

Parents' Bill of Rights for Data Privacy and Security

In accordance with New York State Education Law Section 2-d, the Nyack Union Free School District (the "District") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security, which is applicable to all students and their parents and legal guardians.

- (1) New York State Education Law Section 2-d ("Section 2-d") and the Family Educational Rights and Privacy Act ("FERPA") protect the confidentiality of personally identifiable information. Section 2-d and FERPA assures the confidentiality of records with respect to "third parties," and provides parents with the right to consent to disclosures of personally identifiable information contained in their child's education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In addition, the District will, upon request of parents, or adult students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll.
- (2) A student's personally identifiable information cannot be sold or released for any commercial purposes;
- (3) Personally identifiable information includes, but is not limited to:
 - i. The student's name;
 - ii. The name of the student's parent or other family members;
 - iii. The address of the student or student's family;
 - iv. A personal identifier, such as the student's social security number, student number, or biometric record;
 - v. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

- vi. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
 - vii. Information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.
- (4) In accordance with FERPA, Section 2-d and Nyack Public Schools Board of Education Policy number 5500 “Student Records”, parents have the right to inspect and review the complete contents of their child's education record;
- (5) The District has the following safeguards in place to protect student data, a Fortinet firewall, Intrusion Detection System, AES (Advanced Encryption Standard 256) bit for VPN encryption, SHA (Secure Hashing Algorithm) for VPN message integrity and file and folder security settings to restrict access and passwords protocol, including personally identifiable information stored or transferred by the District.
- (6) New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review, at [NYS SED Data Dictionary.pdf](#).
- (7) Parents have the right to submit complaints about possible breaches of student data or teacher or principal APPR data. Any such complaint must be submitted, in writing, to: Nyack Public Schools, Attn: Chief Privacy Officer, 13A Dickinson Ave, Nyack, NY 10960.

Supplemental Information for Third-Party Contracts

The Nyack Union Free School District (the “District”) has entered into contracts with certain third party contractors who have been sent student data and/or teacher data and/or principal data. The following information includes the list of vendors.

If a parent, student, principal, or teaching staff member would like to challenge the accuracy of data that has been collected they should submit a letter to the following address:

Nyack Public Schools
Attn: Chief Privacy Officer
13A Dickinson Ave
Nyack, NY 10960

(1) Infinite Campus

- a. Student Management system that keeps record of student demographic information, attendance, grades, health/immunizations, schedules and contact information.
- b. Infinite Campus will not share any student information or data obtained pursuant to its contract with the District to subcontractors, research institutions, persons or entities that are not directly an employee or department/office within Infinite Campus’s organization or the District, absent consent from the District, the applicable parent and/or eligible student unless required to do so to comply with legal process and/or a Court Order.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be stored on the District premises and is in sole ownership of the Nyack School District.
- d. During the term of and after this agreement expires, the student data is kept on the District property and is protected by a Cisco firewall and an Intrusion Detection System.

(2) STAR Renaissance

- a. Student assessment tool that helps educators build individualized instruction to accelerate learning for all students. Grades K-8.

- b. STAR Renaissance will not share any student information or data obtained pursuant to its contract with the District to subcontractors, research institutions, persons or entities that are not directly an employee or department/office within STAR Renaissance's organization or the District, absent consent from the District, the applicable parent and/or eligible student unless required to do so to comply with legal process and/or a Court Order.
- c. Absent renewal, this agreement expires on 30th day of June each year. After the expiration of this agreement, the student information becomes the sole ownership of the District.
- d. During the term of and after this agreement expires, the student data is kept at the Southern Westchester BOCES property and is protected by a Cisco firewall and an Intrusion Detection System.

(3) Pearson Education – SchoolNet

- a. Student data-driven educational software which aligns student assessment, curriculum and instruction; guides collaborative, data-informed discussion; and enables targeted instruction for every student, K-12.
- b. Pearson will not share any student information or data obtained pursuant to its contract with the District to subcontractors, research institutions, persons or entities that are not directly an employee or department/office within Pearson's organization or the District, absent consent from the District, the applicable parent and/or eligible student unless required to do so to comply with legal process and/or a Court Order.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be stored on the District premises and is in sole ownership of the District.
- d. During the term of and after this agreement expires, the student data is kept on the District property and is protected by a Cisco firewall and an Intrusion Detection System.

(4) Castle Learning

- a. Instructional support through online review and assessment for Social Studies, Math, English and Foreign Languages, grades 3 -12.
- b. The personally identifiable information supplied to Castle by the District will

not be given, sold, rented, loaned, or otherwise disclosed to any third parties outside of Castle or the District, except when Castle has the District's permission or under extraordinary circumstances, such as when Castle believes in good faith that disclosure is reasonably necessary to (i) comply with legal process, (ii) enforce the Terms of Use of its Agreement with the District, (iii) respond to claims that any content on the Castle web sites violates the rights of third parties, or (iv) protect the rights, property, or personal safety of Castle, its customers, or the public.

- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be removed from the Castle Learning system.
- e. All personally identifiable information is stored by Castle on servers at a location designed specifically to ensure that no unauthorized individuals have access to the server or its data at a co-location facility owned and managed by InetU, Inc., located at 744 Roble Road Suite 70, Allentown, PA 18109.

(5) Achieve 3000

- a. Differentiated online instruction to improve students' reading and writing levels and help to increase their literacy proficiency to reach the 1300 lexile level.
- b. Achieve3000 complies with applicable provisions of the Children's Online Privacy Protection Act (COPPA), which regulates how the operators of commercial websites directed to children may collect, use and disclose individually identifiable personal information concerning children.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be removed from the Achieve 3000 system.
- d. Achieve3000 ensures that all information that it receives is secure against unauthorized access by maintaining it on a secure system that is isolated from direct connection to the Internet. The servers are housed on the main property of Achieve 3000.

(6) Naviance

- a. Naviance is a college readiness platform that helps connect academic achievement to post-secondary goals

- b. Naviance has security measures in place to help protect against the loss, misuse and alteration of the data under Naviance’s control. When Naviance’s platform is accessed using a supported web browser, Secure Socket Layer (SSL) technology protects information using both server authentication and data encryption to help ensure that data is safe, secure and available only to authorized users.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be removed from the Naviance system.
- d. Naviance implements an advanced security method based on dynamic data and encoded session identifications, and hosts its college readiness platform in a secure server environment that uses a firewall and other advanced technology in an effort to prevent interference or access from outside intruders. The Naviance college readiness platform requires unique account identifiers, user names and passwords that must be entered each time a client or user signs on. These safeguards help to prevent unauthorized access, maintain data accuracy and ensure the appropriate use of data.

(7) READ180/Fastt Math/System 44

- a. A reading intervention system that builds fluency using adaptive software for assessment and instruction and print and multi-media materials
- b. Scholastic has policies and procedures in place and takes reasonable measures to protect the confidentiality, security and integrity of Personal Information collected on its site (like SSL encryption for transmissions of payment card information).
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be stored on the District premises and is in sole ownership of the District.
- d. During the term of and after this agreement expires, student data is kept on the District property and is protected by a Cisco firewall and an Intrusion Detection System.

(8) IEP Direct

- a. IEP Direct is a state-specific solution for managing Special Education programs

and IEP's.

- b. IEP Direct agrees to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of IEP Direct or the District who have been authorized by the District to have access. IEP Direct has agreed in writing to advise and require its employees, agents, and subcontractors to keep all personally identifiable student information and data confidential and shall be responsible to the District for any breach of this obligation by its employees, agents, and subcontractors.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be removed from the IEP Direct system.
- d. During the term of this agreement, student data is kept at the Southern Westchester BOCES property and is protected by a Cisco firewall and an Intrusion Detection System.

(9) Transfinder

- a. Transfinder is a school bus routing software application used for student transportation.
- b. Transfinder will not sell, rent, or intentionally disclose personal information that the District provides to it us, unless: (a) Transfinder is required to do so by law, regulation, warrant, subpoena or court order, (b) Transfinder is required in urgent circumstances to protect the personal safety of Transfinder employees, users of Transfinder products or services, or members of the public, or to enforce the Terms of Use of its Agreement with the District; or (c) such disclosure is part of a sale of all (or substantially all) of the assets of Transfinder.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be stored on the District premises and is in sole ownership of the District.
- d. During the term of and after this agreement expires, student data is kept on the District property and is protected by a Cisco firewall and an Intrusion Detection System.

(10) My Learning Plan

- a. My Learning Plan is a web-based educator evaluation and professional learning data management solution.
- b. The My Learning Plan website has security measures in place to protect the loss, misuse and alteration of the information under its control. My Learning Plan limits access to personal information to members of its staff who it believes reasonably need to come into contact with that information to provide products or services to the District or in order to do their jobs. My Learning Plan will not rent, sell, or share personal information about the District employees with other people or nonaffiliated companies.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be removed from the My Learning Plan system.
- d. Access to MyLearningPlan.com account information is password-protected so that only authorized users have access to personal information. During the term of this agreement, student data is kept at the Southern Westchester BOCES property and is protected by a Cisco firewall and an Intrusion Detection System.

(11) eChalk

- a. School, district and teacher web sites for communication and collaboration. Teachers and staff members use eChalk for e-mail, create class pages which can host a calendar of events (e.g.: homework), announcements and class resources from web sites to worksheets.
- b. The information obtained by eChalk from the District will not be given, sold, rented, loaned, disclosed to or shared with any third party except when consent has been provided or when it may be necessary for eChalk to comply with applicable law. Currently, eChalk does not use third parties to provide its services. If eChalk undertakes to do so, at all times, such third parties will be required to maintain the confidentiality of the information with which they may come in contact and will be prohibited from using the information for any purpose other than the purpose which is described above in subparagraph a.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be removed from the

eChalk system.

Each individual user account has a discrete user name to protect the identity of the user and all access is password-protected to prevent unauthorized access. In this way, only authorized members of the District are allowed to access or view any user information submitted as part of the eChalk system. eChalk employs individual password-protected accounts and Secure Socket Layer (SSL) encryption technology to ensure the privacy of any of the District's information.

eChalk's servers are housed in a data center with 24-hour, 365-day/year access and staffed to provide effective protection of all data as well as for maximum uptime and system protection. eChalk reviews its technology safeguards and measures on a periodic basis and strives to use industry-leading encryption technology to ensure the privacy of any user's online information. During the term of this agreement, student data is kept at the Southern Westchester BOCES property and is protected by a Cisco firewall and an Intrusion Detection System.

(12) Horizon – Solana/My Payments Plus

- a. Solana/My Payments Plus are a school meal application used for charging meals to student accounts.
- b. Horizon will not disclose your personally identifiable information to outside parties except: (i) to the extent necessary to provide you with a service you purchased from Horizon, which is provided by a third party under contract with Horizon, (ii) when we believe in good faith that any applicable law, regulation, or legal process requires disclosure; or (iii) when we believe disclosure is necessary to protect or enforce our rights or the rights of another customer. We may also collect customer information on an aggregate basis and disclose the aggregate data to prospective partners or other outside parties. Aggregate customer statistics are not personally traceable to you. We may also provide information to governmental agencies or other companies assisting us in fraud prevention or investigation, when: (1) permitted or required by law; (2) attempting to protect you, another customer or Horizon against actual or threatened fraud; or (3) investigating fraud that has already taken place.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be stored on the District premises and is in sole ownership of the Nyack School District.
- d. Access to Solana/My Payments Plus account information is password-protected so that only authorized users have access to personal information. During the term of this agreement, student data is kept at Horizon.

(13) Houghton Mifflin Harcourt - Journeys

- a. Journey's is an English Language Arts program designed for children ages Kindergarten through sixth grade.
- b. Houghton Mifflin Harcourt does not share Personal Information that they have collected from the District on our Service with third parties for those third parties' direct marketing purposes. To the fullest extent permitted by applicable law, Houghton Mifflin Harcourt may also disclose information if they believe in good faith that doing so is necessary or appropriate to: (i) protect or defend the rights, safety or property of us or third parties (including through the enforcement of this Privacy Policy, our Terms of Use, and other applicable agreements and policies); or (ii) comply with legal and regulatory obligations (e.g., pursuant to law enforcement inquiries, subpoenas or court orders). To the fullest extent permitted by applicable law, we have complete discretion in electing to make or not make such disclosures, and to contest or not contest requests for such disclosures, all without notice to you.
- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the student data will be stored on the District premises and is in sole ownership of the Nyack School District.
- d. Houghton Mifflin Harcourt incorporates commercially reasonable technical, physical and administrative safeguards to help protect and secure your Personal Information in their custody or control.

(14) Frontline Education – Aesop

- a. Aesop is an online attendance system that manages absence requests and finds substitutes for teaching staff.
- b. Frontline Education or Occam may disclose staff Personal Information to parties outside Occam when they have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Occam or its users; or (d) to protect Occam's property rights.

Where personal information has been requested by any governmental entity or other third party pursuant to subpoena or similar legal process, they will notify the staff member as quickly as practicable before providing any such information, unless they are legally prohibited from doing so or they believe in good faith that

disclosure is or may be necessary to protect life, avoid serious physical injury or property loss or damage, or to prevent or investigate an ongoing crime.

- c. Absent renewal, this agreement expires on the 30th day of June each year. After the expiration of this agreement, the staff data will be stored on the District premises and is in sole ownership of the Nyack School District.
- d. Frontline Education/Occam will retain staff Personal Information for as long as the account is active or as needed to provide services. If staff wishes to cancel their account or request that Occam no longer use staff information to provide services, the staff member may delete the account by sending Occam an e-mail at support@frontlinesms.com. Occam may retain and use staff information as necessary to comply with their legal obligations, resolve disputes, and enforce agreements. Consistent with these requirements, they will try to delete staff information quickly upon request.

Access to Frontline Education/Aesop is password protected so that only authorized users have access to staff information. During the term of this agreement, staff data is kept at Frontline Education.

(15) Schoology

- a. Schoology is a learning management system.
- b. Personally identifiable information from education records that are subject to the FERPA act Schoology will comply with the requirements and obligations under FERPA.
- c. This agreement expires on the 30th day of June each year.
- d. The school district owns all information regarding its schools or districts that it uploads to the Schoology system. Schoology shall implement commercially reasonable administrative, technical and physical safeguards for the protection of the security, confidentiality and integrity of the Subscriber Data.

(16) IXL Learning