PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT

Section 2-c and 2-d of the New York State Education Law require that third party contractors, including casual employees, comply with the Parents' Bill of Rights and ensure privacy of any personally identifiable data shared under this contract. Contractor agrees to comply in every respect with all applicable provisions of section 2-c and 2-d of the NYS Education Law and any subsequently promulgated rules, regulations or laws regarding the same. Contractor has read the Parent's Bill of Rights and has read the District's Student Records Policy and agrees to fully comply with both including any amendments. For reference, the Parents' Bill of Rights is included below. The District will notify Contractor of any significant changes to either policy.

The City School District of Albany, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The School District establishes the following Parental Bill of Rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third-party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
- Parents have the right to inspect and review the complete contents of their child's education record;
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov.data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Ave., Albany, NY 12234
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be directed to the District's Data Protection Officer through submission of a form at https://www.albany.k12.ny.us/forms/dataprivacy, or in writing to the Data Protection Officer, 33 Essex Street, Albany, NY 12206. Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 5178-474-0937.

- Parents have the right to be notified in accordance to applicable laws and regulations if a

breach or unauthorized release of their student's PII occurs.

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII
- In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the District's Data Protection Officer.

For purposes of further ensuring confidentiality and security of student data - as well as the security of personally-identifiable teacher or principal data - the Parents' Bill of Rights (above) and the following supplemental information must be agreed to in order to access to this information:

Student Data Privacy Agreement

LinkIt hereinafter referred to as "Partner," has been engaged by the City School District of Albany to provide services. In this capacity, the company may collect, process, manage, store or analyze student and/or teacher/principal personally identifiable information (PII).

Partner will provide the district with *a data warehouse and MTSS solution that will receive PII data related to student assessment records, including student names, IDs, and demographic information. Additional student records, such as attendance, behavior and programmatic associations may also be sent to LinkIt! All such data shall be used and maintained as a service to school and district stakeholders authorized to access the same and exclusively for the purposes of analyzing the data for instructional improvement, professional development and resource allocation purposes, as well as other such purposes as the district may deem necessary and appropriate.*

Partner will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by *limiting production data access for subcontractors to "firecall" access only for a small number of individuals and requiring employees and subcontractors sign a NDA related to data handling. Any breach of this agreement is grounds for termination and the offending party may also risk criminal prosecution and civil penalties as a result.*

Partner by entering into an Agreement with the School District acknowledges it has reviewed the relevant District policies on safeguarding PII, including but not limited to, Policy 8635 and Regulation 8635.

PII will be stored: *in a manner consistent with industry standards and best practices on the industry-leading Amazon (AWS) hosting platform. The LinkIt! data and security model consists principally of the following:*

- ***Physical Security:*** *Web servers, data servers and network data storage are on servers maintained by AWS. We perform full daily backups and hourly incremental*

backups which are stored offsite in the event of a disaster. The data center is located in a secure area with restricted onsite access.

- ***Data Security:*** *LinkIt! utilizes industry-leading Microsoft SQL database that enables encryption in transit and at rest. Electronic access to database servers is restricted through dedicated web servers on a local network. This provides an effective barrier against attempts to directly compromise database integrity.*
- ***Web Security:*** *Our web layer consists of a passcode encrypted web service with enforced business logic. The business logic restricts user activity based upon permission level such that data access is limited to role within the LEA organization.*

Parents may challenge the accuracy of PII held by Partner by contacting t*heir authorized district representative, as LinkIt! security policy prohibits direct communication with parents regarding PII, legal and other sensitive matters. Authorized district personnel may contact the LinkIt! executive in charge of security and privacy using the contact information provided below:*

Karen Winter
CTO/CIO
karen@linkit.com
Ph: 917.583.4071

Partner will take reasonable measures to ensure the confidentiality of PII by implementing the following:

LinkIt! maintains strict privacy and security protocols that are established in accordance with industry standards. These include both technical safeguards and procedural safeguard with respect to data access and sharing procedures. More details on our plan may be found online at: https://www.linkit.com/privacy-policy, but included in such safeguards are the following:

- Password protections *(including strict requirements for strong passwords, two-factor authentication and VPN access controls)*
- Administrative procedures *(including limiting access to data to those individuals who reasonably require such access in the performance of their duties, requiring annual data and security training for all staff, signing NDA/privacy agreements with all staff and contractors, regular security audits and automated notifications, monthly penetration/vulnerability testing.)*
- Encryption while PII is in motion and at rest *(LinkIt! fully encrypts PII data both in motion and at rest in accordance with best practice)*
- Firewalls *(LinkIt! uses advanced firewall solutions provided by Amazon Web Services)*

Partner's agreement with the district begins on ***March 13, 2023***. Once Partner has completed its service to the district, records containing student PII will be ***returned*** *within 30 days following the termination of the engagement in a readable CSV format or in the format originally provided by the district to the extent that services are not renewed.*

_____ 3.10.23

Authorized Representative Date
Partner