DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Fort Plain Central School District Bill of Rights for Data Security and Privacy and Supplemental Information Agreement between Fort Plain Central School District and CodeHS, Inc.

1. **Purpose**

(a) Fort Plain Central School District (hereinafter "District") and CodeHS, Inc. (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the Data Security and Privacy Agreement").

(b) This Data Privacy and Security Agreement, is to ensure that the requirements of Section 2-d. This Data Privacy and Security Agreement consists of a Data Sharing and Confidentiality Agreement, and includes a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor.

(c) Vendor agrees that it will comply with all terms set forth in the Data Privacy and Security Agreement. To the extent that any terms contained in the Data Privacy and Security Agreement conflict the Vendor's online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Data Privacy and Security Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the, Data Privacy and Security Agreement, the terms of this Data Privacy and Security Agreement will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Data Privacy and Security Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Data Privacy and Security Agreement.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

(e) Notwithstanding the foregoing, the parties agree and acknowledge that de-identified, aggregate or anonymized data derived by Vendor from the information obtained in connection with the services: (i) is not personally identifiable information, Protected Data not confidential information of the District; and (ii) may be used by Vendor for its data analytics, marketing, research, or other business purpose in compliance with applicable federal and state laws, rules and regulations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Data Privacy and Security Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Data Privacy and Security Agreement , Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Data Privacy and Security Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within Data Privacy and Security Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Data Privacy and Security Agreement.

(c) Vendor will comply with all described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and

(ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release and the number and names of the schools and students affected.

(b) Vendor will provide such notification to the District by contacting Jessica Sanders, Data Protection Officer, directly by email at jessica.sanders@fortplain.org or by calling (518) 993-4000 ext. 1005.

(c) Vendor will cooperate with the District and provide as much information as possible directly to Jessica Sanders, Data Protection Officer, or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform Jessica Sanders, Data Protection Officer, or her designee.

6. **Additional Statutory and Regulatory Obligations** [1]

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Data Privacy and Security Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Data Privacy and Security Agreement to which this Exhibit is attached.

[1] Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Data Privacy and Security Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Data Privacy and Security Agreement.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

Data Sharing and Confidentiality Agreement

(continued)

Bill of Rights for Data Security and Privacy Fort

Plain Central School District

Parents and eligible students1 can expect the following:

1. A student's personally identifiable information (PII)2 cannot be sold or released for any commercial purpose.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.
3. State and federal laws,3 such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online at www.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.
6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

---

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.

[2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

[3] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.

BY THE VENDOR:

Miri Kudia

Name (Print)

Miri Kudia

Signature

Operations Manager

Title

3/11/2025

Date

Data Sharing and Confidentiality Agreement (CONTINUED)

Supplemental Information about a Data Privacy and Security Agreement between

Fort Plain Central School District and CodeHS, Inc. [2]

Fort Plain Central School District has entered into a Master Agreement with CodeHS, Inc., which governs the availability to the District of the following products or services:

CodeHS is a web-based platform that provides coding curriculum, teacher tools and resources, and teacher professional development.

Pursuant to Data Privacy and Security Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Data Privacy and Security Agreement.

[2] Each educational agency, including a school district, is required to publish a "Bill of Rights for Data Security and Privacy" on its website. *See*, Education Law Section 2-d(3)(a) and Part 121.3(a). The Bill of Rights [that is posted on a district's website] must also include "supplemental information" for each contract that the school district enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data [protected by Education Law Section 2-d]. *See*, Education Law Section 2-d(3)(c) and Part 121.3(c).

Nothing in Education Law Section 2-d or Part 121 requires an educational agency to post its third-party contracts on its website *in their entirety*. In addition, nothing in Education Law Section 2-d or Part 121 requires an educational agency to include the "supplemental information" about each contract, within the contract itself.

However, many school districts and other educational agencies have considered it a best practice to include most or all of the required elements of "supplemental information" within each applicable contract, and have complied with the obligation to include the "supplemental information" for each applicable contract with their

Bill of Rights, by posting *the text from this page of this Exhibit* from each applicable contract (or a link to this text) on their website in proximity to their Bill of Rights.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Data Privacy and Security Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Data Privacy and Security Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Data Privacy and Security Agreement commences on 3/10/2025 and expires on _____.
- Upon expiration of the Data Privacy and Security Agreement without renewal, or upon termination of the Data Privacy and Security Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.
- In the event the Data Privacy and Security Agreement is assigned to a successor Vendor (to the extent authorized by the Data Privacy and Security Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The

measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

CodeHS

New York Ed Law 2-d Compliance

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.

(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.

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
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify): Student Personality Assessments	
Attendance	Student school (daily) attendance data	
	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 Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
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
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	

Category of Data	Elements	Check if used by your system
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content, writing, pictures etc.	X
	Other student work data (Please specify):	
Transcript	Student course grades	
	Student course data	X
	Student course grades/performance scores	
	Other transcript data (Please specify):	

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

NIST CSF TABLE

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	4 - CodeHS keeps an inventory of devices used by employees and personal devices cannot be used without manager approval. Personally identifiable information of CodeHS students is never stored on employee devices. CodeHS does not utilize subcontractors but does utilize Amazon Web Services and Google as 3rd party systems to achieve business purposes.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	6 - The CodeHS company mission and values are communicated biweekly in each all staff meeting, the organization's quarterly and annual objectives are communicated in each all staff meeting, and staff responsibilities and stakeholders are managed by each team. CodeHS staff are trained on their responsibilities for protecting school data during onboarding and are required to sign our CodeHS Employee Student Data Confidentiality Agreement as a condition of employment.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	4 - CodeHS has documented and defined processes for student data confidentiality, data deletion, incident response, and internal documentation for federal, state-specific, and district-specific regulatory requirements that CodeHS employees must abide by
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	4 - CodeHS maintains an internal list of cybersecurity risks to the CodeHS service, infrastructure, and reputation, as well as steps that have been taken to mitigate risks. This document is continually updated and is used in employee onboarding and training.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	4 - CodeHS Leadership monitors the organization's risks and regularly meets to discuss and document our risk decisions.

	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	7 - The services provided by CodeHS do not depend on a traditional supply chain. The physical servers and databases the CodeHS service depends on are spread across multiple availability zones to ensure redundancy and availability, managed by Amazon Web Services, and CodeHS guarantees 99.9% uptime for its users http://status.codehs.com/
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	5 - Physical access to CodeHS web servers and databases is secured and managed by Amazon Web Services. Remote access is managed by AWS role based authentication to restrict access to only trained and authorized employees. CodeHS enforces 2 Factor Authentication for employee accounts across all web services. User identities are permissioned and bound to transactions within the CodeHS service.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	4 - CodeHS employees receive general cybersecurity training during onboarding as well as annual training for current employees. Role-based training is provided based on each employee's role and responsibilities. The CodeHS service itself teaches the fundamentals of cybersecurity and employees are additionally required to complete the curriculum we provide to our users.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	5 - All CodeHS data at rest is encrypted and protected by AWS. All database instances, logs, backups, and snapshots are encrypted using the industry standard AES-256 encryption algorithm. All CodeHS data in transit is encrypted over HTTPS. CodeHS development and testing environments are separate from the production environment. CodeHS uses AWS autoscaling and load balancing to ensure adequate capacity is maintained to keep CodeHS services available as traffic fluctuates.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	5 - CodeHS has a hardened baseline configuration rolled out across devices and critical assets as well as a documented, tested, and iteratively improved process for rolling out updates. CodeHS creates daily encrypted database backups in AWS and keeps them available for 30 days. CodeHS has a documented process for destroying user data by request as needed for privacy compliance. New staff are trained in cybersecurity policies and practices as part of onboarding as well as annually for current employees. CodeHS has a documented and tested Incident Response Plan: https://codehs.com/incidentresponseplan

	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	5 - Maintenance of the physical CodeHS system components is managed by AWS. CodeHS has a documented, tested, and iteratively improved process for rolling out maintenance updates to the CodeHS service itself that allows CodeHS to test and document changes before they are applied to the production environment, and have zero downtime for users. Maintenance that may result in downtime is rare, scheduled, and communicated ahead of time both on the CodeHS website as well as on http://status.codehs.com/ where anyone can subscribe to notifications.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	5 - CodeHS utilizes AWS security solutions including Amazon Web Application Firewall and Amazon CloudFront to log, detect, and block malicious web traffic including DDoS attacks. CodeHS uses AWS autoscaling and load balancing to ensure adequate capacity is maintained in normal and adverse conditions to keep CodeHS services available at all times.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	5 - CodeHS uses Amazon Web Application Firewall and Amazon CloudFront to log, detect, and block malicious web traffic including DDoS attacks. Incident alert thresholds are established and updated to notify CodeHS of anomalous events.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	4 - The physical environment that provides the CodeHS service is managed by AWS. AWS resources are remotely monitored and alerts are configured to identify cybersecurity events and verify the effectiveness of protective measures. CodeHS utilizes AWS Virtual Private Cloud to monitor connections to critical assets and ensure no unauthorized connections are possible.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	5 - Personnel roles and responsibilities for detection are established and understood to ensure accountability. AWS CloudWatch and Web Application Firewall rules are maintained, tested, and continuously improved to ensure awareness of anomalous events. Event detection is communicated both in well defined internal channels as well as externally via status.codehs.com
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	5 - CodeHS has a documented and maintained incident response plan that is executed by personnel during a cybersecurity incident
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	4 - CodeHS personnel know their roles and responsibilities and information is shared both internally and with external stakeholders in accordance with the CodeHS incident response plan

	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	5 - Personnel 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. The impact of the incident is determined and the incident is categorized in accordance with the CodeHS incident response plan
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	5 - Immediate action is taken to contain the impact of any incident and personnel will recommend changes to prevent the occurrence from happening again or infecting other systems. Upon management approval, the changes will be implemented and documented.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	5 - A post mortem is conducted after any incident to incorporate lessons learned, document what happened and what was done, and communicate changes made to prevent incidents in the future.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	5 - CodeHS has a recovery plan that is continuously maintained and executed after an incident. CodeHS personnel restore the affected system(s) to their uninfected state after an incident.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	5 - The CodeHS recovery plan is updated after a post mortem to incorporate lessons learned and update technologies, strategies, and processes going forward
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	5 - CodeHS is well aware of the effects cybersecurity incidents can have on the CodeHS reputation and has a plan in place to maintain public relations and communicate recovery activities both internally and externally according to our incident response plan.