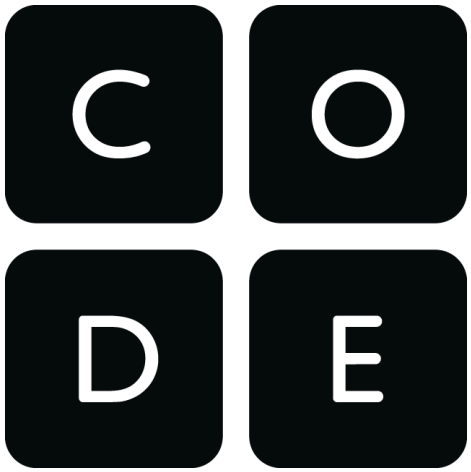

Code.org
Data Security and Privacy Plan

Last Updated: February 2026

1. Purpose and Scope

This Data Security and Privacy Plan (the “Plan”) establishes the policies, procedures, and technical controls that Code.org implements to protect the confidentiality, integrity, and availability of personal data collected and processed through its Services. The Plan reflects Code.org’s commitments as set forth in its publicly available Privacy Policy (available at https://code.org/en-US/privacy) and applicable data privacy agreements with schools and districts.

This Plan applies to all Code.org officers, directors, employees, agents, contractors, and third-party service providers who access, collect, store, process, or transmit personal data on behalf of Code.org. It governs all personal data processed across Code.org’s Services, including, but not limited to, the websites at code.org, studio.code.org, hourofai.org, curriculum.code.org, advocacy.code.org, k12cs.org, and any other online services that link to Code.org’’s Privacy Policy.

The objectives of this Plan are to: (1) ensure compliance with applicable federal, and state privacy laws, including FERPA, COPPA, and applicable state student data privacy laws; (2) establish clear data governance roles and responsibilities; (3) minimize the personal data collected and retained; (4) protect personal data through appropriate technical, administrative, and physical safeguards; and (5) ensure that a user’s data rights can be exercised effectively.

2. Organizational Overview

Code.org is a U.S.-based 501(c)(3) charitable nonprofit organization dedicated to expanding access to computer science in schools and increasing participation by young women and students from other underrepresented groups. Code.org’s vision is that every student in every school has the opportunity to learn computer science.

As a nonprofit, Code.org does not sell personal information or exploit it for financial gain. Code.org does not display advertisements on its Services. Substantially all of Code.org’s revenue is derived from philanthropic gifts and donations. This nonprofit structure is fundamental to ensuring that Code.org’s mission and user trust are never in conflict with a for-profit motive.

3. Privacy Principles

The following core principles guide all of Code.org’s data security and privacy practices:

- **Safe Learning Environment.** Code.org is committed to creating a safe and secure learning environment for students and teachers. Protection of personal information is treated as a foundational priority.
- **Data Minimization.** Code.org does not require personal information to try its courses. Accounts are only needed to save learning progress. Code.org collects only the data necessary to fulfill its educational mission.
- **Mission-Driven Collection.** The only reason Code.org collects data from students or teachers is to succeed at its mission of providing high-quality computer science education.
- **No Commercial Exploitation.** Code.org does not sell any personal information, does not display any advertising, and does not use student data for any targeted or behavioral advertising, profiling, or onward commercial disclosures.

- **De-Identification for Research.** Any student data provided to third-party researchers is limited to the non-commercial purposes of advancing computer science and de-identified per standard industry practice.
- **User Access and Control.** Code.org provides users with access to and control over the information they provide, including the ability to correct, update, and delete their data.
- **School Direction for Student Records.** When student records are provided by a school or district, Code.org retains such information as directed by the school or district.
- **Partner Accountability.** Code.org holds its service providers to the same privacy and security practices no less stringent than its own.

4. Regulatory Framework and Compliance

Code.org's data practices are designed to comply with the following key regulatory frameworks:

Regulation	Full Citation	Applicability
FERPA	Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)	Protects the privacy of student education records. Code.org acts as a "school official" under FERPA when processing Student Records on behalf of schools and districts.
COPPA	Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–6506)	As a nonprofit entity, Code.org is not subject to COPPA. However, Code.org voluntarily adopts practices that meet or exceed COPPA requirements for children under 13.
State Laws	Various state student data privacy statutes	Code.org's practices are designed to comply with state-specific student data privacy laws. User-provided state data allows Code.org to apply state-specific requirements.

Where Code.org has entered into separate student data privacy agreements ("DPAs") with local education authorities or similar entities, such as Code.org's Student Data Privacy Addendum, the processing terms of those agreements supplement this Plan.

5. Data Inventory and Classification

Code.org classifies data into the following categories to ensure that each type receives appropriate protections:

Data Category	Examples	Sensitivity
Student Account Data	Display name, username, password (hashed), age, state, one-way hashed email, parent/guardian email (optional), account identifiers, gender (optional), race (optional)	High
Student Academic / Progress Data	Course progress, lesson attempts, code submissions, assessment answers, projects (apps, animations, stories), survey responses	High
Student-Generated Content	Uploaded images/sounds/videos, free-text entries, data collected by student-created apps, written comments	High

Data Category	Examples	Sensitivity
Student Records	Personal data of students provided by or collected at the direction of a School, including all of the above when associated with a Teacher's section	Highest
Teacher Account Data	Email address, first and last name, school/district name and address, role, grades taught, subjects, verified teacher ID (temporary), section data, survey/demographic data	Moderate-High
Teacher Professional Learning Data	Workshop attendance, online PL progress, answers, documents, peer reviews, lesson plans, self-assessment results, comment feedback	Moderate
Technical / Operational Data	IP address, browser type, ISP, login times, clickstream data, operating system, cookies, pixel tags	Low-Moderate
Non-Curriculum / Contact Data	Names, email addresses, postal codes, billing/shipping info for donations/purchases, petition signatures, volunteer info, event registrations	Low-Moderate

6. Data Collection Practices

Code.org generally collects personal data through three channels: (1) information voluntarily provided by Users, (2) information automatically collected as Users interact with the Services, and (3) information from third parties (such as authentication services or LMS providers like Google Classroom, Clever, Canvas, or Schoology).

6.1 Data Minimization Measures

Code.org implements the following data minimization measures:

- No account is required to try Code.org courses or participate in Hour of Code tutorials.
- Student email addresses are never stored in retrievable form; only a one-way hash is retained.
- Code.org collects age (not birthdate), and does not collect student physical addresses or phone numbers.
- Payment instrument data (credit card numbers, wallet information) is never collected or stored by Code.org; donations and purchases are processed by third-party payment processors.
- Biometric and health-related data are not collected.
- Verified teacher identification documents are deleted immediately after verification is complete.

6.2 Third-Party Authentication and LMS Integration

When users register through an authentication service (Google, Microsoft, Facebook) or LMS provider (Google Classroom, Clever, Canvas, Schoology), Code.org receives, but does not share information with these third party services. Districts and schools may revoke Code.org's access at any time. Users may disconnect third-party services via account settings.

6.3 Cookies and Tracking Technologies

Code.org uses cookies, pixel tags (web beacons), and similar technologies to provide functionality, understand usage patterns, and ensure service reliability. Code.org does not use these technologies to

engage in third-party tracking for advertising purposes and does not display targeted advertising on the Services. Details are available in the Code.org Cookie Notice and the Hourofcode.com Cookie Notice.

6.4 Advertising Prohibition and Third-Party Embeds

Code.org does not allow advertising on its Services and does not collect web search history across third-party websites or search engines. Because Code.org does not display advertising or track browsing on third-party sites, it does not take different action in response to “do not track” signals transmitted by web browsers.

Code.org uses the embedded YouTube player in Privacy Enhanced Mode to deliver computer science videos within its curriculum. This means YouTube does not place cookies or track viewing behavior for advertising purposes. The student-facing curriculum does not embed any YouTube videos that are not part of the curriculum. The “rel” functionality of YouTube is disabled to prevent the embedded player from playing related content outside the curriculum, and all YouTube videos are tagged for “child-directed treatment.” Schools may also choose to block access to YouTube, in which case Code.org uses a fallback option that plays videos directly from its Services.

On student-facing course and activity pages, Code.org does not offer links to third-party social networking services (such as Facebook or Twitter) to students under the age of 13, or in schools that have blocked Internet access to those services.

7. Data Use and Processing

Code.org uses personal data for the following purposes:

- **Providing Services.** Operating the learning platform, saving progress, providing personalized learning experiences, and enabling teacher classroom management.
- **Communication.** Sending transactional emails (e.g., password resets, classroom updates) and, with opt-in consent, non-transactional updates about courses, professional learning, and computer science news. All non-transactional emails contain an unsubscribe link.
- **Professional Development.** Facilitating teacher professional learning workshops, tracking attendance and progress, and supporting coaching by Local Partners and facilitators.
- **Service Improvement.** Conducting internal research to improve, repair, or develop products, services, or technology; identifying and repairing technical errors.
- **Safety and Security.** Preventing, detecting, protecting against, and responding to security threats or incidents; performing internal operations.
- **Legal and Compliance.** Complying with applicable laws, responding to lawful requests, and enforcing Terms of Service.
- **De-Identified Research.** Publishing aggregated, de-identified data about student performance. Research partners agree not to attempt re-identification.

8. Data Sharing and Disclosure

Code.org will never share personal data with third-party organizations without user consent, except as described below. Code.org does not share personal data with donors or sponsors without explicit consent.

8.1 Authorized Disclosures

- **Third-Party Service Providers.** Code.org engages service providers (email platforms, analytics, LLM providers for AI-supported curricula, hosting, customer support) who may access personal data solely to provide contracted services under Code.org's direction. Providers are prohibited from using personal data for any other purpose.
- **Teacher–Student Sharing.** Student account information and course progress are shared with Teachers in whose sections the Student is enrolled. Students see limited Teacher information (display name, section info).
- **School and District Reporting.** Schools and districts may access reporting data on student progress and achievement at student, classroom, teacher, grade, or school levels.
- **Local Partners and Facilitators.** Limited teacher personal data (never student data) is shared with Regional Partners and International Partners for professional development support. Partners sign agreements requiring compliance with this Privacy Policy.
- **Publicly Posted Information.** Users may voluntarily post information publicly (e.g., teacher forum, school map, volunteer listings). Code.org clearly communicates what will be shared.
- **Legal Requirements.** Code.org may disclose personal data when required by law, court order, subpoena, warrant, or administrative request.
- **Protection of Rights.** Code.org may disclose personal data in good faith to protect against liability, fraudulent or abusive uses, third-party claims, or to protect the security or integrity of the Services.
- **Organizational Changes.** In the event of a merger, acquisition, or change of control, personal data may be transferred, subject to the same protections described in this Plan.
- **De-Identified or Aggregate Data.** Code.org may share de-identified or aggregate data that does not identify any individual for research, reporting, and service improvement.

9. Technical Security Controls

Code.org employs technical safeguards designed to protect the confidentiality, availability, integrity, and security of personal data. Code.org's security practices are generally aligned to the NIST Cybersecurity Framework.

Control	Description
Encryption in Transit	All personal information is encrypted in transit using TLS/HTTPS.
Encryption at Rest	All personal information is encrypted at rest using industry-standard encryption algorithms.
Hashing	Student email addresses are stored only as irreversible one-way hashes; clear-text addresses are never retained.
Hardened System Configuration	Production systems follow hardened configuration baselines with minimized attack surfaces.
Two-Factor Authentication	Two-factor authentication is enforced for privileged access to Code.org systems and infrastructure.
Patch Management	A patch management program ensures timely application of security updates across all systems.
Access Controls	Role-based access controls restrict system and data access to authorized personnel with a legitimate business need.

Control	Description
Monitoring and Logging	Security events and access to personal data are logged and monitored to detect anomalous activity.
Content Moderation	Automated text analysis and moderation in elementary school tools (Play Lab, Sprite Lab) helps prevent sharing of personal data such as email addresses and phone numbers.
Upload Restrictions	For students under 13, controls block sharing of projects containing custom uploads (images, sounds, videos).
Disaster Recovery	Disaster recovery processes are in place to ensure service continuity and data availability.

10. Administrative Security Controls

Control	Description
Employee Background Checks	Code.org conducts background checks on employees as part of the hiring process.
Security and Privacy Training	All Code.org staff receive security and privacy training. Officers, directors, employees, agents, and contractors are required to comply with this Plan and the Privacy Policy.
Confidentiality Obligations	All personnel with access to personal data are required to treat it as confidential information. Access requires a legitimate business reason related to Code.org's educational mission.
Support Representative Agreements	Support representatives (employees and independent contractors) sign agreements requiring protection and non-disclosure of confidential information, including user personal data.
Least Privilege Access	Access to personal data is granted on a need-to-know basis. Only personnel with a legitimate business reason may access user personal data.
Vendor Risk Management	Third-party service providers are contractually required to maintain privacy and security practices no less stringent than Code.org's own and to use data only for contracted purposes.
Policy Review Cadence	This Plan and supporting policies are reviewed and updated at least annually, or as required by changes in law or operations.

11. Physical Security Controls

Code.org implements physical safeguards to protect the infrastructure supporting its Services at its physical office location in Seattle, WA:

- **Data Center Access Restrictions.** Physical access to its offices and data centers hosted with Amazon Web Services (AWS) is restricted to authorized personnel only.
- **Environmental Controls.** Offices employ environmental protections including fire suppression, climate control, and power redundancy.
- **Office Security.** Code.org office facilities implement access controls to restrict entry to authorized personnel.

12. Student Data and School Records (FERPA)

When Code.org Services are used as part of a school's educational curriculum, personal data related to students may constitute "education records" under FERPA or be covered by similar state student data privacy laws. Code.org has implemented controls and procedures to help schools address their obligations under such laws.

12.1 Definition of Student Records

"Student Records" include personal data of students that is (1) provided to Code.org by a School or collected by Code.org during the provision of Services to a School, and (2) associated with accounts created by a School (e.g., teacher-created accounts or accounts created by students at the direction of a School using a school email address and associated with a Teacher's section). Student Records do not include information provided by a student independent of their school-directed use of the Services.

12.2 Code.org's Role

Code.org acts as a "school official" with a legitimate educational interest under FERPA when processing Student Records. Code.org uses Student Records solely to provide and improve its educational Services and does not use Student Records for any commercial purpose.

12.3 School Oversight and Control

- Schools and districts may access reporting data on student progress at student, classroom, teacher, grade, or school levels.
- Teachers may manage student accounts, reset passwords, view student projects and progress, and provide feedback.
- Schools may direct Code.org to share or delete Student Records in accordance with applicable DPAs.
- Districts or schools using third-party rostering services (e.g., Clever, Google Classroom) may revoke Code.org's access at any time.

12.4 Teacher Responsibilities

When registering an account for a student under 13, the Teacher represents and warrants that they or the educational organization has proper permission and has obtained necessary parental consent for collection of the student's personal information for the use and benefit of the school and for no other commercial purpose.

13. Children's Privacy Protections (COPPA)

Although Code.org, as a nonprofit entity, is not subject to COPPA, Code.org voluntarily adopts practices that meet or exceed COPPA requirements to protect children under 13. The following measures apply:

- Student email addresses are never stored in retrievable form; only irreversible one-way hashes are retained.
- Code.org collects age (not full date of birth) and does not collect student physical addresses or phone numbers.
- Public user profiles are not generally displayed. When student projects are featured, only the first initial of the student's display name and their age are shown.

- Online messaging between students is not supported, except through the teacher-supervised Internet Simulator tool in classrooms (messages auto-delete after two hours of class inactivity).
- Only students age 13 or older may post projects to social media accounts.
- In elementary school tools (Play Lab, Sprite Lab), text entered by students is automatically monitored and moderated to prevent sharing of personal data.
- When students under 13 upload custom images, sounds, or videos, they control block sharing of those projects outside the classroom.
- In jurisdictions requiring parental consent for child account creation, Code.org implements a consent flow via parent email and deletes accounts and associated data if consent is not received within the prescribed timeframe.
- Code.org restricts child account access to age-restricted features (e.g., sharing projects on social media).

13.1 Account Creation Methods for Children

Code.org strongly recommends that Teachers use one of the following account creation methods for classrooms with children under 13, rather than personal logins:

- Rostering via Google Classroom or Clever.
- Picture passwords or secret word passwords set by the Teacher (no personal information required).

14. State Student Data Privacy Compliance

Code.org fully complies with all state Student Data Privacy laws, including the California Student Online Personal Information Protection Act (SOPIPA.) Specifically:

- Code.org does not use, disclose, or compile personal information of K–12 students on the Services for the purpose of marketing or advertising commercial products or services.
- Code.org does not disclose personal information of students to third parties for marketing purposes.
- Code.org does not use student records for targeted or behavioral advertising, profiling, or onward disclosure for non-educational commercial purposes.
- Code.org does not sell student personal information.
- Code.org has signed the Student Privacy Pledge to further demonstrate its commitment to student privacy.

15. Data Rights

Code.org provides users (and parents/guardians of students under 18) with the ability to exercise the following rights with respect to their personal data:

Right	How to Exercise
Access	Users may access their personal data through their Code.org account settings page.
Correction / Update	Users may correct or update personal data through account settings or by contacting support@code.org.

Right	How to Exercise
Deletion	Users may delete their accounts and associated data through the account settings self-service delete function, or by contacting support@code.org. Teachers may request deletion of student accounts in their sections.
Appeal	Users who believe a request was improperly denied may appeal by emailing privacy@code.org. Code.org will respond within 45 days with a written explanation.
Data Portability	Due to the nature of the Services, data portability requests are considered on a case-by-case basis.
Opt-Out of Emails	All non-transactional emails contain an unsubscribe link. Unsubscribing does not require a password.

15.1 Identity Verification

Before processing data subject requests, Code.org verifies the requester's identity. For student accounts with a personal login, authentication is performed by requiring an email from the address used to establish the account (verified via the one-way hash). For teacher account requests, Code.org generally requires an email from the account's registered email address but may use alternative verification where additional teacher information is on file.

15.2 Parental Rights

Parents may access, control, and request deletion of their child's account by: (a) logging into the child's account and using the self-help delete function; or (b) contacting Code.org from the parent email address associated with the child's account at support@code.org. Where administrative controls are held by the School, parents should direct requests to the School.

16. Data Retention and Deletion

Code.org's approach to data retention is guided by the principles of data minimization and purpose limitation:

- **Active Accounts.** Personal data is retained as long as a user account is active, as long as the data is necessary or useful for operational purposes, or as required by contract or applicable law.
- **Inactive Accounts.** Code.org automatically deletes personal data associated with student or teacher accounts that have remained unused and inactive for a period of time in accordance with its data retention policies.
- **Deletion Requests.** Upon receiving a deletion request, Code.org processes the request promptly. A brief recovery period is provided after an online deletion to allow for account recovery. Users may request immediate permanent deletion by contacting support@code.org.
- **School-Directed Deletion.** Code.org may be contractually obligated to delete student accounts at a school's request, including accounts enrolled in a teacher's section even if using a personal login.
- **De-Identification.** As part of the deletion process, Code.org may de-identify data by removing identifiers to allow for ongoing research or product improvement (e.g., retaining a gender identifier for aggregate diversity analysis).
- **Non-Personal Data.** De-identified or aggregated data may be retained indefinitely as it is no longer personal data.

- **Certificate Data.** Certificate completion data is periodically deleted, which may affect the certificate sharing function.
- **Internet Simulator Messages.** All messages in the Internet Simulator tool are deleted after two hours of class inactivity or upon manual reset by the Teacher.
- **Petition Data for Minors.** When a user under 13 years of age signs Code.org's online petition, any name or email address is deleted from servers and never used.

17. Third-Party Service Provider Management

Code.org engages third-party service providers to support its operations. All providers are subject to the following requirements:

- Service providers receive access to personal data only to provide services for which Code.org has contracted and based on Code.org's direction.
- Providers are contractually prohibited from using personal data for any purpose beyond the contracted services without user consent or user direction.
- Code.org holds providers to privacy and security practices no less stringent than its own.
- Code.org maintains a publicly available list of third-party service providers.
- Research partners receiving de-identified data must agree in advance not to attempt re-identification of users.
- Local Partners (Regional Partners and International Partners) sign agreements requiring compliance with Code.org's Privacy Policy and treatment of shared information as confidential.

17.1 Third-Party Links and Services

The Code.org Services may link to, and may be linked from, websites operated by other entities or individuals. Some third-party websites, such as Code.org's social media pages, may be co-branded with Code.org's name or logo. Use of these third-party services is completely optional and typically intended only for adult users. These services are governed by the privacy policies of the respective third parties. Code.org encourages users to review third-party privacy policies before engaging with those services.

18. Incident Response and Breach Notification

Code.org maintains an incident response program to address data security incidents promptly and effectively.

18.1 Incident Detection and Response

Code.org employs monitoring and logging systems to detect potential security incidents. When an incident is identified, Code.org's incident response team is activated to investigate, contain, and remediate the incident.

18.2 Breach Notification

If Code.org learns of a data security incident that compromises or appears to compromise personal information of users or students, Code.org will:

- Attempt to notify affected users electronically so they can take appropriate protective steps.

- Notify affected schools and districts in accordance with applicable DPAs and legal requirements.
- Comply with all applicable federal and state breach notification laws, including timelines and content requirements.
- Cooperate with applicable regulatory authorities as required.

18.3 International Data Transfers

Code.org's Services are operated and managed on servers located within the United States. Users who access the Services from outside the United States acknowledge and consent to the transfer of their personal data to the United States. By providing personal data on the Services, international users provide their consent to that transfer.

18.4 Contact Information

Users who suspect a security incident or have privacy concerns may contact Code.org at:

- **Privacy inquiries:** privacy@code.org
- **General support and data requests:** support@code.org
- **Online request form:** https://code.org/contact

19. Training and Awareness

Code.org maintains a training and awareness program to ensure all personnel understand their responsibilities under this Plan:

- **New Hire Training.** All new employees and contractors receive privacy and security training as part of onboarding.
- **Ongoing Awareness.** Code.org provides periodic refresher training on data security, privacy practices, and incident reporting.
- **Role-Based Training.** Personnel with access to sensitive data or student records receive additional targeted training appropriate to their role.
- **Policy Acknowledgment.** All personnel are required to acknowledge and comply with this Plan and the Privacy Policy.

20. Plan Review, Governance, and Amendments

This Plan is a living document and is subject to periodic review and updates:

- **Annual Review.** This Plan will be reviewed at least annually by the Office of General Counsel and updated as necessary to reflect changes in law, regulation, organizational practices, or technology.
- **Ownership.** The Office of General Counsel is responsible for maintaining this Plan and ensuring organizational compliance.
- **Amendment Process.** Material changes to this Plan require review and approval by the General Counsel. Non-material clarifications and updates may be made by authorized personnel.
- **Privacy Policy Alignment.** This Plan is designed to implement and supplement Code.org's publicly available Privacy Policy. In the event of any inconsistency, the Privacy Policy as presented to users shall control.

- **Communication of Changes.** Material changes to this Plan or the Privacy Policy will be communicated to all affected personnel and, where appropriate, to users and partner organizations.
- **Student Records Change Notification.** Consistent with the Privacy Policy, Code.org will not make any material changes to the Privacy Policy relating to the collection or use of Student Records without first giving notice to the School and providing a choice before Student Records are used in a materially different manner than was disclosed when the information was collected.
- **Commitment to Existing Data Practices.** Code.org will not change how it uses personal data already collected from Users in any material way without providing notice of the change via email, through the Services, or through other means, and obtaining consent via the User's continued use.