

MEMORANDUM OF UNDERSTANDING
Between the Shared Learning Collaborative, LLC
And
Illinois State Board Of Education

A. Background.

1. The Shared Learning Collaborative, LLC (the “Company”) is designing and developing the Shared Learning Infrastructure (“SLI”), a system intended to support state and local education agencies in enhancing teaching and learning. The Company is a not-for-profit entity organized and operated to carry out the charitable and educational purposes of its members within the meaning of Section 501(c)(3) of the Internal Revenue Code of 1986.

2. The Company has launched the pilot phase of the SLI (“SLI Pilot”) in partnership with Illinois State Board of Education (“ISBE”) so that ISBE can inform the design and development of the SLI, offer to its school districts the educational benefits of the SLI, and extend the functionality and value of its current and future investments in state education technology infrastructure and initiatives (“State Ed Infrastructure”).

3. This Memorandum of Understanding (“MOU”) memorializes the Company’s and ISBE’s shared vision for the SLI, their understanding regarding the purpose of the SLI Pilot, and each organization’s role during the SLI Pilot. The parties understand that this MOU and its exhibits will be public documents and may be subject to disclosure under applicable state disclosure laws.

B. Understandings of the Parties

1. **Vision for the SLI.** The Company’s and ISBE’s vision for the SLI is a system of shared technology services, common to all states that adopt it, operated as a public good in a sustainable manner and that supports the following to enhance teaching and learning:

- a. *Personalized Learning Experiences.* The SLI is intended to link standards-aligned content from many providers to student data from many source systems and learning applications, allowing teachers to differentiate instructional practices and create personalized learning experiences for their students. (See Exhibits A and B for the Approach and Scope of the Technology Build.)
- b. *Educational content and instructional tools.* The SLI is intended to allow large and small for-profit and non-profit organizations to distribute an array of choices of curriculum, digital content and tools. (See Exhibits A and B for the Approach and Scope of the Technology Build.)
- c. *Alignment to the Common Core State Standards (“CCSS”).* The SLI is intended to support teachers in the implementation of CCSS in their classrooms, to support content developers in mapping their content to CCSS, and to be sufficiently flexible to support mapping of additional commonly adopted standards. (See Exhibits A and B for the Approach and Scope of the Technology Build.)

- d. Integration with State and Local Education Agency Data. The SLI is intended to integrate with existing state and local education agency source data systems and lower the costs of ongoing integration of new instructional technology products. (See Exhibits A and B for the Approach and Scope of the Technology Build.)
- e. Teacher Forum and Community of Practice. The SLI design contemplates supporting application providers that could provide teachers with the means to connect with colleagues and exchange information about such topics as educational products, tools, and teaching techniques. (See Exhibits A and B for the Approach and Scope of the Technology Build.)

2. **Design Elements of the SLI.** The Company intends that the design and development of SLI will incorporate the following design elements:

- a. Interoperability. The Company intends that the SLI support the interoperability of existing data systems, interoperability of content, and the interoperability of instructional tools and applications. (See paragraph B.3.b of this MOU and Exhibit B.)
- b. Accessibility. The Company intends that software components of the SLI developed by or on behalf of the Company will be available under an open source license, except to the extent that releasing that code puts privacy and security of student data at risk. Consistent with industry best practices, the Company will release code to the developer community in stages to ensure the vision for the SLI is understood by the developer community before release.
- c. Privacy and Security.
 - i. The SLI is intended to permit the Company, states, districts and schools to operate in compliance with the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, and the regulations promulgated thereunder (“FERPA”). The SLC intends to accomplish this by meeting the requirements of the Data Privacy and Security Plan, included herein as Exhibit C.
 - ii. For avoidance of doubt, each state, district, and school will be independently responsible for complying with FERPA and other applicable data privacy and security laws.
 - iii. For avoidance of doubt, if education records are disclosed to the Company or its contractors: (a) the Company is responsible for complying, and requiring that its contractors comply, with the provisions of, and the obligations imposed on, the Company or contractor under FERPA; and (b) the Company is responsible for providing, and requiring that its contractors provide, public access to its applicable data privacy and security policy.
 - iv. The Company’s contractors will not be permitted to share personally identifiable information with parent companies or other affiliates without the express written consent of the applicable state, district, or school that supplied the personally identifiable information. For purposes of this

Section, “personally identifiable information” includes, but is not limited to: any information defined as personally identifiable information under FERPA; names of teachers and other educators; and names of students’ parents (or persons in parental relationship to such students).

- v. Specific privacy and security obligations, including but not limited to, independent code and network security reviews following each major release (i.e., Alpha Release, Release 1.0, Release, 1.x, etc.) and no more than once in every six (6) month period thereafter, the existence and role of an independent advisory board, the ability to differentially delete data supplied by a state, school, or local education agency (LEA), and on-demand access to security and audit logs for independent review, will be addressed through data sharing agreements, as provided in paragraph B.3.f of this MOU.

3. **Purpose of the SLI Pilot: SLI Design, Development & Testing.** The Company and ISBE each acknowledges the purpose of the SLI Pilot is to develop, test and implement the SLI in a limited number of states including ISBE. The Company and ISBE each acknowledges the following:

- a. *SLI Design and Development Input.* During the SLI Pilot, the Company intends to gather input from SLI Pilot states, and ISBE intends to provide input to inform the design and development of the SLI. The Company intends to design and develop the SLI consistent with the terms of this MOU including but not limited to the “Approach to Technology Build,” included herein as Exhibit A, and the “Scope of Technology Build,” included herein as Exhibit B. ISBE intends to fulfill the requirements for state pilot participation consistent with the terms of this MOU, including but not limited to the terms set forth in Exhibit A.
- b. *SLI Design and Development Resources.* The Company intends to engage a number of vendors to participate in the design and development of the SLI.
 - i. The Company has engaged and will compensate Wireless Generation, Inc. (“WGen”) through a work-for-hire contract (“WGen Agreement”) to design and develop the software necessary to facilitate data integration and application interoperability. See Exhibit B, Scope of Technology Build. WGen will not own intellectual property or have operational rights to the software and has not been engaged to host data and applications.
 - ii. The Company intends to engage with a third-party provider, other than WGen, for data and application hosting during the testing and pilot phase of the SLI by issuing an RFP in the second quarter of 2012. Potential vendors include, but are not limited to, Rackspace Hosting, Microsoft Azure, and Amazon Web Services.
 - iii. The Company intends that most applications accessible via the SLI will be provided by state education agencies, local education agencies, or third-party educational technology providers. Nonetheless, the Company intends to engage vendors, including Intentional Futures, LLC and Double Line Partners, LLC, to develop three to four core teacher

applications that are of interest to the states participating in the SLI Pilot. These applications will be developed based on input from teachers in SLI Pilot states.

- iv. The Company intends to work in partnership with ISBE to help it secure commitments from education content application and technology services vendors, of particular interest to ISBE, to work in concert with the SLI.
 - v. The Company intends to rely on the Learning Resource Metadata Initiative (LRMI), a joint project of the Association of Educational Publishers and Creative Commons Corporation aimed at improving education search and discovery via a common framework for tagging and organizing learning resources on the web.
 - vi. The Company intends to leverage the Common Core Learning Maps, an application being developed by Applied Minds, LLC, to enable teachers and students to view individual student's progress toward mastery of CCSS and to access aligned content and learning applications.
- c. State Ed Infrastructure Integration. The Company intends to work with ISBE to complete a technology landscape of ISBE's State Ed Infrastructure and to determine the appropriate level of integration and relationship between the SLI and ISBE's State Ed Infrastructure. The Company and ISBE intend for that landscape to assist ISBE in identifying i) the interdependencies between the SLI and the State Ed Infrastructure, and ii) the opportunities for ISBE to leverage the SLI and reduce the scope of ISBE's investments in State Ed Infrastructure. Additional interdependencies of the State Ed Infrastructure on the SLI may be identified by ISBE from time to time, and, if so, the Company and ISBE intend to make good faith efforts to address such interdependencies. The Company intends to assist ISBE, for example by reviewing any RFP language, providing documentation related to the SLI to support ISBE's discussions with possible vendors, and answering related questions, so that enhancements to the State Ed Infrastructure will continue to be able to leverage the SLI.
- d. Test Data.
- i. For purposes of testing SLI during the SLI Pilot, ISBE intends to provide Test Data, as described in Exhibit B, to the Company. In no event will Test Data include personal identifiers.
 - ii. The Company and ISBE acknowledge that prior to ISBE providing to the Company any "real" or "live" data or information of state education agency and local education agency organizations and employees, schools, teachers, parents, and students, including student personally-identifiable data, for use in the implementation of the SLI, ISBE will authorize Company's access to such data through a data sharing agreement, as contemplated in paragraph B.3.f of this MOU.
- e. Notice. In the event that the Company becomes aware of any failure or change in the intentions described in paragraph B.2.a through B.2.c and B.3.a through

B.3.d and the referenced Exhibits, it will promptly notify ISBE in writing to the address set forth below:

Darren Reisberg, Deputy Superintendent & General Counsel
Illinois State Board of Education
100 W Randolph St, Ste 14-300
Chicago, IL 60601

In the event that ISBE becomes aware of any failure or change in the intentions described in paragraph B.3.a through B.3.d and referenced Exhibits, it will promptly notify the Company in writing to the address set forth below:

Stacey Childress
Chair, SLC Board of Managers
In care of: Bill & Melinda Gates Foundation
PO Box 23350
Seattle, WA 98102
stacey.childress@gatesfoundation.org

- f. SLI Implementation. The Company and ISBE will be better informed about the terms essential to an agreement or agreements governing the implementation of the SLI once the development of the SLI is nearing completion on or before December 31, 2012. As such, the Company and ISBE will in good faith negotiate and, if agreement is reached, enter into separate agreement(s) related to the implementation of the SLI, including specific commitments regarding services, service levels, software licensing, and data sharing. The parties recognize that the Company may also enter into separate service and/or data sharing agreements with local education agencies, related to but not superseding any service and/or data sharing agreements between the Company and ISBE.

4. The Parties' Joint Acknowledgments of Risk and Mitigation. The Company and ISBE each recognizes and acknowledges that the SLI is a long-term project and that the SLI Pilot is an important step toward achieving the Company's and ISBE's shared vision for the SLI.

The Company and ISBE each recognizes and acknowledges there are risks of failure in any technology project, and that the potential risk associated with the SLI is outweighed by the potential educational benefits for students in ISBE's state and the opportunity to extend the functionality and value of ISBE's current and future investments in State Ed Infrastructure.

To contribute to the mitigation of risk, the Company and ISBE each intend to contribute skilled and dedicated staff to the SLI Pilot, retain skilled and experienced vendors or other project personnel, as needed, to support the SLI Pilot, and frankly and openly share with each other information and views regarding the SLI Pilot. The Company intends to make available as shared resources for the pilot states one or more technical contractors to (a) assist with integration, technical readiness, and user preparedness planning; (b) develop shared implementation aides; (c) deliver informational workshops; and (d) provide ad-hoc technology subject matter expertise as needed.

- a. The Company's SLI Team Leads:
- Sharren Bates, Senior Program Officer, Bill & Melinda Gates Foundation, leading the SLI work on data integration;
 - Steven Coller, Senior Program Officer, Bill & Melinda Gates Foundation, leading the work on content and application interoperability;

- Leah Hamilton, Program Officer, Carnegie Corporation of New York leading the work on governance;
- Henry Hipps, Senior Program Officer, Bill & Melinda Gates Foundation, providing overall project management and coordinating the state consortium;
- Alvarez & Marsal, LLC, contributing four staff for project management and state and district implementation support;
- CELT Corp., contributing four staff for state relationship management and coordination.

b. ISBE's Project Team:

- Brandon Williams, Project Administrator, ISBE, leading the Illinois SLI team
- Jim Peterson, Technology Director, Bloomington School District 87, leading the SLI Pilot work in Bloomington
- Loren Baele, Technology Director, McLean County Unit School District 5, leading the SLI Pilot work in McLean County
- Michael McKindles, Longitudinal Data System Project Manager, ISBE
- Bernie Acs, Architect, National Center for Supercomputing Applications at University of Illinois
- Harvey Smith, Director, Illinois Interactive Report Card
- Jonathan Furr, Counsel, Holland & Knight

5. **Purpose of the SLI Pilot: Governance.** During the SLI Pilot, the Company intends to define the long-term governance of the SLI and the long-term business model of the SLC, including a plan to facilitate the transition of ownership of the SLI to a Section 501(c)(3) not-for-profit organization that will maintain the SLI on a sustainable basis. To accomplish this, the Company intends to do the following:

a. *Role of the Governance Advisory Group.* The Company has formed the Governance & Organization Technical Advisory Group (G&O TAG) to develop recommendations to the Company's governing board, known as the Board of Managers, regarding long-term governance, organization function and structure, and long-term business plan.

i. *G&O TAG Representatives.* The G&O TAG consists of a representative providing a state perspective (currently the Executive Director of the Council of Chief State School Officers), a representative providing teacher union perspective, and representatives from Carnegie Corporation of New York and the Bill & Melinda Gates Foundation, the two foundations which have provided all funding to date for the formation of the SLI and the SLI Pilot. In addition, the Company recruited for the G&O TAG five senior-level professionals ("External Advisors") who bring expertise and perspective regarding governance, education technology, development of new markets, government and policy, privacy, innovation, business, open source, and other professional domains that impact on SLC development.

ii. *Outreach to the Pilot States.* The G&O TAG, through individual interviews, group webinars, conference calls, and in-person meetings,

will solicit input from the pilot states, including ISBE, through the Chief State School Officer and his or her designee(s) on issues relevant to the design of the long-term governance framework, organizational model and business plan. Briefing topics are intended to include, but will not be limited to, privacy and security, data ownership and access, software and content issues, cost structures and revenue models.

iii. *Recommendations.* The G&O TAG will meet several times collectively and individual members will provide guidance on an ongoing basis in their areas of expertise to provide expert input and ensure key issues are being addressed as questions on governance, organization, and the business model are being answered. The G&O TAG will rely on the input from the pilot states and its representatives, including its External Advisors, to inform the recommendations that are made by the G&O TAG to the Board of Managers.

b. *Engagement of McKinsey & Co.* The Company has engaged McKinsey & Co. to provide strategic and analytic support on governance. The Company intends that the McKinsey team will facilitate and participate in pilot state briefings, as well as all strategy sessions with the G&O TAG.

c. *Timeline and Deliverables.* As planned, the G&O TAG presented recommendations regarding the mission, vision, a set of organizational goals and metrics, and privacy and security policies to the Company's Board of Managers by December 2011. The Company intends that recommendations defining a final set of organizational goals and metrics, the long-term governance structure, organizational development plan and business plan will be delivered to the Board of Managers by March 2012. For any governance topics reviewed with the pilot states, the Company will communicate its decisions to the pilot state chiefs and designees.

6. **Term.** This MOU will be effective on the date of last signature and will expire on December 31, 2012 or upon the execution by the Company and ISBE of a service level agreement governing implementation of the SLI, whichever is earlier.

7. **Confidentiality and Publicity.**

a. The Company and ISBE recognize that this MOU involves development of software and specifications that are proprietary unless or until released under an open source license in accordance with this MOU or any subsequent agreements. The Company and ISBE further recognize that this project will require them to have a free and frank exchange of opinions, advice and criticism to assist the Company in making design and development decisions and to assist ISBE in evaluating and making internal decisions about its State Ed Infrastructure.


b. The Company agrees it will notify ISBE prior to referencing ISBE in any press releases, media statements or interviews, presentations at conferences and seminars about this MOU, the SLI Pilot, or the Technology Build.

- c. ISBE agrees it will use all reasonable efforts to notify the Company prior to referencing the Company, this MOU, the SLI Pilot, or the Technology Build in any press releases, media statements, press or media interviews, or presentations. ISBE agrees to use all reasonable efforts to provide the Company with an advance copy of any press releases, media statements, presentations, or other written material intended for public release in order to allow the Company to review and provide comment. Except as, and to the extent, required by law, ISBE agrees to not disclose, and will maintain the confidentiality of, certain specifications and/or software specifically related to protecting data privacy and security that may be disclosed to ISBE under this MOU and that the Company marks or otherwise indicates in writing is to be treated as confidential, restricted, or proprietary.

8. MOU Purpose. The purpose of this MOU is to provide a non-binding expression of intent between the Company and ISBE; **except for the confidentiality obligations set forth in Section B.7, which the Company and ISBE agree shall be legally binding.**

9. Counterparts. This MOU may be executed in one or more counterparts, each of which will be considered an original for all purposes, all of which taken together will constitute one single MOU between the Company and ISBE, notwithstanding that both are not signatories to the original or to the same counterpart.

SHARED LEARNING COLLABORATIVE, LLC

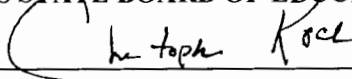
By: 

Name: Stacey Childress

Title: Member and Chair, Board of Managers

Date: April 19, 2012

ILLINOIS STATE BOARD OF EDUCATION

By: 

Name: Dr. Christopher A. Koch

Title: State Superintendent

Date: 4/13/12

EXHIBIT A APPROACH TO TECHNOLOGY BUILD

This Exhibit A to the MOU provides additional details, of particular interest to the Company's SLI Team and ISBE's Project Team, regarding how each will undertake the development of the SLI and the Technology Build, the scope of which is further detailed in Exhibit B to the MOU.

1.0 Schedule. The Company intends that the Technology Build will be designed, developed, and released according to the following schedule:

- Data Infrastructure Design/Build Start Date: June, 2011
- Draft API Documentation: December 2011
- Final API Documentation April 2012
- Developer Sandbox: June 2012
- Data Infrastructure Alpha Release: June 2012
- SLI and Generic Views ("Release 1.0"): December 2012

2.0 Feature Design, Prioritization, Project Timelines, and Technical and Functional Design Documents. Consistent with paragraph B.3.a of the MOU, the Company intends to share with ISBE feature design, and prioritization decisions, project timelines, and draft/final technical and functional design documents for the Technology Build and solicit ISBE's input. The Company intends such feature design, and prioritization decisions, project timelines, and draft/final technical and functional design documents will include, but not be limited to, the following:

- APIs and data model
- Data import/export formats
- Identity management and single sign-on (SSO) functionality
- Educator dashboard application
- Administration tools
- Developer sandboxes

3.0 Intellectual Property. Except as otherwise provided in paragraph B.2.b of the MOU, the Company intends that software components of the SLI developed by or on behalf of the Company will be available under an open source license. The Company intends any such license to apply to the following:

- Data stores and API service layers
- Identity Management and SSO services
- Automated bulk data loading tools
- Interactive bulk data loading tools
- Standard dashboard application and source code
- Administration tools
- Developer sandboxes
- Educator and school-building-level staff applications
- Results of all educator focus groups

4.0 ISBE's Participation in the SLI Pilot. Consistent with paragraph B.3.a of the MOU, ISBE acknowledges it will need to meet certain requirements to participate in the SLI Pilot, including but not limited to:

- a. *SLI Pilot and State Ed Infrastructure.* ISBE intends to develop, enhance and/or maintain its State Ed Infrastructure to enable data and content interoperability with the SLI, with a goal of providing students and educators access to educational content and applications that support personalized learning.

ISBE has identified the following as its technical point of contact for the SLI pilot: Brandon Williams, bwilliam@isbe.net.

- b. *SLI Pilot and Local Education Agencies.* ISBE intends to identify Local Education Agencies (“LEAs”) within ISBE’s state that will participate in the SLI Pilot with ISBE (“Participating LEAs”). ISBE intends to work with Participating LEAs as needed to encourage their full participation in the SLI Pilot and identify and share with the Company a technical point of contact for each Participating LEA.
- c. *Data Scope.* The current scope of the Technology Build includes the ability for states to load a student’s pre-K through grade 12 data. ISBE intends to work with their Participating LEAs and the Company to determine the full historical data scope and timeline, as contemplated by the Technology Build Scope, Exhibit B.
- d. *Data Domains.* ISBE intends to work with their Participating LEAs and the Company to assist it in finalizing the data sets and domain types, set forth in Exhibit B.
- e. *Data Ingestion.* ISBE, and/or its Participating LEAs, will be responsible for sourcing, governing, loading and validating any data made available to the SLI, including the ability to:
 - i. Source and provide ingestion data for these key domain spaces: Education Organization, Teaching and Learning, Staff, Enrollment;
 - ii. Create Ed-Fi XML files according to the published specifications at ed-fi.org;
 - iii. Create Comma-Separated-Value formatted files, per written specifications provided by the Company;
 - iv. Work with the Company to influence additional student information system and assessment vendors to build SLI-compatible adaptors;
 - v. Integrate with local SIF (Schools Interoperability Framework) implementation;
 - vi. Resolve data errors or warnings during automated imports.
- f. *Data Identification.* ISBE intends to establish or has established and will utilize unique and permanent (i.e., do not change from one academic year to the next) identifiers for all students, faculty and staff who will have access to the SLI whether they are associated with ISBE, Participating LEAs, or schools within those LEAs. ISBE intends to establish, or has established, and utilize a unique, stable identifier to tag each teaching, learning and assessment object that ISBE or its Participating LEAs intend to make accessible via the SLI.
- g. *Third Party Application Data Access.* In order for third-party educational application and content providers to leverage SLI identity, which allows user login through the SLI and authentication permitting a user to see appropriate

student-level data, participating state and local education agencies must approve such providers' access to relevant data provided by state and local education agencies via the SLI. As such, ISBE intends to develop a process for such approval, and will inform Participating LEAs about the need to develop a similar process for approval.

- h. *Intellectual Property and Open Source.* ISBE recognizes that any enhancements made by or on behalf of ISBE to open source licensed SLI code will be made available consistent with the terms of such license. The Company and ISBE agree that software and applications developed by or on behalf of ISBE that are interoperable with, but separate from, the SLI will not be subject to the SLI open source license terms.
- i. *Browser Access.* It is ISBE's intent that it will require its SLI Pilot users to have access to a browser compatible with the SLI (see Exhibit B, section 8.0)

5.0 Data Sharing. For purposes of testing SLI during development, ISBE intends to provide to the Company sample data of the type, quantity and format the Company defines as required to test SLI. ("Test Data") In no event will Test Data include personal identifiers.

* * *

EXHIBIT B **Scope of Technology Build**

This Exhibit B to the MOU provides additional details, of particular interest to the Company SLI Team and ISBE’s Project team, regarding the Scope of the Technology Build.

1.0 Overall Scope of the Technology Build. The Company intends that the Technology Build will provide a secure, multi-tenant, cloud-hosted data store designed to help states and districts manage their student enrollment and achievement information currently housed in multiple source systems.

2.0 The Data Store and Data Model. The Company intends the following with respect to the data store and data model and is working with its vendors to incorporate these features and functions into the SLI consistent with the terms of the vendor agreements:

- a. The data store will be available to states and districts to maintain data about organizations, schools, employees of SEAs and LEAs and student enrollment, biographical and achievement data.
- b. The complete SLI Core Entity Model, which describes the data that may be housed in the SLI data store by SEAs and LEAs, is modeled after the Ed-Fi initiative, which provides alignment with many other common educational data initiatives, such as CEDS. For more information, visit <http://www.ed-fi.org/>.
- c. The current scope of the SLI includes the ability for states to load a student’s pre-K through grade 12 data.

3.0 Data Domains. The Company intends the following with respect to data domains and is working with its vendors to incorporate these features and functions into the SLI consistent with the terms of the vendor agreements:

- a. The SLI Model defines a total of 250 types or entities. The domain types contain over 400 granular data elements and the flexibility to add more as needs evolve. However, these are captured in 39 high-level “Domain Types:”

AcademicWeek	DisciplineIncident	Program
Assessment	EducationOrganization	ReportCard
AssessmentItem	EducationServiceCenter	School
AssessmentRatingStandard	Grade	Section
AttendanceEvent	GradingPeriod	Session
BellSchedule	LearningObjective	Staff
CalendarDate	LeaveEvent	Student
ClassPeriod	LocalEducationAgency	StudentAcademicRecord
Cohort	Location	StudentAssessment
Course	ObjectiveAssessment	StudentAssessmentItem
CourseTranscript	OpenStaffPosition	StudentExpectation
Diploma	Parent	StudentObjectiveAssesment
DisciplineAction	PostSecondaryEvent	Teacher

- b. These entities, in relation to each other, provide the building blocks for 14 logical data spaces that are generally well-recognized in the K-12 education data space. They are:

Alternative/Supplemental Services	School Calendar
Assessment	Staff

Bell Schedule	Student Academic Record
Student Discipline	Student Attendance
Education Organization	Student Cohort
Enrollment	Student Identification and Demographics
Graduation	Teaching and Learning

- c. The expected datasets that will be stored in SLI will continue to develop over time with feedback from our Pilot States.
- d. In addition to storing core entities and attributes like the ones above, the data store will also include the ability to store custom data that may be unique to a particular SEA/LEA or application. This custom data will be accessible through the API layer.

3.0 Data Ingestion Methods. The Company intends the following with respect to data ingestion and is working with its vendors to incorporate these features and functions into the SLI:

- a. The SLI will be configured so that a variety of SEA and LEA source systems can create and manage the data that can be maintained in the SLI.
- b. Because student attendance, transcript, class schedule and assessment data are typically stored in many different systems within the LEA and SEA, the SLI will offer a data store to integrate that data and an API layer to make it available to other applications.
- c. The SLI will be built with the assumption that LEAs and SEAs will be responsible for sourcing, governing, loading and validating their data. The SLI will offer robust bulk data ingestion and validation tools to enable successful data integration.

SLI Data Ingestion Options to be included by v.1

- XML Format (Ed-Fi Data Interchange Schemas)
- CSV format
- SIF Agent
- Built-in adapters for select SIS/Assessment vendors

Submission Channels

- File drops / Web Services
- Web based interactive tools

Robustness

- Data Integrity Checks
- Robust and Structured Error Reporting

Security

- Certificates used to provide authentication and authorization for ingestion
- Encrypted transport via SSL

4.0 Identity Integration. The Company intends the following with respect to identity integration and is working with its vendors to incorporate these features and functions into the SLI consistent with the terms of the vendor agreements:

- a. In addition to integrating the datasets that represent the key enrollment and achievement data used by SLI applications, the SLI will allow user identities that exist in SEA and/or LEA IT systems to be integrated for authentication and authorization of users and to enable such users to access personally-identifiable information (PII) in a manner designed to permit states, districts, and schools to operate in compliance with FERPA.
- b. The SLI will provide multiple mechanisms for connecting to existing Identity Directories
 - Federation via SAML 2.0
 - Delegation via Web Services (Salesforce model)

The SLI may provide additional directory integration methods, such as OAuth and/or OpenID based on the information gathered by the SLC from the site landscape analysis planned for October and November with pilot states.

- c. The SLI will host identity information for SLI/SEA/LEA Administrators and Operators.
- d. The SLI will permit other education technology applications to leverage SLI identity and student-level data, but only those applications that are approved by relevant LEA and SEA Administrators.
- e. The SLI will manage user authentication and authorization as follows:
 - Users are authenticated by an SEA or LEA directory
 - Access to data is controlled by Role and Context
 - User roles are determined by the SEA or LEA directory
 - Context is determined by enrollment data in SLI (e.g. for which students does a Teacher or Principal have authority to view PII)
 - SEA/LEA roles are mapped to SLI Roles
 - Standard SLI Roles with default permissions
 - Custom Roles created by SEA or LEA

5.0 API Scope. The Company intends the following with respect to API's and is working with its vendors to incorporate these features and functions into the SLI consistent with the terms of the vendor agreements:

- A uniform interface for application to easily access data
- RESTful Web Service accessible over HTTPS
- Synchronous near-real-time read-write access
 - For each Data Entity at a unique URL
 - For List/View access to common groups of entities
 - E.g. "List students for teacher X in grade K."
 - For common Aggregate metrics
 - E.g. "Percentage of students at achievement level X on assessment Y in grade K."
- Asynchronous/batched access for bulk extracts

6.0 SDK Scope. The Company intends the following with respect to the Software Developer Kit (SDK) and is working with its vendors, within the terms of the vendor agreements, to develop an SDK that includes: a) Robust and clear developer documentation, including simple “Getting Started” and “How-to” guides and full API specifications; b) Automatically provisioned sandbox accounts with access to realistic test data and an ability to reset sandbox to “factory defaults” and c) Simple sample application code in multiple languages to demonstrate full breadth of API usage, such as Java, Python, .NET

7.0 SLI Core Applications. The Company intends that most applications accessible via the SLI will be provided by SEAs, LEAs or third-party educational technology providers.

- a. The Company intends that the SLI will include three applications that support successful classroom implementation of the Common Core State Standards, and is working with its vendors, consistent with the terms of the vendor agreements, to include in the SLI:
 - i. Educator Dashboards with the following features:
 - “Out-of-the-box” access to student data housed in SLI
 - Configurable, accessible and intelligible presentation of data
 - Individual and aggregated views of data for users at all organizational levels
 - Open Source implementation for SEA/LEA enhancement
 - Email functionality for educators to report inaccurate data to LEA administrator

Types of dashboards and the types of student data visible on them will be prioritized based on feedback from states gathered during the SLI Pilot.
 - ii. An Educator Portal with that includes login and landing pages, access to SLI-aligned applications and can be customized by SEA/LEAs.
 - iii. Admin and Developer Portals that include account provisioning and configuration, diagnostic information for developers and integrators, sandbox functionality with modeled fake student data for testing purposes, and administrative validation and error reporting tools for LEAs and SEAs.
- b. Consistent with paragraph B.3.b.iii of the MOU, the Company is considering incorporating into the SLI up to three (3) educator-facing content or student assessment applications that enable successful implementation of the Common Core Standards and that are of interest to the states participating in the SLI Pilot.

8.0 Browser Compatibility. The Company intends that SLI will support Internet Explorer version 8 and version 9, and Safari version 4 and 5. The Company will endeavor to add Firefox version 6 and 7.

EXHIBIT C
Data Privacy and Security Requirements

The following Data Privacy and Security Plan was agreed to between the Company and Wireless Generation, Inc. (“WGen”) as a part of the WGen Agreement, a work-for-hire contract to design and develop the SLI software necessary to facilitate data integration and application interoperability, referenced in paragraph B.3.b of the MOU.

Shared Learning Infrastructure
Exhibit C – Data Privacy and Security Plan

Table of Contents

Table of Contents	i
Table of Figures	ii
1. Introduction	1
2. Definitions	1
3. Privacy in SLI	2
3.1 Permissions to Data Within an Institution	3
3.2 Delegation of Administrative Privileges	4
3.3 Authentication and Authorization	5
3.4 Initial Authentication and Manual Dispute Resolution	6
3.5 Access to Third Parties	7
3.6 Application Approval and Deployment	7
3.7 API Security	8
3.8 District Opt-Out from SLI	9
4. Data Security in SLI	9
4.1 Security Personnel	10
4.2 Internal Information Security Policy	11
4.3 Internal Controls and Audits on Employee Access	11
4.3.1 Credential Management for System Access	11
4.3.2 Security of Wireless Generation Employee Credentials	12
4.4 Security in the Development Process	12
4.4.1 Baseline Application Security Requirements and Guidelines	12
4.4.2 Code Review Process	13
4.5 Development Environments and De-Identified Data	13
4.6 Security Functionality of Applications	13
4.6.1 Permissions and Data Access	13
4.6.2 Baseline Requirements for Application Credentials	13
4.7 Configuration and Deployment Security	14
4.7.1 Network and Infrastructure Security	14
4.7.2 Patching and Vulnerability Management	14
4.7.3 Logging and Auditing	14
Appendix A.	15

Table of Figures

Figure 1 - State/District/School/Class Hierarchy	2
Figure 2 – Example of User Permissions and Context.....	3
Figure 3 – Example of Default Roles, Custom Roles, and Assigning Permissions	4
Figure 4 - Examples of Base Permission Assignment	5
Figure 5 – Example of Mapping an External Directory.....	6
Figure 6 - Two Ways for Data to be Read or Written	8
Figure 7 - Information Security Approach	10

1. Introduction

This Data Privacy and Security Plan (the “*Plan*”) describes the concepts of user identity and system access that will serve as the foundational principles for the design, implementation and operation of the Shared Learning Infrastructure (“*SLI*”). In addition, the Plan describes the technical and procedural information security mechanisms being put in place by Wireless Generation during the development and initial deployment of SLI to reduce the risk of data breaches and compromises.

The Plan is intended for the use of the Shared Learning Collaborative, LLC (“*SLC*”), and supersedes Exhibit F to Work Order #1 under the Master Services Agreement between Wireless Generation and SLC. [Appendix A](#) hereto outlines how each item in Exhibit F is being addressed.

2. Definitions

Aggregate Data – Aggregate data is created by combining the data of multiple individuals such that no individual-level record information is displayed.

Authentication - Authentication is the process of verifying the unique identity of a user.

Authorization - Authorization is the process of assigning a specified level of system access and control to a user. Authorization will generally be determined based on pre-defined Roles.

Bulk Data API – Bulk Data API is an API that asynchronously processes large numbers of records. The data must be in file format.

Directory - A Directory is a service that manages user identities and user Roles.

Group – A Group is a collection of Institutions or individual students within SLI.

Institution – An Institution is a school, a school district, or a state.

Permissions - Permissions are a set of actions a user is allowed to take in SLI (e.g., “Can see student assessment data for students the user teaches” or “Can change administrative setting for an account”).

Record-Level API – Record-Level API is an API that synchronously provides access to individual records or small collections of records.

Roles - A Role is a pre-defined relationship between a user and an Institution in SLI (e.g., teacher or principal) that corresponds to a specific set of Permissions.

SLC – Shared Learning Collaborative, LLC

SLI – Shared Learning Infrastructure

Super-Administrator – Super-Administrator is the Role description for a user assigned a set of Permissions within an Institution that grant the user complete administrative control over all data within SLI associated with that Institution.

3. Privacy in SLI

The basic hierarchy of SLI is State-District-School-Class:

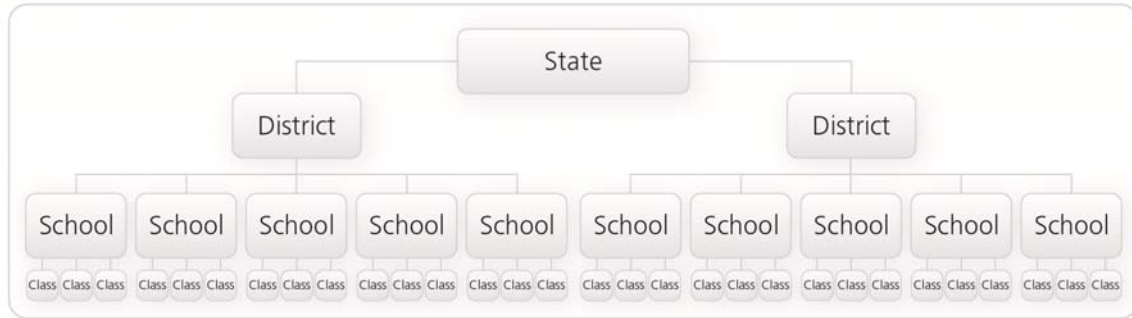


Figure 1 - State/District/School/Class Hierarchy

It is assumed that all schools within SLI belong to one District, and all Districts belong to one State.

SLI recognizes the District as the ultimate arbiter of who is able to view the District's student data and SLI is built to facilitate District control over data. However, SLC recognizes that Districts may have contractual or regulatory arrangements enabling States to administer data on their behalf. For this reason there are currently two available paths for initial system registration in SLI – State-level registration, and District-level registration. Individual school registration for SLI is not currently supported.

State-Level Registration: States may enter into an agreement with SLC to adopt SLI and register all Districts within the State. If the State is the adopting institution, then the State will have the authority and responsibility to define all Districts within the State. State-level registration in SLI requires the designation of a Super-Administrator at each District (see Figure 4 for a visual representation of the Super-Administrator Role and associated Permissions within SLI).

In the event that a State has acquired the right to manage District data, it may upload a District's data into SLI. For existing Districts in the system, a Super-Administrator of that District will need to first grant this permission to the State or another third party.

District-Level Registration: After the pilot period, an individual District may enter into an agreement with SLC if its State has not done so. The agreement between the District and SLC must designate the identity of the District's first Super-Administrator.

A District may create additional Super-Administrators or re-assign the Super-Administrator role; however, each District must have at least one Super-Administrator at all times.

The high-level description of Roles, Permissions, authentication practices, and of the API in the remainder of this Section 3 is subject to more specific parameters and values that will be detailed during the course of development of SLI. All examples in this Section 3 are illustrative only.

3.1 Permissions to Data Within an Institution

All data within an Institution is viewable in accordance with the Roles and Permissions within SLI. SLI determines user Permissions according to the Institutions associated with the user. For example, a principal at a given school will be able to view all student data for students in her school, but will not have Permissions to view the student data of students in other schools in the District. To determine some SLI permissions, other information from the data model is needed including institutional hierarchy and course/section enrollment. For instance, Permissions associated with the teacher Role will depend on the classes taught by the teacher and the students enrolled in those classes.

Default Permissions and Custom Roles –

Each SLI Role will determine what Permission the users who are assigned that Role will have. Permissions will determine what operations a user is allowed to perform and, in the context of the Institution with which they are associated, what data they are allowed to access, as per Figure 2 below.

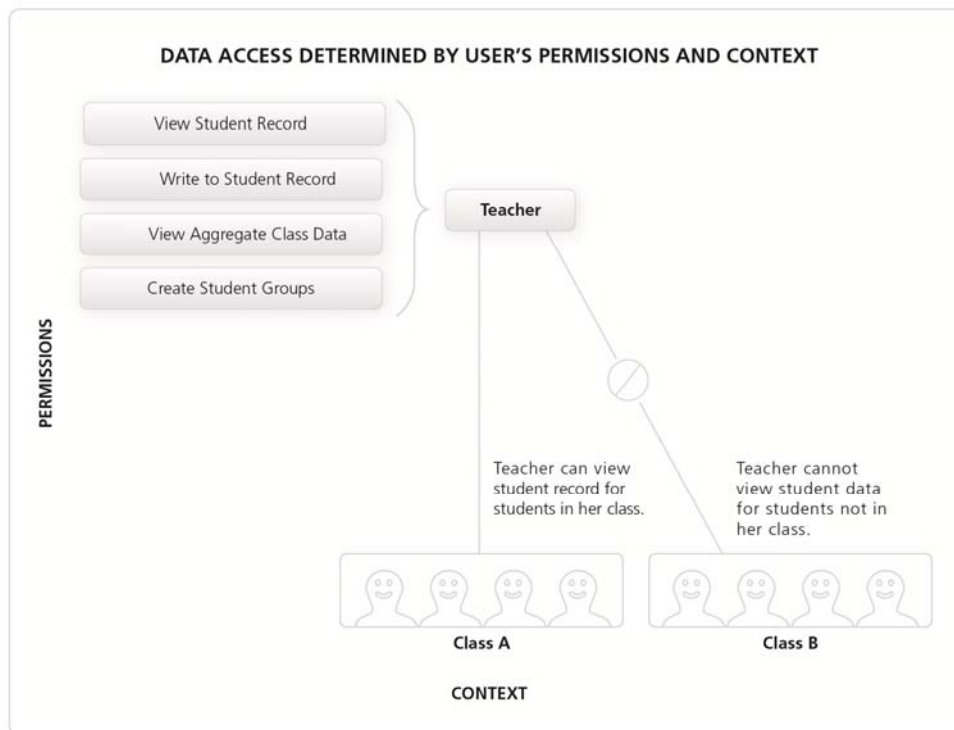


Figure 2 – Example of User Permissions and Context

SLI will define certain pre-defined default Permissions and Roles. For instance, a user with the Role of “teacher” might be able to see all student data for students that they teach, and create assessment results for students that they teach. A “principal” might be able to see PII for all students in her school but have no permission to create assessment results. The precise definition of the default Permissions and Roles will be specified as part of the development of SLI.

While the pre-defined Roles cannot be changed, Super-Administrators or other users with the appropriate Permissions will be able to create custom Roles via the administrative interface. These custom Roles are defined by associating the Role with any combination of the existing SLI Permissions, as shown in Figure 3. Super-Administrators or users with the appropriate Permissions can define a custom Role that has a new grouping of Permissions, but cannot create new Permissions.

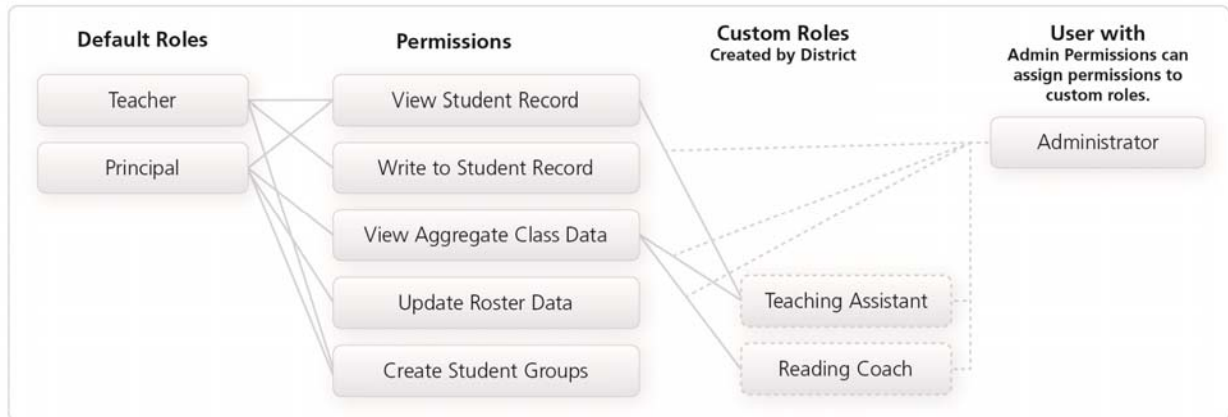


Figure 3 – Example of Default Roles, Custom Roles, and Assigning Permissions

SLI will support the ability to give access to aggregate data only. An aggregate view will allow the user to view data created by combining the data of multiple individuals but not to view individual-level record information or data aggregated from a sufficiently small data set. Administrators with the appropriate Permission will be able to configure the corresponding small data set threshold. Users viewing aggregate data will not be able to view data aggregated from a number of records below this threshold.

3.2 Delegation of Administrative Privileges

The Super-Administrator Role represents a collection of administrative privileges as represented in Figure 4. Any Super-Administrator can delegate this Role to other users. A Super-Administrator can also delegate a subset of the administrative privileges to other users by performing the appropriate Directory mapping as described in Section 3.3.

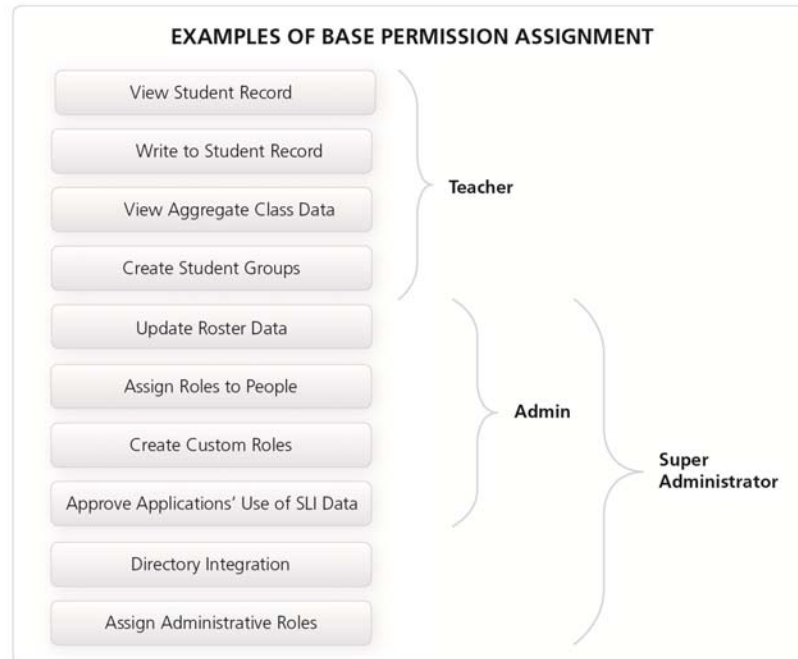


Figure 4 - Examples of Base Permission Assignment

3.3 Authentication and Authorization

Username, credentials, and Roles can be stored in either:

- A District-designated Directory
- An SLI-hosted Directory.

Access to SLI functionality is determined by the user's Role in the Directory and the user's relationship with the data model, such as a teacher whose access to data is restricted by the classes they teach. Each user must be associated with one or more Roles. In addition, each user will need to be attached to at least one Institution within SLI in order to have Permissions within SLI.

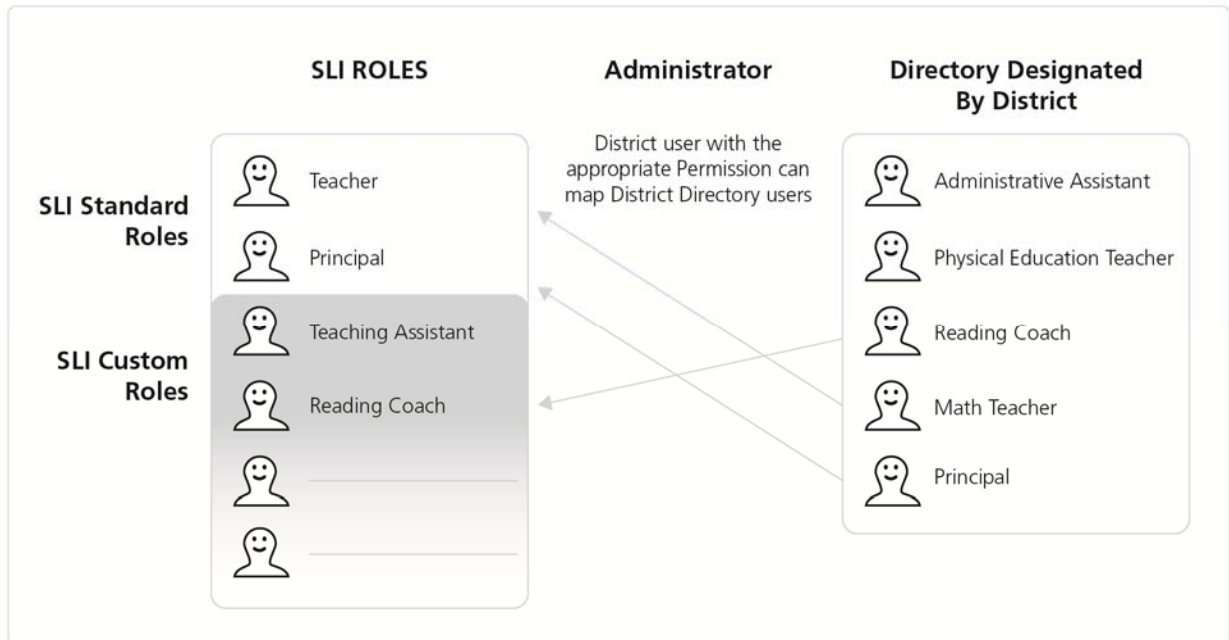


Figure 5 – Example of Mapping an External Directory

Integration with an External Directory: In order for an Institution to integrate with SLI, they need to have a Directory (or set of Directories) that stores all of the users that will access SLI. This Directory will need to be integrated with SLI. When users log into the SLI portal or an SLI application, their identity will be authenticated by a District or State's Directory, not by the SLI system itself. The District or State's Directory will verify that the username and password credentials supplied are valid and return this information to SLI.

After a user is authenticated, the SLI API will provide a time-limited authenticated user token for the authenticated user. All subsequent calls to the SLI API for this user's session will need to include this authenticated user token. The API will use this token to determine who the user is and which actions he or she is allowed to perform.

Each District or State will need to map the roles in their Directory to SLI Roles (which can be done by an administrator with appropriate Permissions) as shown in Figure 5. At each successful user login, SLI will get role information from the local Directory and map those roles to SLI Roles to determine the logged-in user's Permissions.

3.4 Initial Authentication and Manual Dispute Resolution

Once an initial District Super-Administrator is registered, all subsequent administrative decisions will be made by the Super-Administrator or individuals who have been delegated the appropriate Permissions. Disputes by third parties regarding whether a Super-Administrator is indeed authorized to represent a District will be addressed through a process at the District or between the District and the SLC.

3.5 Access to Third Parties

Districts are responsible for determining the eligibility of third parties to access SLI data and documenting appropriate agreements.

3.6 Application Approval and Deployment

SLI data will be accessible through either the Record-Level API or the Bulk Import/Export API as shown in Figure 6. The Record-Level API will enable applications to leverage the existing users, roles, and permissions within SLI. External applications will be able to import and export data through the Bulk Import/Export API under terms of use to be determined by SLC.

Districts will be required to approve any application that accesses data controlled by that District. Administrators with the appropriate Permission will be able to grant District approval through the SLI administrative portal. District administrators will be responsible for licensing and service level requirements as well as security/privacy compliance of approved applications.

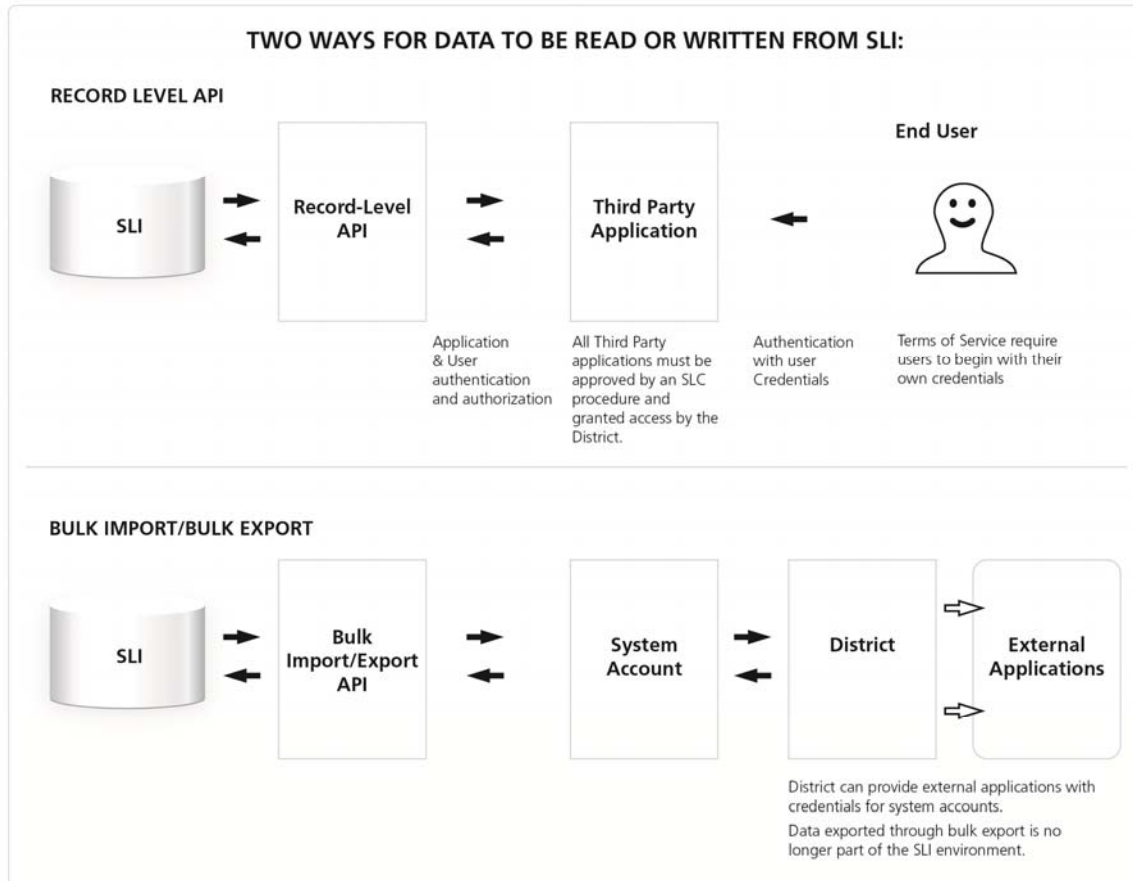


Figure 6 - Two Ways for Data to be Read or Written

3.7 API Security

In addition to the user authentication and authorization, SLI will only accept API calls from approved applications. These are applications that have been approved by the relevant State or District. Before returning any data, the API will authenticate that the Application ID and signature match the approved applications. The technical means for authenticating the Application ID and signature are currently under development.

Each API call that returns student PII will be made on behalf of an authenticated user and must contain:

- Application ID
- Evidence that the authenticated user provided credentials
- API parameters
- Signature

Before returning any data, the API will:

- Validate the application ID
- Check that the user is authenticated
- Check that the appropriate District has approved the application
- Get the Roles for the user
- Check that the user has the appropriate Permissions to execute the API call
- Return the appropriate data for the user's Role, context, and API parameters

3.8 District Opt-Out from SLI

If a school district decides they no longer wish to use the SLI system, they may request that district student data be deleted from the SLI data store. SLI will have a mechanism to delete these records from the data store.

4. Data Security in SLI

The privacy provisions described in the Section “Privacy in SLI” are enforced through industry-standard information security mechanisms. This Section 4 describes some of the key technical, procedural, and organizational information security measures deployed at Wireless Generation for the development of SLI and the operation of the alpha version of SLI. An overview of the components of this approach is shown in Figure 7 below:



Figure 7 - Information Security Approach

4.1 Security Personnel

Wireless Generation has a dedicated Chief Information Security Officer with full responsibility for all information security issues. The Chief Information Security Officer is a member of the Wireless Generation Executive Committee.

All employees are responsible for adhering to the company's Information Security Policy. In addition, specific information security responsibilities within the organization are assigned within IT Operations and other product development teams.

Wireless Generation also makes extensive use of external resources for manual code review and penetration testing. Developers building the SLI will undergo security training in how to code defensively and avoid common vulnerabilities.

4.2 Internal Information Security Policy

Wireless Generation has an Information Security Policy that governs the use of all company data. All Wireless Generation staff are trained in the Information Security Policy and required to adhere to it.

The Information Security Policy contains the following components:

- Categorizes different levels of sensitive information
- Defines corporate roles and responsibilities
- Defines rules for accessing and handling different kinds of data
- Defines appropriate use of computing systems

Principles of the Information Security Policy include:

- Only authorized individuals should have access to sensitive student data.
- All access to sensitive student data is on a business need-to-know basis.
- Controls are in place to register and audit access to sensitive student data.
- Resources are allocated efficiently to protect data in accordance with its sensitivity.

Exceptions to the Information Security Policy require approval by the Chief Information Security Officer.

4.3 Internal Controls and Audits on Employee Access

Wireless Generation implements internal access controls to ensure that employees only have access to the data that they are authorized to view. For production systems that house sensitive student data, the following principles guide access:

- All access must tie back to a named employee account. Any required shared accounts (such as root passwords for servers) are only reachable by first logging into a named account.
- System access is logged and periodically audited.
- New access is granted only on the basis of a logged request that goes through the proper authorization channels.
- Access is lost immediately upon termination or cessation of employment.

4.3.1 Credential Management for System Access

Wireless Generation uses a credential management system to securely store sensitive credentials that allow access to student PII. The use of the credential management system facilitates the use of complex passwords and provides a complete audit trail indicating who accessed what password at what time.

All production passwords or passwords that give access to student PII are stored in the system. This includes:

- Root and system accounts on Unix servers
- Router and other networking passwords
- Database system-passwords
- Firewall passwords

The following are the key operating procedures of the credential management system:

- Credentials are stored in “safes” based on need-to-know provisions.
- Each safe has an administrative owner responsible for adding and removing users on a business need-to-know basis.
- All non-individual credentials with access to sensitive data are stored in the system.
- Passwords may never be stored outside of the credential management system in flat files or other insecure methods.
- The credential management system is only accessible via the internal network to authorized users.
- No vendor-supplied default passwords are used.

4.3.2 Security of Wireless Generation Employee Credentials

Wireless Generation implements the following measures to protect employee credentials:

- Internal Active Directory credentials are subject to mandatory periodic password change.
- Internal Active Directory credentials are subject to password complexity requirements.
- Account lockout occurs after a series of failed login attempts.
- Accounts are deactivated immediately upon termination or cessation of employment.

4.4 Security in the Development Process

Wireless Generation integrates security into each step of the application design and deployment process. In particular, the following elements are at the core of Wireless Generation’s secure development process:

- Security decisions are made early in the design process.
- Security is a key factor in design decisions.
- Code is periodically reviewed to discover vulnerabilities.
- Third parties with specific application-security expertise review code to identify vulnerabilities.
- Exceptions to standard security requirements require the approval of the Chief Information Security Officer.

4.4.1 Baseline Application Security Requirements and Guidelines

Wireless Generation implements a Security Checklist Process of baseline security requirements which form the base guidelines to which applications are built.

Key baseline security requirements and guidelines in the Security Checklist process include:

- A general review of the code against typical security vulnerabilities as documented in industry best practices, such as the Open Web Application Security Project (OWASP) Top 10 list.
- All external input is validated to mitigate the risk of SQL injection attacks.
- All sensitive data is sent over SSL when travelling over external networks.
- Minimization of risks associated with Cross-Site Scripting.
- Minimization of data leakage in client-side scripts.
- Server-side checks for authorization to access sensitive data.
- Authentication of all web pages with sensitive data.

Any exceptions to the Security Checklist are documented and require the approval of the Chief Information Security Officer.

In addition, Wireless Generation uses external security experts to provide guidelines for security best practices specific to the languages and platforms that are in common use in the organization.

4.4.2 Code Review Process

The objective of code reviews is to find security vulnerabilities, validate the proper use of security mechanisms, and evaluate the use of best practices in the application. This involves a combination of manual penetration testing, automated code analysis, and manual code analysis to discover flaws.

Wireless Generation reviews code both prior to release and periodically afterwards. Wireless Generation uses a risk-management approach to rate the severity of vulnerabilities found in code. Vulnerabilities are assigned a likelihood and impact score relative to their technical and business context. Discovered issues are ranked by severity and tracked for resolution.

4.5 Development Environments and De-Identified Data

Wireless Generation provisions development environments that are strictly separated from corresponding production environments. This separation occurs at the network level using standard firewall technology. In addition, credentials for key systems differ between development and production.

4.6 Security Functionality of Applications

Wireless Generation implements standard security functionality around user authentication and permissions to enforce the business logic and permission model of the underlying applications.

4.6.1 Permissions and Data Access

All Wireless Generation applications restrict PII access to authenticated users with valid login credentials. Depending on the particular product, end-user accounts may be provisioned and managed by the application itself, the customer, or a third party.

4.6.2 Baseline Requirements for Application Credentials

All application end-user credentials meet the following security requirements:

- Password complexity requirements are enforced.
- Applications lock following a set number of failed login attempts.
- Credentials are stored in secure and protected areas only.
- All credentials are passed in encrypted channels when travelling over public networks using standard technologies such as SSL.

4.7 Configuration and Deployment Security

Wireless Generation takes the following industry-standard steps to ensure the security of its corporate servers:

- Credentials on all servers comply with password complexity requirements.
- Only authorized individuals have the ability to log onto servers.
- Logs recording system access are maintained.
- Server configurations are periodically reviewed for security.
- Server logs are maintained and periodically reviewed.
- Technical contacts receive vulnerability alerts for all core installed systems.

4.7.1 Network and Infrastructure Security

Wireless Generation restricts network access on servers that contain sensitive data or are public facing. In particular, web-facing servers allow only limited traffic (ports 80 and 443). Firewall rules restrict access from the internal corporate network to application servers.

All substantial changes to firewall configurations go through a change management process that involves the approval of the Head of IT Operations and the Chief Information Security Officer.

4.7.2 Patching and Vulnerability Management

Servers containing sensitive student data are managed through central configuration management tools. This allows the standardization of server configurations and for efficient review of security postures. Wireless Generation periodically reviews the security configurations of all managed servers that contain sensitive student data.

4.7.3 Logging and Auditing

Activities on Wireless Generation systems are logged and audited. A centralized logging solution records significant system activity together with the user name and other relevant information of the system administrator.

SLI application logs will also be maintained and periodically reviewed in accordance with the operating procedures that will be developed for SLI. Significant security events will be written to logs stored in a secure location.

Appendix A.

Exhibit F Requirements	SLI Solution
<p>A. Restrictions and authentication processes limiting access to Student PII only to:</p> <p>a. the School District that provided the data and to other recipients authorized by the School District; and</p> <p>b. employees of the host of SLI and to other recipients based on pre-defined roles.</p>	<p>a. Role-based solution that will use user identity data and enrollment data to provide access only to users authorized by the District.</p> <p>b. Documented processes for restricting and recording any necessary access by Wireless Generation.</p>
<p>B. Recording requests for access to and disclosures of Student PII to third party users not identified in SLI as authorized School District users, including the name of the requester or recipient of the disclosure and the interest of the party in requesting or receiving the disclosure;</p>	<p>For v.1, the only access the SLI provides to third-party users is through applications approved by School Districts.</p> <p>Application providers will request application access to student data. SLI district administrators or users with delegated permissions will use an SLI administrative interface to approve applications and approve the types of student data that applications can access. The SLI will record lists of approved applications.</p> <p>Beyond v1, the SLI may enable third party users to login to something like a research interface to request student data. If this functionality is prioritized by the SLI steering committee, at the request of the SLC this plan will be amended to include the security requirements for this functionality in accordance with the terms of Work Order #1.</p>
<p>C. Electronic acceptance by participating School Districts of terms of use agreements required for participation in SLI;</p>	<p>All users will electronically accept terms of use agreements, via click-through, about use of student data. Further agreements between Districts and/or States and the SLC will be handled offline, as deemed appropriate by the SLC.</p>
<p>D. Electronic agreements between participating School Districts and organizations conducting research for or on behalf of the School Districts; and</p>	<p>The SLI steering committee has not prioritized research functionality for v1. In v1 the only way for third party users to access student data is through approved applications.</p> <p>Beyond v1, the SLI may enable third party users to login to something like a research interface to request student data. If this functionality is prioritized by the SLI steering committee, at the request of the SLI this plan will be amended to include the security requirements for this functionality in accordance with the terms of Work Order #1</p>
<p>E. Destruction or return to a School District of School District records at the request of the School District or upon termination of services to or for the School District.</p>	<p>Districts will be able to stop sending data or request destruction or return of data at any time.</p>