OVERVIEW

CodeHS is compliant with NY Ed Law 2-d. Please submit your district's Data Privacy Agreement and Parents' Bill of Rights to hello@codehs.com for review. The following document provides the additional information requested under Ed Law 2-d.

In this packet:

- *Third Party Contractor's Data Security & Privacy Plan*
- *Third Party Contractors Supplemental Agreement*
- *CodeHS Privacy Policy*
- *CodeHS Incident Response Plan*
- *CodeHS Data Deletion Policy*
- *Schedule of Data*

THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN

Exclusive Purposes for Data Use

CodeHS will only use student data for the purposes outlined in this agreement and the CodeHS Terms of Use and Privacy Policy.

Data Accuracy/Correction Practices

Parents or students should contact their LEA directly with requests to challenge the accuracy of their data stored on CodeHS.

LEA privacy representatives should contact CodeHS at hello@codehs.com with any requests to correct data.

Subcontractor Oversight Details

CodeHS does not utilize subcontractors. Any subcontractors CodeHS uses in the future will be required to uphold privacy policies and procedures that are of an equal or greater standard than the terms of this agreement.

Current list of any subcontractors can be found at https://codehs.com/subcontractors.

Security Practices

Data is stored with Amazon Web Services ("AWS") in encrypted databases. All data and traffic are encrypted using HTTPS.

THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY SUPPLEMENTAL AGREEMENT

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

(i) Contractor will implement State and federal data security and privacy contract requirements for the duration of its contract that is consistent with the school district's data security and privacy policy by:

CodeHS Privacy Policy and Terms of use can be found at https://codehs.com/privacy and https://codehs.com/terms, respectively. All employees with access to data are trained to uphold these documented privacy standards and procedures, and all data is encrypted using HTTPS.

(ii) Contractor will use the following administrative, operational and technical safeguards to protect personally identifiable information:

All data and traffic are encrypted using HTTPS. Data is stored with AWS in encrypted databases.

(iii) Contractor has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information attached to its contract or written agreement with the District, or as follows:

CodeHS supplemental Data Security and Privacy Plan can be found above, on the first page of https://codehs.com/privacy/newyork.

(iv) Contractor's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:

All employees receive annual Cybersecurity training. All employees with access to PII receive training on confidentiality laws and company procedures to ensure that PII is kept secure and confidential.

(v) Contractor will use the following subcontractors and will ensure that personally identifiable information received by its subcontractors is protected, as follows:

CodeHS does not utilize subcontractors. Any subcontractors CodeHS uses in the future will be required to uphold privacy policies and procedures that are of an equal or greater standard than the terms of this agreement.

Current list of any subcontractors can be found at https://codehs.com/subcontractors.

(vi) Contractor will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the school district of any breach or unauthorized disclosure as follows:

CodeHS Incident Response Plan can be found below and is also available at [*https://codehs.com/incident_response*](https://codehs.com/incident_response)*.*

(vii) Data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated as follows:

Upon written request by the district, CodeHS will delete all student data.

CodeHS Data Deletion Policy can be found below and is also available at [*https://codehs.com/data_deletion*](https://codehs.com/data_deletion)*.*

CODEHS PRIVACY POLICY

About CodeHS

CodeHS, Inc. is a comprehensive online coding platform to help schools and districts teach computer science. The platform includes web-based curriculum, teacher tools and resources, and professional development.

Please read this Privacy Policy carefully before accessing or using the Website. In this Policy, we refer to these products as the "Website" or the "Services".

What is this policy all about?

This privacy policy (the "Policy") explains what data we collect, why we collect it, and what we do with it. It applies to you if you're a student, a teacher, or anyone else who uses our Website.

This Policy applies to information that we collect when you use our Services online. It does not apply to information we may collect offline or if you provide any information to a third party (including through any application or content that may link to or be accessible from the Website). We use the term "Personal Information" to refer to any information that would identify you as an individual (e.g. your name and/or email address).

By using the Service, you accept and agree to this Privacy Policy. Your use of the Service is also governed by the Terms of Use. You should read both of these documents together.

What information do we collect and why?

We aim to collect only the information necessary to provide you with a great learning or teaching experience. We receive and store any information you knowingly enter on the Services. We also receive and store some information automatically. The following section provides further explanation of what we collect and why.

Account information
When you create an account (as either a student or a teacher), you need to enter your name, a username, and your email address. For students in schools, you will enter a class code provided by your teacher to link your account to your classroom and your school. For teachers, you will be asked to provide information about your school so we can verify that you are a real teacher.

Technical data

As you use our Website, we may use automatic data collection technologies to collect information about your equipment, browsing actions, and patterns. For example, we may collect: details of your visits to our Website, including traffic data, location data, logs, and other communication data; and information about your computer and internet connection, including your IP address, operating system, and browser type.

The information we collect automatically is statistical data and does not include Personal Information. It helps us to improve our Website and to deliver a better and more personalized service, including by enabling us to:

- estimate our audience size and usage patterns;
- monitor site performance and uptime;
- resolving technical issue for Website users;
- store information about your preferences, allowing us to customize our Website for you; and
- recognize you when you return to our Website.

The technologies we use for this automatic data collection may include tools such as cookies and web beacons. Cookies are small files that websites place on your computer as you browse the web. Web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) are small electronic files that permit us, for example, to count users who have visited certain pages or opened an email and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity). You may choose to disable cookies in your browser settings. However, if you choose to do this, many of our Website's features may not function properly.

Coursework and grading

If you are a student, we collect information about your projects, including the responses you provide, how many attempts you made, and the time taken. This helps us to give you a great experience with our Service, including allowing you to save your work, helping us to improve our courses, and allowing teachers to assess and monitor students' progress.

Student code, programs, projects, and uploaded files

If you are logged in to your CodeHS account, we save the code and programs you have written. We do this so that teachers and students can revisit their work at a later time, and can continue working on their programs where they left off. As a student or a teacher, you can also upload content through the Website. If a student or teacher uploads content as part of writing a program, that content will be stored on the Website.

Student and teacher websites

As you work on CodeHS, students and teachers have the option to create personal websites. You can upload and create content on these sites, which will then become publicly available.

Messages

Students may send messages to their teacher through the Website, and a teacher may send messages to their students. In the case where an individual learner or school has specifically signed up for tutoring services, messages may be sent between students, teachers, and tutors. Only the participants in each of these conversations may see the contents of the messages.

Surveys and demographics

Occasionally we will send out optional online surveys to students asking for data such as age, gender, race and academic background. This data is only ever used in the aggregate and for the purposes of improving the Website and ensuring that we are reaching a diverse and representative group of learners.

Who can access your information?

We do not sell or rent your Personal Information to any third party for any purpose, including advertising or marketing. We do not allow any advertising on our services.

We restrict access to your information to CodeHS employees, contractors and agents who need to know that information in order to process it for us and who are subject to strict contractual security standards and confidentiality obligations. They may be disciplined or their contract terminated if they fail to meet these obligations.

Account information, coursework and grading, as well as student programs, projects, and uploaded files can be accessed by the student who created them and his or her teacher. Messages are accessible to participants in that conversation. All users of the Website must abide by the Terms of Use, which include obligations about interacting with other users.

We may disclose information that we collect or you provide as described in this privacy policy to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, in which Personal Information that we hold is among the assets transferred. This Privacy Policy will continue to apply to your information, and any acquirer would only be able to handle your Personal Information as per this Policy (unless you give consent to a new policy). We will provide you with prompt notice of an acquisition, by posting on our homepage, or by email to your email address that you provided to us. If you do not consent to the use of your Personal Information by such a successor company, you may request that the company delete it.

We may also disclose your Personal Information:

- to comply with any court order, law, or legal process, including to respond to any government or regulatory request;
- to ensure site security, or to enforce or apply our Terms of Use and other agreements, including for billing and collection purposes;
- if we believe disclosure is necessary or appropriate to protect the rights, property, or safety of CodeHS, Inc., our customers, or others; and
- to a state or local educational agency, including schools and school districts, for K-12school purposes, as permitted by state or federal law.

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

How do we store and delete your information?

Website users may update, correct, or remove Personal Information in their CodeHS accounts at any time via the Account Settings page.

Students and teachers may deactivate their account at any time from the Account Settings page.

A teacher or a student may request deletion of your own Personal Information by sending us an email at hello@codehs.com. In appropriate circumstances, teachers and parents may also request deletion of a student's Personal Information. IN SUCH CASE, WE WILL NO LONGER ALLOW THE APPLICABLE USER TO USE THE SERVICES. We will delete your or your student's information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion. When we delete a user's Personal Information, it will be deleted from our active databases but we may retain an archived copy of such user's records as required by law or for legitimate business purposes.

We will retain Personal Information, including after the school term in which a teacher or student uses the Services, for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. Generally, CodeHS will delete a user's Personal Information 4 years after the user's last login to the Services.

How do we protect and secure your information?

We have implemented reasonable measures designed to secure your information from accidental loss and from unauthorized access, use, alteration, and disclosure. Any payment information is transmitted using HTTPS encryption and is processed through Stripe, a third party payment provider. CodeHS does not directly collect or store payment instruments.

The safety and security of your information also depends on you. You are responsible for choosing a strong password and keeping it confidential.

If there is a data breach affecting your information, we will comply with any relevant legal or regulatory notification requirements.

Children under the age of 13

Because some of our users may be interested in it, we have included some information below related to the Children's Online Privacy and Protection Act ("COPPA"). COPPA requires that online service providers obtain parental consent before they knowingly collect personally identifiable information online from children who are under 13. Therefore, we only collect Personal Information through the Services from a child under 13 where that student's school, district, and/or teacher has agreed (via the terms described in the Terms of Use) to obtain parental consent for that child to use the Services and disclose Personal Information to us. A parent or guardian may sign up his or her child for the Services and provide Personal Information about that child to us. However, no child under 13 may send us any Personal Information unless he or she has signed up through his or her school, district or teacher and such school, district or teacher has obtained parental consent for that child to use the Services and disclose Personal Information to us. If you are a student under 13, please do not send any Personal Information to us if your school, district, and/or teacher has not obtained this prior consent from your parent or guardian, and please do not send any Personal Information other than what we request from you in connection with the Services. If we learn we have collected Personal Information from a student under 13 without parental consent from his or her parent or guardian or obtained by his or her school, district, and/or teacher, or if we learn a student under 13 has provided us personal information beyond what we request from him or her, we will delete that information as quickly as possible. If you believe that a student under 13 may have provided us personal information in violation of this paragraph, please contact us at hello@codehs.com.

If you are signing up for this service and creating accounts on behalf of student(s), you represent and warrant that you are either (a) a teacher or school administrator or otherwise authorized by a school or district to sign up on behalf of students or (b) the parent of such student(s). If you are a school, district, or teacher, you represent and warrant that you are solely responsible for complying with COPPA, meaning that you must obtain advance written consent from all parents or guardians whose children under 13 will be accessing the Services. When obtaining consent, you must provide parents and guardians with these Terms and our Privacy Policy. You must keep all consents on file and provide them to us if we request them. If you are a teacher, you represent and warrant that you have permission and authorization from your school and/or district to use the Services as part of your curriculum, and for purposes of COPPA compliance, you represent and warrant that you are entering into these Terms on behalf of your school and/or district.

Changes to the Privacy Policy

Our Privacy Policy may change from time to time. We will post any changes we make on this page with a notice on the Website's homepage that the privacy policy has been updated. If we make material changes to this Privacy Policy, we will email you at the email address associated with your account. You can access older versions of this Privacy Policy at codehs.com/privacy2013.

Questions?

To ask questions or comment on this Privacy Policy and our privacy practices, contact us at hello@codehs.com.

INCIDENT RESPONSE PLAN

This document describes the procedures CodeHS will follow in response to the report of a data breach or security incident.

Discovery and Response to Incident

1. If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.
2. If the person discovering the incident is not a member of the IT department or affected department, they will call the CodeHS Headquarters at 415-889-3376.
3. The headquarters office manager will refer to the IT emergency contact list or affected department contact list and call the designated numbers in order on the list. The grounds security office will log:
   a. The name of the caller
   b. Time of the call
   c. Contact information about the caller
   d. The nature of the incident
   e. What equipment or persons were involved?
   f. Location of equipment or persons involved
   g. How the incident was detected
   h. When the event was first noticed that supported the idea that the incident occurred.
4. The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could possibly add the following:
   a. Is the equipment affected business-critical?
   b. What is the severity of the potential impact?
   c. Name of system being targeted, along with operating system (if applicable), IP address, and location.
   d. IP address and any information about the origin of the attack.
5. Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
   a. Is the incident real or perceived?
   b. Is the incident still in progress?
   c. What data or property is threatened and how critical is it?
   d. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
   e. What system or systems are targeted, where are they located physically and on the network?
   f. Is the incident inside the trusted network?
   g. Is the response urgent?
   h. Can the incident be quickly contained?
   i. Will the response alert the attacker and do we care?
   j. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

6. An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
    a. Category one - A threat to sensitive data
    b. Category two - A threat to computer systems
    c. Category three - A disruption of services
7. Team members will establish and follow one of the following procedures basing their response on the incident assessment:
    a. Worm response procedure
    b. Virus response procedure
    c. System failure procedure
    d. Active intrusion response procedure - Is critical data at risk?
    e. Inactive Intrusion response procedure
    f. System abuse procedure
    g. Property theft response procedure
    h. Website denial of service response procedure
    i. Database or file denial of service response procedure
    j. Spyware response procedure.

    The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.
8. Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused.
9. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
10. Upon management approval, the changes will be implemented.
11. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    a. Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    b. Make users change passwords if passwords may have been sniffed.
    c. Be sure the system has been hardened by turning off or uninstalling unused services.
    d. Be sure the system is fully patched.
    e. Be sure real-time virus protection and intrusion detection are running.
    f. Be sure the system is logging the correct events and to the proper level.
12. Documentation—the following shall be documented:
    a. How the incident was discovered
    b. The category of the incident
    c. How the incident occurred, whether through email, firewall, etc.
    d. Where the attack came from, such as IP addresses and other related information about the attacker
    e. What the response plan was
    f. What was done in response?
    g. Whether the response was effective

13. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
14. Notify proper external agencies—team members will notify the police and other appropriate agencies if prosecution of the intruder is possible.
15. Review response and update policies—team members will plan and take preventative steps so the intrusion can't happen again. The following factors will be considered:
    a. Whether an additional policy could have prevented the intrusion
    b. Whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future
    c. Was the incident response appropriate? How could it be improved?
    d. Was every appropriate party informed in a timely manner?
    e. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
    f. Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    g. Have changes been made to prevent a new and similar infection?
    h. Should any security policies be updated?
    i. What lessons have been learned from this experience?

Notification to LEA

In the event that Student Data is accessed or obtained by an unauthorized individual, CodeHS shall provide notification to LEA within forty-eight (48) hours of discovering the breach.

1. CodeHS shall follow the process described below:
    a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
    b. The security breach notification described above in section (a) shall include, at a minimum, the following information:
        i. The name and contact information of the reporting LEA subject to the data breach.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
        iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
        v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
    c. At LEA's discretion, the security breach notification may also include any of the following:
        i. Information about what the agency has done to protect individuals whose information has been breached.

        ii.   Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. CodeHS agrees to adhere to all requirements in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. At the request and with the assistance of the District, CodeHS shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

f. In the event of a breach originating from LEA's use of the Services, CodeHS shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

DATA DELETION POLICY

This document describes the procedures CodeHS will follow regarding data deletion.

If a separate data privacy agreement is executed between CodeHS and a customer school or district, that agreement will take precedence over this policy.

End of Life Data Deletion

Upon written request from the LEA, CodeHS will dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account.

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses, Use of cookies etc.	X
	Other application technology meta data (specify):	X (Browser, OS used)
Application Use Statistics	Meta data on user interaction with application	X
	Standardized test scores	
	Observation data	
Assessment	Other assessment data (specify): Student Personality Assessments	
	Student school (daily) attendance data	
Attendance	Student class attendance data	X
Communications	Online communications that are captured (emails, blog entries)	X

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information (specify):	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	

Category of Data	Elements	Check if used by your system
Parent/ Guardian Contact Information	Address	
	Email	
	Phone	
Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
Category of Data	Elements	Check if used by your system
	Student scheduled courses	
Schedule	Teacher names	

Category of Data	Elements	Check if used by your system
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): First Generation College Student	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	X
	Student app username	X
	Student app passwords	X

		Check if used by your system
Student Name	**First and/or Last**	X
Student In-App Performance	**Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)**	X
Student Program Membership	**Academic or extracurricular activities a student may belong to or participate in**	
Student Survey Responses	**Student responses to surveys or questionnaires**	X
	Student generated content, writing, pictures etc.	X
Student work	**Other student work data (Please specify):**	
	Student course grades	

Transcript

Category of Data	**Elements**	**Check if used by your system**
	Other transcript data (Please specify):	
	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
Transportation	**Other transportation data (Please specify):**	
Other	**Please list each additional data element used, stored or collected by your application**	

	Student course data	X		
	Student course grades/performance scores			