formats and may NOT be transmitted through email.

Highly Confidential Data (L2)

Highly Confidential (L2) is a class of information that, if disclosed or modified without authorization, would have severe adverse effects on the operations, assets, or reputation of TECH TREK or our obligations concerning information privacy. Information in this class includes, but is not limited to:

- Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.
- Information deemed confidential by federal and state legislation
- Payroll, personnel, and financial information with special privacy requirements.

Access

Access to Level 2 data will be granted upon approval from the data owner and a legitimate business reason to have access to the data. In addition, TECH TREK Staff and Program Delivery Organizations must complete data protection training prior to accessing level 2 data and only access such data using TECH TREK credentials (e.g., @Tech Trekpartners.org). Third party entities such as vendors or suppliers who have access to level 1 data must have proper data protection practices in place and have a signed agreement with TECH TREK that includes a confidentiality clause.

Storing

Highly confidential data will be stored on TECH TREK-supported and/or approved servers, cloud infrastructure, and databases. In addition to the recommended locations, Level 2 data can also reside in applications approved by the Program Director. For a complete list of approved applications, to find out if an application has been previously approved, or to get a new application approved contact techtrek@aauw-ca.org.

Sharing

Level 2 data can also be shared in applications approved by the Data Governance Team. For a complete list of approved applications, to find out if an application has been previously approved, or to get a new application approved, please contact a member of the Data Governance Team to receive clarification or instruction.

Note: It is the recommendation of the Data Governance Team that whenever possible Highly Confidential data only be stored and transferred in encrypted formats, including the use of encrypted storage drives, and encrypted methods of transfer. Highly Confidential data may NOT be transmitted through unencrypted email.

Company Confidential (L3)

Company Confidential (L3) is a class of information that, if disclosed or modified without authorization, would have a serious adverse effect on the operations, assets, or reputation of TECH TREK, or TECH TREK 's obligations concerning information privacy. Company Confidential information is an information class used primarily for data that would harm the company, but not necessarily any individual person if unauthorized exposure occurred. Information in this class includes, but is not limited to:

- Corporate strategic documentation.
- Draft documents and policies not approved for distribution.
- Supplier contracts and communications.

This includes information that requires protection from unauthorized use, disclosure, modification, or destruction, but is not subject to any of the items listed in the Level 1 definitions above.

Access

Access to Level 3 data will be granted upon approval from the data owner and a legitimate business reason to have access to the data. In addition, TECH TREK Staff and Program Delivery Organizations must complete data protection training prior to accessing level 3 data and only access such data using TECH TREK credentials (e.g., @Tech Trekpartners.org). Third party entities such as vendors or suppliers who have access to level 3 data must have proper data protection practices in place and have a signed agreement with TECH TREK that includes a confidentiality clause.

Storing

Internal Use data can be stored in TECH TREK-supported applications, shared drives, and TECH TREK issued laptop or desktop computers. Copies of this data shall not generally be made unless business requires it.

Level 3 data can also reside in approved third-party hosted applications, but those applications must be approved by the Data Governance Team. Third-Party hosted applications that store this data must meet TECH TREK Data Privacy requirements and have signed an agreement with TECH TREK.

Hard copy (physically printed) data shall be stored in locked receptacles and rooms.

Sharing

Company Confidential data should be shared on TECH TREK-supported servers, cloud infrastructure and databases. Any data that is transmitted on a recurring basis to external vendors must be transmitted via SharePoint. Employees are permitted to transmit Level 3 data via unencrypted email when required and sent to a known third party that has an existing business relationship with TECH TREK.

Publicly Available (L4)

Publicly Available data is a TECH TREK category of information intended for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of TECH TREK, or the obligations of TECH TREK concerning information privacy. There are no restrictions on access, storing and sharing of L4 data.

Reporting a Data Breach Incident

In the event that Personal Data or highly confidential data is breached, you must immediately contact the Program Director at techtrek@aauw-ca.org or 619-431-2514. Data breaches include not only data stored on the cloud, server, computer, or other device, but also paper documents.

Policy Enforcement

All principles described in this policy must be strictly followed. A breach of data protection guidelines could invoke disciplinary action as outlined in the employee handbook and, in certain cases, possible legal action may be taken against any person who violates this policy. External partners/agencies must follow any agreements/contracts and are subject to audit and potential legal action due to policy violations.

Policy Review

The policy will be reviewed on a yearly basis. Notifications will be sent out when and if this policy is updated. TECH TREK employees who wish to make comments or suggestions about the Policy may forward them to the Data Governance Team.

Further Assistance

TECH TREK staff or volunteers who require assistance in understanding this Policy or need consultation are encouraged to contact the Program Director at techtrek@aauw-ca.org.