

SUFFOLK TRANSPORTATION SERVICE INC.

Data Security and Privacy Plan

The following document is intended to comply, in all respects, with the requirements of New York State Education Law Section 2-d (*Unauthorized Release of Personally Identifiable Information*) and Commissioner's Regulations Sections 121.1, et. seq. (*Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information*) and to constitute the Data Security and Privacy Plan required of third-party contractors of school districts pursuant to said statute and regulations.

Suffolk Transportation Service Inc. ("Suffolk") is a corporation maintaining offices located at 10 Moffitt Boulevard, Bay Shore, NY 11706 which provides transportation services to school district students pursuant to contract. As such it comes into possession of or creates personally identifiable information ("PII") regarding students such as: name, address, email address, age, school attended, grade, athletic team and/or extracurricular activity participation, still and/or video photographs, medical alerts, and need for equipment and/or personnel and/or other accommodations.

The following is Suffolk's Data Security and Privacy Plan in connection with the specific requirement therefore of the school district ("District") to which this Data Security and Privacy Plan is submitted and to whose Data Security and Privacy Agreement with Suffolk it is intended to be attached. The italicized paragraph headings hereof are intended to reflect the subdivisions of Section 121.6 of the said Regulations addressed by the responses:

1. *How Suffolk will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the District's Data and Security Plan.*

Suffolk's data security and privacy practices are designed and implemented so as to comply with all applicable federal and state laws and regulations and District policies promulgated to comply with same and including, but not limited to, the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g), the Individuals with Disabilities Education Act (20 U.S.C. § 1400, et. seq.) and their implementing regulations, NYS Education Law Section 2-d regarding the Unauthorized Release of Personally Identifiable Information and Part 21 of the Regulations of the Commissioner of Education, and the District's Parents' Bill of Rights for Data Security and Privacy.

2. *What administrative, operational and technical safeguards and practices does Suffolk have in place to protect personally identifiable information it will receive under its contract with the District.*

Access to PII is based on a "least-privileged" model whereby individual Suffolk staff members are only provided that information necessary to complete their job functions.

Such PII, in paper form (“route book”) or contained on tablet devices, is maintained under lock and key when not in use and transmitted solely between Suffolk employees. Drivers obtain their “route books” upon signing in before their individual routes, keep them in their personal custody and control while students are on the bus and return them to their dispatcher when signing out at the end of their shift. Route books contain names and addresses and/or pick-up/drop-off locations of, and any medical and/or other special alerts/accommodations required for, individual students.

Under the direction and control of Suffolk’s Supervisor of Information Technology, such PII, in digital form, is maintained and transmitted in encrypted form and in alignment with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (“NIST CSF”). Suffolk’s policies and practices align with “Maturity Levels” of no less than 6 (to the extent applicable and except for RS “Communications” rated a 5). Access is password protected and limited to those staff to whom access is necessary to complete their job functions.

3. *How Suffolk will comply with its obligations under Section 121.3(c) of the Commissioner’s Regulations.*

Suffolk utilizes PII exclusively for the purposes delineated in and as defined by the District in the parties’ contract. The District does not provide Suffolk with teacher or principal data and Suffolk does not create such data.

Suffolk utilizes the services of subcontractors such as WheresTheBus LLC and Georef Systems Ltd. (“BusPlanner”) in performance of its student transportation contracts. Suffolk does not disclose PII to other persons or entities (i) without the prior written consent of the parent or eligible student (as provided by the District); or (ii) unless required by statute or court order and after providing notice of the disclosure to the District no later than the time the information is disclosed; unless providing notice of the disclosure is expressly prohibited by statute or court order.

When the contract between the District and Suffolk expires or sooner terminates, Suffolk will expeditiously destroy and/or delete all PII remaining in its possession.

Parent’s and eligible students may challenge the accuracy of PII in accordance with the procedures of the District in connection with same.

Suffolk maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of all PII in its possession.

Suffolk requires all who have access to PII to abide by applicable laws and regulations. Suffolk employees receive training concerning their obligations with respect to PII by way of postings prominently displayed in the workplace, periodic written communications, and in-person instruction/training at the time of initial employment and while on the job and during periodic refresher sessions.

Suffolk protects PII in physical form as described in answer to question 2. Digital PII while at rest and in motion is protected by way of encryption and/or firewall. Access to the PII on Suffolk servers is protected by the use of passwords and in alignment with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (“NIST CSF”).

4. *How Suffolk’s officers and employees who have access to PII will receive training on the federal and state laws governing confidentiality of PII.*

The District does not provide teacher or principal data to Suffolk. Suffolk neither subcontracts nor assigns its responsibilities under the contract with the District to any other entities or individuals.

Suffolk’s officers and employees who have access to PII receive training on federal and state laws governing its confidentiality and maintaining its security by way of in-person instruction/training and/or written materials provided at the time of their initial employment and periodically thereafter. In addition, information designed to inform and/or remind them of their responsibilities are also prominently posted in the workplace from time to time. Route and/or district supervisors are urged to review this policy and the agreement between the District and Suffolk regarding Data Security and Privacy (including the Parents’ Bill of Rights which forms a part of same) – and to certify their review and familiarity with the same. Such supervisory personnel are also required to provide on-the-job instruction and mentorship to staff under their control.

5. *How will Suffolk utilize subcontractors and how will it manage those relationships and contracts to ensure PII is protected?*

Suffolk utilizes the services of subcontractors such as WheresTheBus LLC and Georef Systems Ltd. (“BusPlanner”) in performance of its student transportation contracts. The contracts between Suffolk and both subcontractors obligates them, respectively: (1) to maintain industry-standard administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data [any data provided by Suffolk]; and (2) not to disclose student data to anyone without the written consent of Suffolk and permit Suffolk to visit its offices to ensure that student data is properly secured.

6. *How will Suffolk manage data security and privacy incidents that implicate PII and how does it plan to identify breaches and unauthorized disclosure and to promptly notify the District?*

Suffolk will notify the District of any confirmed breach of security resulting in an unauthorized release of PII in the most expedient way possible and without unreasonable delay.

7. *Will Suffolk return, destroy/delete, or transition data to a successor contractor when the contract is terminated or expires?*

Suffolk will expeditiously destroy and/or delete, as appropriate, all PII in its possession upon expiration or sooner termination of its contract with the District.