



# GWC Clubs Data Privacy and Security Plan (NY § 2-d)

## **Overview**

Girls Who Code (“GWC”) is compliant with NY Ed Law 2-d. Below are materials provided by GWC for your Educational Agency (“EA”) to review in accordance with Ed Law 2-d. Additionally, please review the following links for additional information about GWC Clubs Data Privacy and how you EA can sign a Data Privacy Agreement/Addendum (“DPA”) with GWC.

## **GWC NY State DPA**

### ***Student Data Privacy Consortium DPA***

Girls Who Code is a member of the [Student Data Privacy Consortium](#) and utilizes the National Student Data Privacy Addendum for the state of New York. You can review the NY State NDPA for GWC [here](#). You can download the Eight State Data Privacy Addendum (which includes New York) in its entirety for your review and signature [here](#).

### ***Girls Who Code DPA***

Girls Who Code has a [standardized DPA](#) for districts not participating in the Student Data Privacy Consortium, located here. For NY State, this GWC Clubs Data Privacy and Security Plan is considered [Exhibit F](#) of that DPA and will be incorporated therein.

### ***District Specific DPA***

If you have a District Specific Data Privacy Agreement (and Parents’ Bill of Rights), please email them to [legal@girlswhocode.com](mailto:legal@girlswhocode.com) for review.

## **GWC Data Privacy and Security Materials**

GWC has a robust data privacy and security center, located [here](#). In addition to these materials, GWC is committed to the following:

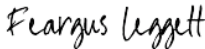
- GWC will only use student data for the purposes outlined in EA and GWC agreements and in the GWC Clubs Privacy Policy and Terms of Service.
- Parents or eligible students should contact their EA directly for questions about their data stored with GWC Clubs, and GWC will be responsive to the EA privacy representative (please contact us at [privacy@girlswhocode.com](mailto:privacy@girlswhocode.com)).
- GWC carefully tracks and monitors all data collected as part of GWC Clubs activities and does not sell data for commercial purposes. Please see the GWC Clubs Data Transparency Chart [here](#).
- GWC conforms with industry standard data security methodologies and process, including NIST framework. To learn more please visit the GWC Security White Paper [here](#).

**Please see the following pages for additional NYS Ed Law 2-d required documents.** For any further questions about GWC Clubs commitment to Education Law 2-d, please reach out to [privacy@girlswhocode.com](mailto:privacy@girlswhocode.com).

# EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children’s Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to EA at their email address and (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	<b>Feargus Leggett</b>
[Title]	<b>Chief Financial Officer</b>
Date:	<b>August 1,2024</b>

## EXHIBIT B

### BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	<b>Girls Who Code</b>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	<b>To deliver services and supports to schools hosting Girls Who Code Clubs.</b>
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date <u>  Upon Agreement  </u> Contract End Date <u>  End of Agreement  </u>
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties.</li> <li>• Securely delete and destroy data.</li> </ul>

<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input checked="" type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>We utilize data security framework (NIST) and monitor all data collection via our proprietary product developers (hosted on AWS) and in collaboration with third party cloud infrastructure (where we have contracts for data privacy and security in place).</p>
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

<b>CONTRACTOR</b>	
<b>[Signature]</b>	<i>Feargus Leggett</i>
<b>[Printed Name]</b>	<b>Feargus Leggett</b>
<b>[Title]</b>	<b>Chief Financial Officer</b>
<b>Date:</b>	<b>August 1, 2024</b>

## EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

### CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	GWC has a Clubs Privacy Policy at <a href="https://girlswhocode.com/clubs-privacy-policy">https://girlswhocode.com/clubs-privacy-policy</a> and a Clubs Terms of Service located at <a href="#">Clubs-Terms-of-Service-6-2-24.pdf</a> that highlight how we implement data security and privacy contract requirements. All employees of GWC with access to data are trained to uphold these standards and processes.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	GWC has a security white paper that outlines our safeguards, located at <a href="#">GWC-Security-Whitepaper-1.pdf</a> .
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All GWC employees receive training on applicable security practices and an annual cyber security training. GWC also has a Data Governance Committee to continuously update and notify staff of confidentiality and data privacy rules.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All GWC employees agree to confidentiality and data security as part of their employment via the GWC handbook. All subcontracts with access to data have written agreements in place. All subcontractors for GWC Clubs are listed on our Third-Party Contractor chart, located at <a href="https://girlswhocode.com/clubs-third-party-service-providers">https://girlswhocode.com/clubs-third-party-service-providers</a> .

5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	GWC has an incident response process which includes directly notifying the EA of any identified breaches, in alignment with the EAs processes.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	GWC has a Data Retention Policy and DPA terms that identify the timeline and process by which EA data will either be destroyed or returned to the EA.
7	Describe your secure destruction practices and how certification will be provided to the EA.	GWC has a Data Retention Policy located at <a href="https://girlswhocode.com/Clubs-Data-Retention-Schedule">https://girlswhocode.com/Clubs-Data-Retention-Schedule</a> .
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We are committed to meeting the standards of EAs through our data security practices (see white paper) and our focus on data governance and minimization (please see the Clubs Data Privacy Center at <a href="https://girlswhocode.com/clubs-privacy-center">https://girlswhocode.com/clubs-privacy-center</a> ).
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE SEE SECURITY WHITE PAPER.