


**DATA PRIVACY PLAN AND  
PARENTS' BILL OF RIGHTS FOR  
DATA SECURITY AND PRIVACY**

Pursuant to Section 2-d of the Education Law, agreements entered between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("PII") to contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy.

As such, Bond, Schoeneck & King, PLLC, being a third-party contractor ("Bond"), agrees that the following terms shall be incorporated into the contract for services ("the Contract") and it shall adhere to the following:


1. Bond's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here: <http://www.upreprochester.org/wp-content/uploads/2019/02/UPrep-Combined-Manuals-July-2017.pdf>.
2. Bond shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.
3. The student data or teacher or principal data will be used exclusively for the provision of legal services and advice only for the term of Bond's engagement as legal counsel for the District
4. The Contract shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:
  - a. PII data will be protected using encryption while in motion and at rest by hard drive encryption, TLS, AES-256, and HTTPS web encryption depending on the secure system used to transport or store the data.
  - b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored by saving to our document management system (highly secure with all activity logged) or our eDiscovery review platform (also highly secure and logged, accessible only by the Bond case team). The security of this data will be ensured by encryption and user access control.
  - c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows: Bond's Document Management System is multi-tiered to prevent all access to content except through the secure middle-tier. As such, all access to sensitive data is tightly controlled to the team working on the

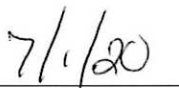
matter. In our eDiscovery platform, access to the encrypted sensitive data is restricted only to the matter team.

5. Bond shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.
  - a. By initialing here  Bond represents that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required pursuant to paragraph 6 below.
6. Bond shall ensure that all employees, subcontractors, or other persons or entities who have access to PII will abide by all applicable data protection and security requirements, including, but not limited to those outlined in applicable laws and regulations (e.g., FERPA, Education Law Section 2-d). Bond shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows: Through Bond's Privacy and Security Committee instruction and our On-Guard cybersecurity education system. All users must participate in the security and privacy education programs provided or their access to all Bond systems are revoked.
7. Bond shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, Bond shall notify the New York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.
8. Upon expiration of the contract, the PII will be returned to the District and/or destroyed. Specifically, in our Document Management System and our eDiscovery review system is either purged from our systems or exported and transferred to the District through the Kiteworks file sharing system or the secure system of its choice. Upon transfer, the data is purged.
9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected by contacting [Privacy@BSK.com](mailto:Privacy@BSK.com) or contacting the firm's CIO (Joe Fousek).
10. Bond shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII. Bond will follow their Incident Response Plan including the steps below.
  - a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Bond shall provide notification to the District's data privacy officer by phone and by email.
  - b. Bond shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.

- c. Where a breach or unauthorized release is attributed to Bond, Bond shall pay for or promptly reimburse the District for the full cost of such notification.
11. A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

The District shall publish this contract addendum on its website.

  
Vendor Signature

  
Date