BILL & MELINDA GATES *foundation*

PO Box 23350
Seattle, WA 98102, USA
V 206.709.3100
F 206.709.3180
www.gatesfoundation.org

October 2, 2012

Ken Wagner
Associate Commissioner
Office of Curriculum
Assessment and Educational Technology New York State Education Department
89 Washington Avenue, Room 875 EBA
Albany, NY 12234

Dear Ken:

Please find enclosed, three partially executed Service Agreements with the Shared Learning Collaborative, LLC. Review the document/s thoroughly, including any attached policies and exhibits. If acceptable, please countersign and return to me a scanned/electronic copy of the Agreement by email or fax at (206) 494-7010. We do not require hard copy signatures.

Thank you,

Holly Ashinhurst
Contracts Administrator, U.S. Program

Enclosures: Service Agreement (3)

BILL & MELINDA GATES *foundation*

PO Box 23350
Seattle, WA 98102, USA
V 206.709.3100
F 206.709.3180
www.gatesfoundation.org

October 2, 2012

Ken Wagner
Associate Commissioner
Office of Curriculum
Assessment and Educational Technology New York State Education Department
89 Washington Avenue, Room 875 EBA
Albany, NY 12234

Dear Ken:

Please find enclosed, three partially executed Service Agreements with the Shared Learning Collaborative, LLC. Review the document thoroughly, including any attached policies and exhibits. If acceptable, please countersign and return to me one hard copy of the Agreement by email or fax at (206) 494-7010.

If there is an enclosure or someone is to be copied on the letter, type "cc:" or "Enclosure" three hard returns below the name block and tab over one inch. If more than one person is being copied, please list alphabetically.

Sincerely,

Holly Ashinhurst
Contracts Administrator, U.S. Program

Enclosure: Service Agreement (3)

SERVICE AGREEMENT

This Service Agreement ("Agreement"), dated as of the "Effective Date" specified herein, is made and entered into by and between the Shared Learning Collaborative, LLC ("Service Provider") and the "Customer" specified herein. Service Provider 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. Customer is a State Educational Agency. As a State Educational Agency, Customer is subject to and bound by the Additional Terms applicable to SEAs set forth in Attachment E. This Agreement consists of this Background and Agreement Summary and Signature Page together with the "Attachments" specified herein. Capitalized terms that are not otherwise defined in this Agreement shall have the meanings assigned to such terms in the Data Privacy and Security Policy. This Agreement is not effective unless and until signed by both parties.

Background

The Shared Learning Infrastructure is intended to help School Districts and State Educational Agencies provide teachers, parents, and students access to instructional and assessment tools that integrate information about the student with resources and programs to meet the students' needs. In the course of accessing and using the SLI Service and participating in the SLI Pilot, participating School Districts and State Educational Agencies may disclose, consistent with Section 444(b)(1)(A) of FERPA, Personally Identifiable Information from student education records for students enrolled in the participating School District to the SLI.

The Shared Learning Infrastructure is also intended to benefit State Educational Agencies in performing their functions for evaluating and overseeing compliance in federal and state-supported education programs, both indirectly and through the development and provision of aggregate data or through the disclosure to them of Personally Identifiable Information under Section 444(b)(3)&(5) of FERPA and state Data Privacy and Security Laws. In the course of accessing and using the SLI Service and participating in the SLI Pilot, participating School Districts and State Educational Agencies may disclose Personally Identifiable Information from student education records for students enrolled in the participating School District to the Service Provider, as the authorized representative of the State Educational Agency, consistent with the additional terms in Attachment E.

Service Provider intends to work with State Educational Agencies to determine, prior to Release 1.0 launch: (a) whether there are scalable alternatives to requiring that each additional School District and other Local Educational Agency (LEA) in a State Educational Agency's state enter into a separate, written service agreement with Service Provider; and (b) whether the SLI Service may be expanded to include use of Personally Identifiable Information for third party research purposes, in accordance with FERPA.

Agreement Summary and Signature Page

Customer	
Customer Name:	New York State Educational Department
Department Name:	Information and Reporting Services
Address:	Room 863 Education Building Annex, 89 Washington Avenue
	Albany, NY 12234
Contact Person:	Ken Wagner, Associate Commissioner for the Office of Curriculum and Assessment
Email:	kwagner@mail.nysed.gov
Telephone:	(518) 473-7880
Facsimile:	(518) 473-7737
Effective Date	

This Agreement commences on:	The date this Agreement is countersigned by Customer
Attachments	
This Agreement includes:	Attachment A (Terms & Conditions) Attachment B (SLI Service) Attachment C (Support Services) Attachment D Reserved Attachment E (Additional Terms applicable to SEAs) Attachment F (MOU) Attachment G (Super Administrator(s))

Service Provider and Customer hereby agree to all terms of this Agreement effective as of the Effective Date.

Service Provider:	**Customer:**
Shared Learning Collaborative, LLC	**New York State Educational Department**
By:	**By:** Valerie Grey
Name: Stacey Childress	**Name:** Valerie Grey
Title: Member Manager	**Title:** Executive Deputy Commissioner
Date: September 27, 2012	**Date:** Oct 11 2012

ATTACHMENT A
Terms and Conditions

1. **Definitions.**

1.1 **"Additional Services"** has the meaning provided in Section 5 of this Attachment.

1.2 **"Alpha Release"** means an alpha version of the SLI Service, as described in the "SLC Alpha Environment: Alpha Release Scope & Timeline" document made available to State Educational Agencies and School Districts participating in the SLI Pilot, as may be updated from time to time. A current version of this document (current as of the Effective Date) can be found at: http://slcedu.org/sites/default/files/downloads/SLC%20Alpha%20Scope%20and%20Timeline%2005-25-2012_1.pdf.

1.3 **"Authorized Users"** means Customer Authorized Users and Third Party Authorized Users.

1.4 **"Confidential Information"** means: (i) Personally Identifiable Information contained in Customer Data; and (ii) certain specifications and/or software specifically related to protecting data privacy and security that Service Provider marks or otherwise indicates in writing is to be treated as confidential, restricted or proprietary; provided, however, that this subsection 1.2(ii) may be superseded, as mutually agreed by the parties, once Service Provider has developed and published an intellectual property management plan for the SLI Service.

1.5 **"Customer Authorized User"** means an individual employee or contractor of Customer authorized by Customer in accordance with the Data Privacy and Security Policy and the User Materials to access the SLI Service. For the avoidance of doubt, if Customer is a State Educational Agency, Customer Authorized User does not include an individual employee or contractor of a School District unless authorized by Customer in accordance in accordance with the Data Privacy and Security Policy and the User Materials to access the SLI Service.

1.6 **"Customer Data"** means all information, records, files, and data stored in the SLI Service by or on behalf of Customer, including by any Authorized User. Customer Data may include Personally Identifiable Information.

1.7 **"Custom Role"** shall have the meaning set forth in the Data Privacy and Security Policy.

1.8 **"Customer Output"** means all information, records, files, data, documents, reports, statements, certificates, and other output of the Services created, generated, or processed by or on behalf of Customer.

1.9 **"Data Privacy and Security Laws"** means all applicable federal, state, regional, territorial and local laws, statutes, ordinances, regulations, rules, executive orders, of or by any United States federal or state government entity, or any authority, department or agency thereof governing the privacy and security of Personally Identifiable Information, social security numbers, and security breach notification relating to Personally Identifiable Information (including, without limitation, FERPA), and any other laws in force in any jurisdiction (regulatory or otherwise) in which the SLI Service is being provided.

1.10 **"Data Privacy and Security Policy"** means the Data Privacy and Security Plan provided in Exhibit C to the MOU, attached here as Attachment F. Service Provider intends to replace this Data Privacy and Security Plan no later than Release 1.0 launch with a more comprehensive Data Privacy

and Security Policy, as approved by the independent advisory board following a notice and comment period as described in Section 10.6(b)(iv) and such policy will supersede and replace the Data Privacy and Security Plan and thereafter shall constitute the Data Privacy and Security Policy. Service Provider may thereafter modify the Data Privacy and Security Policy from time to time, as approved by the independent advisory board. Customer's continued use of the SLI Services will indicate its acceptance of the Data Privacy and Security Policy.

1.11 "FERPA" means the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, and the regulations promulgated thereunder, as may be amended from time to time.

1.12 "Industry Standard" means that degree of skill, care and diligence normally shown by (and generally accepted as being appropriate for) information technology industry professionals performing services and work of a scope, purpose and magnitude comparable with the SLI Services.

1.13 "Initial Term" has the meaning provided in Section 8.1 of this Attachment.

1.14 "Malicious Code" means (a) any code, program, or sub-program whose known or intended purpose is to damage or interfere with the operation of the computer system containing the code, program or sub-program, or to halt, disable or interfere with the operation of the SLI Service or related software, code, program, or sub-program, itself, or (b) any device, method, or token, of which one of its intended purposes is to permit a person to circumvent the normal security of the SLI Service or the system containing the code.

1.15 "Memorandum of Understanding" or **"MOU"** means the memorandum of understanding between Service Provider and Customer attached as Attachment F.

1.16 "Normal Business Hours" means 8:00 a.m. – 9:00 p.m. Eastern Time (5:00 a.m. – 6:00 p.m. Pacific Time) Monday through Friday, excluding days recognized as a holiday by Service Provider (including but not limited to New Year's Day, Martin Luther King Jr. Day, Memorial Day, Independence Day, Labor Day, Thanksgiving, Day after Thanksgiving, Christmas Eve, Christmas Day, and New Year's Eve.

1.17 "Personally Identifiable Information" or **"PII"** means any information defined as personally identifiable information under FERPA, as well as names of teachers and other educators.

1.18 "Release 1.0" means a version of the SLI Service that is ready to support production applications to be launched to Authorized Users within states participating in the SLI Pilot. Additional functionality will be prioritized by SLC based on Feedback received during Alpha Release.

1.19 "Role" shall have the meaning set forth in the Data Privacy and Security Policy.

1.20 "School District" or **"District"** means a local educational agency or independent special purpose school system, school network, or a dependent school system under the control of state or local government.

1.21 "Service Provider Data" means all information, records, files, and data created, generated, or collected by Service Provider outside the performance of its Services under this Agreement and not in breach of this Agreement. Service Provider Data does not include Customer Data or Third Party Data.

1.22 "Service Provider Materials" means all Service Provider Confidential Information, specifications, manuals, tapes, programs, documentation, reports, report formats, systems and software (including without limitation, relating to the SLI Service) and other tangible or intangible material of any nature whatsoever used, developed or produced by Service Provider in connection with the Services and/or this Agreement.

1.23 "Services" means the SLI Service (including the SLI Pilot), Support Services, training and any Additional Services.

1.24 "Shared Learning Infrastructure" or **"SLI"** means the software system more fully described on Attachment B.

1.25 "SLI Pilot" means the pilot phase of the SLI Service as described in the MOU, commencing on the effective date of the MOU and continuing through the Initial Term of this Agreement.

1.26 "SLI Pilot Participant" means each of the five (5) State Educational Agencies and six (6) School Districts participating in the SLI Pilot.

1.27 "SLI Service" means access and use of the Shared Learning Infrastructure software as further described in Attachment B.

1.28 "State Educational Agency" or **"SEA"** means the state educational agency primarily responsible for the supervision of public elementary and secondary schools in any of the 50 United States, the Commonwealth of Puerto Rico, or the District of Columbia.

1.29 "Super Administrator" shall have the meaning set forth in the Data Privacy and Security Policy.

1.30 "Support Services" means those technical support and maintenance services provided by Service Provider to Customer under this Agreement and as set forth on Attachment C attached hereto.

1.31 "Third Party Application Providers" means third party application providers that Customer has elected to grant access to the SLI Service and Customer Data in compliance with the requirements of this Agreement for purposes of either: (a) providing services to students in accordance with applicable Data Privacy and Security Laws and FERPA, provided, however, that a State Educational Agency may not provide such access, unless: (i) specifically authorized to do so by a School District; or (ii) the State Educational Agency is itself a Third Party Application Provider for a School District Customer and access is provided to assist the State Educational Agency in performing this function; or (b) providing services to the State Educational Agency as its authorized representative for purposes of the State Educational Agency's evaluation and compliance functions related to federal or state-supported educational Programs.

1.32 "Third Party Authorized Users" means employees or contractors of Third Party Application Providers authorized by Customer in accordance with the Data Privacy and Security Policy and the User Materials, provided, however, that a State Educational Agency may not register such users for purposes of providing services to students, unless specifically authorized to do so by a School District.

1.33 "Third Party Data" means all information, records, files, and data stored in, the SLI Service by or on behalf of a third party not for the benefit or use of Customer. Third Party Data does not include Customer Data or Service Provider Data.

1.34 "User ID" means a unique user identification assigned to an individual Authorized User as set forth in Section 7.2 and in accordance with the Data Privacy and Security Policy.

1.35 "User Materials" means any on-line help files, written technical instructions, or other written instruction manuals regarding the use of the SLI Service, as may be amended from time to time.

2. **SLI Service**

2.1 License. Service Provider grants to Customer a nonexclusive, nontransferable license, during the term of this Agreement, to allow its Authorized Users to access and use the SLI Service on its behalf solely for Customer's use or with respect to Third Party Authorized Users, solely for the benefit of Customer. This license is subject to Customer's and its Authorized Users' (including Third Party Authorized Users') compliance with the terms and conditions set forth in this Agreement.

2.2 Restrictions. Customer may only use the SLI Service to process, manage, and store Customer Data strictly in accordance with Data Privacy and Security Laws; the Data Privacy and Security Policy; FERPA; the User Materials; any agreements between Customer and its School District(s) or State Educational Agency, as applicable, and Third Party Application Providers; and any other restrictions and requirements set forth in this Agreement. During the Initial Term, Customer may not use the SLI Service to process, manage, or store social security numbers, unless and to the extent the parties otherwise agree on a case-by-case basis and reflect such agreement in an amendment to this Agreement.

2.3 Service Suspension. Service Provider reserves the right to suspend access to the SLI Service by Customer, a Third Party Application Provider or an applicable Authorized User:

(a) upon ten (10) days' prior written notice if the other party is in material breach of this Agreement and the breaching party fails to remedy such breach within ten (10) days after notice from the other party; provided ; or

(b) at any time with or without prior written notice if Service Provider reasonably believes such party or person is violating Customer's obligations hereunder with respect to Confidential Information or otherwise using the SLI Service in violation of Data Privacy and Security Laws, the Data Privacy and Security Policy or FERPA.

3. **Authorized Users.**

3.1 Administration.

(a) Customer shall designate one or more Super Administrators in accordance with the Data Privacy and Security Plan and User Materials, and hereby designates as Super Administrator(s) the individual(s) identified in Attachment G, as such designation may be

changed from time to time as provided in User Materials. Through the Super Administrator(s), Customer shall be responsible for assigning and maintaining Roles and Custom Roles (both as defined in the Data Privacy and Security Plan or User Materials) in accordance with the Data Privacy and Security Policy and in order to ensure disclosure of Personally Identifiable Information solely to users with a legitimate need in the Customer Data to carry out the purposes of this Agreement.

(b) Customer, directly or, if Customer is a School District, either directly or through its State Educational Agency, is responsible for maintaining a directory of User IDs for all Authorized Users and associating each User ID with one or more Roles or Custom Roles. As between the parties, Customer is responsible for ensuring that its Authorized Users use only their respective assigned User IDs and will not use another's User ID. Customer will adopt and maintain such security precautions for User IDs and passwords to prevent their disclosure to, and use by, unauthorized persons.

3.2 Disclosures.

(a) **Disclosures by a School District Customer to a State Educational Agency.** Through the Super Administrator, a School District Customer will implement a process to ensure that Customer Data used by a State Educational Agency for evaluation and compliance purposes is disclosed only to authorized representatives of the State Educational Agency, in accordance with Attachment E.

(b) **Disclosures to Third Party Application Providers.** Through the Super Administrator, Customer may approve disclosures of Personally Identifiable Information to a Third Party Application Provider only after the School District from which the Personally Identifiable Information was obtained (by the State Educational Agency or the Service Provider) or the State Educational Agency – if specifically authorized by such School District, or if the Third Party Application Provider is an authorized representative of the State Educational Agency with respect to its functions for evaluating and ensuring compliance with federal and state supported education programs – has entered a written or electronic agreement with such Third Party Application Provider to obtain services from the Third Party Application Provider; if the disclosures are needed to provide such services; and if the agreement provides that the Personally Identifiable Information will be used only for that purpose and that the Personally Identifiable Information will be destroyed when the service is terminated or when the Customer Data is no longer needed for that purpose. An agreement between a State Educational Agency and a Third Party Application Provider as its authorized representative for evaluation and compliance purposes shall comply with the requirements in Attachment E.

4. **Support Services; Service Levels; Maintenance and Additional Services.**

4.1 Support Services. Upon Release 1.0 launch, Service Provider will provide the Support Services to Customer as more specifically set forth in Attachment C attached hereto.

4.2 SLI Service Availability. Upon Release 1.0 launch, Service Provider will use commercially reasonable efforts to make the SLI Service available 24 hours a day, 7 days a week, with an annual uptime percentage of at least 99.9% ("Availability"), during the term of the Agreement, excluding Scheduled Maintenance and Other Causes. The SLI Service is "available" when an Authorized User does not experience a critical system failure in any of the SLC components listed in Attachment B (SLI Service). As used herein, "Other Causes" means (a) downtime caused solely by an Authorized User's use of the SLI Service other than in accordance with this Agreement, the User Materials, the Data Privacy and

Security Policy or other documentation; (b) Customer's lack of availability or untimely response time, as reasonably-requested, to respond to Errors (as defined in Attachment C) that require Customer's participation for source identification or resolution; or (c) unavailability caused by circumstances beyond Service Provider's and its subcontractors' reasonable control, including, without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Service Provider's employees), and computer, telecommunications, Internet service provider ("ISP") or hosting facility failures or delays involving hardware, software or power systems not within Service Provider's and its subcontractors' reasonable control.

4.3 Scheduled Maintenance. Service Provider and its contractors reserve the right to take down applicable servers hosting the SLI Service to make improvements or changes or to conduct routine maintenance checks ("Scheduled Maintenance"). Service Provider will use commercially reasonable efforts to give at least 8 hours' notice prior to any Schedule Maintenance and to perform Scheduled Maintenance Monday through Friday from 9:00 p.m. to 6:00 a.m. Eastern Time (6:00 p.m. to 3:00 a.m. Pacific Time) or weekend hours from 9:00 p.m. Eastern Time Friday (6:00 p.m. Pacific Time) to 6:00 a.m. Eastern Time (3:00 a.m. Pacific Time) Monday. Service Provider will not be responsible for any damages or costs incurred by Customer, if any, for Scheduled Maintenance.

5. **Additional Services.** If requested by Customer, Service Provider may agree to provide, in Service Provider's sole discretion, additional training services and/or consulting, interface development or other services not set forth in Attachment B ("Additional Services"). Upon Service Provider's request, Customer will deliver a written services request to Service Provider for the Additional Services requested by Customer. Service Provider will have no obligation to provide Additional Services prior to its receipt of a properly completed services request and Service Provider's acceptance thereof.

6. **Fees and Payment.**

6.1 Fees. In recognition of Customer's investment of time and resources during the SLI Pilot, Customer will not pay to Service Provider any fees for:

(a) SLI Service or Support Services during the Initial Term; and

(b) Additional Services performed during Alpha Release only, provided Customer is an SLI Pilot Participant

For the avoidance of doubt, additional School Districts within an SLI Pilot Participant's state will not pay any fees for SLI Service or Support Services during the Initial Term, but will pay to Service Provider a fee for any Additional Services as may be mutually agreed in accordance with Section 5.

6.2 Taxes. Each party will bear its own taxes, if any, associated with this Agreement in accordance with applicable law.

7. **Customer Responsibilities.**

7.1 Authorized Users. Customer will: (a) remain responsible for all obligations under this Agreement arising in connection with its Authorized Users' use of the SLI Service, including, without limitation, compliance with Data Privacy and Security Laws and the Data Privacy and Security Policy; and (b) be liable for any act or omission by any of its Authorized Users, which, if performed or omitted by Customer, would be a breach of this Agreement; and any such act or omission of any Authorized User will be deemed to be a breach of this Agreement by Customer. Service Provider reserves the right to require a Third Party Application Provider to agree to Service Provider's then-current standard terms of

use or end user license reasonably requested by Service Provider, which may include but not be limited to specific obligations of Third Party Authorized Users to comply with Data Privacy and Security Laws, the Data Privacy and Security Policy, and FERPA.

7.2 Computer System. Customer will: (a) cooperate and consult with Service Provider in the set-up and activation of the SLI Service for Customer; and (b) provide and maintain, in good and working order at all times, its own Internet access and all necessary communications equipment, software and other materials necessary for Customer Authorized Users to access and use the SLI Service. As between the parties, Customer is responsible for the security of the computer systems of Customer and Customer Authorized Users and the security of the access to and connection with the SLI Service by Customer and Customer Authorized Users. Customer will contractually obligate Third Party Authorized Users to ensure the security of their computer systems and access to and connection with the SLI Service.

7.3 Authorization; Noninfringement; Transmission of Customer Data.

(a) Customer is responsible for obtaining all authorizations, consents, releases, and permissions necessary or desirable to store Customer Data in the SLI Service, to use the SLI Service to process and store Customer Data and to receive the Services and Customer Output.

(b) Customer and its Authorized Users will not submit any Customer Data or use the Services in any way that infringes, misappropriates, or violates any trademark, copyright, patent, trade secret, publicity, privacy or other right of any third party or violates any applicable local, state or federal laws, statutes, ordinances, rules or regulations, including without limitation Data Privacy and Security Laws and FERPA, or any judicial or administrative orders.

(c) When transmitting Customer Data and receiving Customer Output, Customer and its Authorized Users shall use transmission methods that conform to Service Provider's specifications and requirements as described in User Materials. Customer shall be responsible for acquiring at its own expense all equipment needed for such transmission unless otherwise agreed by the parties. Customer shall bear all costs associated with the method of transmission used. Service Provider shall not be liable or responsible for any loss or delay of Customer Data, Customer Output or any other information that pertains to Customer or the Services during any period of transit or electronic transmission to or from the SLI Service, unless and to the extent attributable to the gross negligence or willful misconduct of Service Provider.

7.4 No Interference with Service Operations. Customer will not take any action, and will use commercially reasonable efforts to prohibit its Authorized Users from taking any action, that: (a) interferes or attempts to interfere with the proper working of the SLI Service or engage in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of the SLI Service; or (b) circumvents, disables, or interferes or attempts to circumvent, disable, or interfere with security-related features of the SLI Service or features that prevent or restrict use, access to, or copying of any Customer Data, Service Provider Data, or Third Party Data, or enforce limitations on use of the SLI Service, Customer Data, Service Provider Data, or Third Party Data. Further, Customer will take reasonable actions and precautions to prevent the introduction and proliferation of Malicious Code into the Service Provider's environment and the SLI Service.

7.5 Customer Review and Responsibility. Service Provider makes no representations concerning, and shall not be liable for, the accuracy, completeness, authenticity, or utility of any Customer Data or any Customer Output or concerning the qualifications or competence of any Authorized User that may place Customer Data in the SLI Service. Customer shall be solely responsible for ensuring

accuracy, completeness, authenticity and compliance of any Customer Output provided to any third party, and all liabilities and responsibilities in connection with such Customer Output, and Service Provider shall not be responsible for the accuracy, completeness, or compliance thereof. Other than Service Provider's obligation to destroy Customer's Confidential Information either upon request or upon termination of this Agreement in accordance with Section 10.4 below, Customer will be solely responsible for deleting all Customer Data after such Customer Data is no longer needed.

8. Term and Termination.

8.1 Term. This Agreement will be effective for a term ending on December 31, 2014 ("Initial Term"). The parties may mutually agree to extend the term of this Agreement with such amendments to this Agreement as are appropriate and mutually agreed to for making available the SLI Service after the Initial Term.

8.2 Termination.

(a) Each party will have the right to terminate this Agreement upon thirty (30) days' prior written notice if the other party is in material breach of this Agreement and the breaching party fails to remedy such breach within thirty (30) days after notice from the other party; provided, however: (i) if the failure stated in the notice cannot be corrected within the applicable period, the non-defaulting party will not unreasonably withhold its consent to an extension of such time if corrective action is instituted by the defaulting party within the applicable period and diligently pursued until the default is corrected; and (ii) such extension shall not exceed ninety (90) days after the initial notice.

(b) Each party will have the right to terminate this Agreement for any reason upon ninety (90) days' prior written notice.

(c) Notwithstanding Sections 8.2(a) and (b), either party may terminate this Agreement immediately upon written notice to the other party if the party reasonably believes such other party is intentionally violating its obligations hereunder with respect to Confidential Information or otherwise uses the SLI Service in violation of Data Privacy and Security Laws, the Data Privacy and Security Policy or FERPA.

8.3 Effect of Expiration or Termination.

(a) Upon expiration or termination for any reason, all licenses granted hereunder will automatically terminate (except as otherwise provided in Section 9.2), and Service Provider will immediately disable and discontinue Customer's access to and use of the SLI Service without additional notice to Customer.

(b) Upon expiration or termination for any reason, Service Provider will destroy Customer Confidential Information in Service Provider's possession as provided in Section 10.4(b).

(c) The provisions of Sections 6, 7.4, 8.3, 9, 10, 11.2, 11.3, 11.4, 11.5, 12, 14.1, and 14.3 through 14.14 of this Attachment (together with any other provisions of this Agreement that by their sense and context are intended to survive expiration or termination) will survive any expiration or termination of this Agreement.

9. **Proprietary Rights.**

9.1 Customer Data. Customer grants to Service Provider a non-exclusive license, during the term of this Agreement, to use Customer Data and Customer Output for the purposes of performing Service Provider's obligations under this Agreement. Subject to the foregoing license, Customer will retain all intellectual property and other rights that it may have in the Customer Data and Customer Output. For the avoidance of doubt, as between the parties, Customer owns all Customer Data and Customer Output.

9.2 SLC Code. Following Release 1.0 launch, Service Provider will make production software code developed by or on behalf of Service Provider for the SLI Service available under the Apache License 2.0 (as defined at www.apache.org/licenses), as a reference implementation intended for community maintenance and improvement. Such software code will include, but may not be limited to, software code related to: (a) data stores and API service layers, (b) identity management and single sign-on services, (c) automated bulk data loading tools, (d) interactive bulk data loading tools, (e) standard dashboard application and source code, (f) administration tools, (g) developer sandboxes, and (h) educator and school-building-level staff applications.

9.3 Feedback. To the extent that Service Provider receives from Customer or any of its Authorized Users any suggestions, ideas, improvements, modifications, feedback, error identifications or other information related to the SLI Service or any other products or services ("Feedback"), Service Provider may use, disclose and exploit such Feedback without restriction, including to improve the Services and to develop, market, offer, sell and provide other products and services in furtherance of Service Provider's charitable purpose.

10. **Confidential Information; Compliance with Laws.**

10.1 Public Documents. The parties understand that this Agreement and its attachments will be public documents and may be subject to disclosure under applicable state disclosure laws.

10.2 Obligations. The parties acknowledge that the Services require disclosure by each party ("Disclosing Party") to the other party ("Receiving Party") of certain of the Disclosing Party's Confidential Information. With respect to Confidential Information of the Disclosing Party that is disclosed to the Receiving Party, the Receiving Party shall, subject to the exceptions stated herein:

(a) maintain and protect the confidentiality of the information with the same degree of care and measures to avoid unauthorized disclosure or access as the Receiving Party uses with its own Confidential Information, but in no event less than a reasonable standard of care;

(b) use the information solely to carry out the purposes for which the information was disclosed; and

(c) limit access to the information to: (i) employees of the Receiving Party, or of its subsidiaries or affiliates, who have a need to know to facilitate, monitor or review the delivery, receipt or performance of the Services; (ii) employees of the Receiving Party's contractors, suppliers or licensors who have a need to know the information solely for the purpose of facilitating the performance, delivery or use of the Services; and (iii) the Receiving Party's external attorneys and auditors; or (iv) as otherwise required by law. The Receiving Party shall remain responsible to the Disclosing Party for acts or omissions of such individuals that if committed by the Receiving Party would constitute a violation of the Receiving Party's confidentiality obligations hereunder. Notwithstanding the foregoing, nothing herein shall be

construed to authorize the disclosure of Personally Identifiable Information if such disclosure will violate any Data Privacy and Security Laws, FERPA or any other federal or state law or regulation.

10.3 Exceptions. Except to the extent disclosure would be in violation of any Data Privacy and Security Laws or FERPA, the Receiving Party shall not be in violation of this Agreement for:

(a) disclosing Confidential Information of the Disclosing Party that (i) is or becomes publicly available other than as a result of a breach of this Agreement, (ii) is disclosed to the Receiving Party by a third party not subject to any obligation of confidentiality, (iii) was already known by the Receiving Party prior to the date of this Agreement (unless disclosed in connection with negotiations and discussions related to this Agreement or associated transactions), or (iv) was independently developed by the Receiving Party without reference to Confidential Information received from the Disclosing Party; or

(b) disclosing Confidential Information of the Disclosing Party when required to do so by (i) the Receiving Party's federal or state regulatory agencies, or (ii) a federal or state law or regulation, or a subpoena or court order or agency action that requires disclosure, provided, however, that, if disclosure of Confidential Information is required by any of the foregoing, the Receiving Party shall, at least to the extent required by law, regulation or court or agency order, notify the Disclosing Party and, at the Disclosing Party's request and expense, cooperate with the Disclosing Party's efforts, if any, to prevent or limit the disclosure.

10.4 No License; Destruction of Customer's Confidential Information.

(a) Nothing in this Section shall be construed as a grant or assignment of any right or license in the Disclosing Party's Confidential Information. The Disclosing Party's Confidential Information shall at all times remain the property of the Disclosing Party.

(b) At any time Customer reasonably requests, and in any event when Customer determines that the Confidential Information of Customer is no longer needed to obtain SLI Service, or upon the termination or expiration of this Agreement, Service Provider shall promptly destroy the Customer's Confidential Information in Service Provider's possession; provided that (i) if Customer is a School District, Customer may request or approve that Confidential Information of Customer not be destroyed and be made available to Customer's State Educational Agency for its use in performing their functions for evaluating and overseeing compliance in federal and state-supported educational programs in accordance with Section 444(b)(3)&(5) of FERPA and State Data Privacy and Security Laws, and (ii) at Customer's request, Customer shall be provided up to thirty (30) business days, according to Customer's request, to export Confidential Information of Customer prior to its destruction.

(c) Notwithstanding anything contained in this Section 10.4 to the contrary, during Alpha Release, Service Provider may delete Customer Data without notice.

10.5 Remedies and Responsibilities. The Receiving Party acknowledges that the Disclosing Party has the right to take all reasonable steps to protect the Disclosing Party's Confidential Information, including without limitation, seeking injunctive relief and/or any other remedies that may be available at law or in equity, all of which remedies shall be cumulative and in addition to any rights and remedies available by contract, law, rule, regulation or order. Any requirements for a bond in connection with any such injunctive or other equitable relief are hereby waived by both parties.

10.6 Compliance with Laws. Service Provider and Customer each agree to comply with federal Data Privacy and Security Laws, the Data Privacy and Security Policy and FERPA in connection with performing its obligations under and exercising its rights under this Agreement. Without limiting the foregoing, the Parties agree:

(a) As between the parties, Customer is independently responsible for:

(i) processing and managing Customer Data strictly in accordance with Data Privacy and Security Laws, the Data Privacy and Security Policy, FERPA, the User Materials and any other restrictions and requirements set forth in this Agreement; and

(ii) determining whether this Agreement and the Data Privacy and Security Policy are sufficient to enable Customer to comply with its applicable state and local Data Privacy and Security Laws.

(b) If Personally Identifiable Information is disclosed to Service Provider or its subcontractors, Service Provider is responsible for:

(i) complying, and requiring that its subcontractors comply, with the provisions of, and the obligations imposed on, Service Provider or subcontractor under FERPA and other federal Data Privacy and Security Laws, the Data Privacy and Security Policy, and any other restrictions and requirements set forth in this Agreement;

(ii) no later than Release 1.0 launch, providing public access to the Data Privacy and Security Policy;

(iii) no later than Release 1.0 launch, either requiring its subcontractors comply with the Data Privacy and Security Policy, to the extent applicable, or, if subcontractor is providing cloud hosting services, certifying that such subcontractor has agreed to meet Industry Standard data privacy and security requirements (e.g., in accordance with FedRAMP or other standard mutually agreed by Service Provider and Customer, such agreement not to be unreasonably withheld); and

(iv) no later than Release 1.0 launch, establishing an independent advisory board charged with approving Service Provider's updates to, and compliance with, the Data Privacy and Security Policy. Prior to the review and approval of any material update to the Data Privacy and Security Policy, Service Provider will provide notice to Customers and Customers will have thirty (30) days after such notice to submit written comments to the proposed revisions. At the end of the comment period, the independent advisory board will in good faith review any written comments submitted and may approve updates to the Data Privacy and Security Policy. If the independent advisory board approves any updates to the Data Privacy and Security Policy, Service Provider will notify Customer by email at the email address provided on page one of the Agreement and make the updated Data Privacy and Security Policy publicly available.

(c) Service Provider's subcontractors will not be permitted to share Personally Identifiable Information provided by Customer with parent companies or other affiliates without the express written consent of Customer.

11. **Warranty; Limitations; Disclaimer.**

11.1 Limited Warranty. Service Provider warrants that:

(a) the SLI Service will perform materially as described in this Agreement, the Data Privacy and Security Policy and User Materials;

(b) The SLI Services will be performed in accordance with Industry Standards, provided however that if a conflicting specific standard is provided in User Materials, the User Materials will prevail; and

(c) Service Provider will maintain adequate and qualified staff and subcontractors to perform its obligations under this Agreement.

11.2 Privacy and Security Limitations. Service Provider does not warrant or represent that by using the SLI Service, Customer will be in compliance with Data Privacy and Security Laws, FERPA or any other federal or state law or regulation. Service Provider does not warrant that its electronic files containing Customer Data are not susceptible to intrusion, attack, or computer virus infection, but given the confidential nature of much of this Customer Data, Service Provider will (a) implement reasonable and appropriate measures for the SLI Service (as determined by Service Provider, but consistent with Industry Standards, and consistent with the Data Privacy and Security Policy) designed to reasonably secure Customer Data against accidental or unlawful loss, access or disclosure; and (b) in the event of a security breach that results in accidental or unlawful loss, access or disclosure of Customer's Confidential Information, a party shall immediately notify the other party after becoming aware of such breach. If any individual(s) are required by applicable federal or state law to be notified about a security breach that is attributable to Service Provider's breach of its obligations under this Agreement, Service Provider shall bear all direct and reasonable costs associated with such notifications. Service Provider will take reasonable actions and precautions in accordance with the Industry Standard to prevent the introduction and proliferation of Malicious Code into the SLI Service and Customer systems that feed Customer Data into the SLI Service.

11.3 Service Limitations. The SLI Service may be temporarily unavailable from time to time due to Scheduled Maintenance, telecommunications interruptions, or Other Causes as more fully described in Section 4.2 above. Service Provider may also make improvements and/or changes in the SLI Service at any time without notice, subject to Section 4.3 above. Service Provider will not be responsible for any damages that Customer may suffer arising out of use, or inability to use, the SLI Service. Service Provider will not be liable for alteration, destruction, corruption, or loss of Customer Data through accident, fraudulent means or devices, or any other method unless and to the extent attributable to the gross negligence or willful misconduct of Service Provider or its subcontractors. It is hereby acknowledged that it is Customer's responsibility to validate for correctness all Customer Output and to protect Customer Data from loss by maintaining back-ups of all Customer Data and routinely updating such back-ups. Customer hereby waives any damages occasioned by lost or corrupt Customer Data or incorrect Customer Output, resulting from a programming error, operator error, equipment or software malfunction, or from the use of third-party software, unless and to the extent such damages result from Service Providers breach of Section 11.1.

11.4 Disclaimer of Warranties. EXCEPT AS SET FORTH IN SECTION 11.1, SERVICE PROVIDER MAKES NO WARRANTIES RELATED TO THE SERVICES PROVIDED BY SERVICE PROVIDER HEREUNDER, AND HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NONINFRINGEMENT. CUSTOMER ASSUMES TOTAL RESPONSIBILITY FOR THE SELECTION OF THE SERVICES TO ACHIEVE CUSTOMER'S INTENDED RESULTS AND FOR ITS USE OF THE RESULTS OBTAINED FROM THE SERVICES. SERVICE PROVIDER DOES NOT WARRANT THAT THE SERVICES MEET CUSTOMER'S REQUIREMENTS OR WILL BE UNINTERRUPTED OR ERROR FREE.

11.5 Limitations of Liability. IN NO EVENT WILL SERVICE PROVIDER (INCLUDING ITS SUBSIDIARIES, ITS MEMBERS AND SUBSIDIARIES OF ITS MEMBERS, ITS SERVICE PROVIDERS AND LICENSORS, AND THE EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS THEREOF) BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR PUNITIVE DAMAGES UNDER THIS AGREEMENT OR IN CONNECTION WITH ANY SERVICES PROVIDED BY SERVICE PROVIDER HEREUNDER ARISING OUT OF THE USE OR INABILITY TO USE THE SERVICES, CUSTOMER DATA OR ANY CUSTOMER OUTPUT, EVEN IF SERVICE PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF AVAILABLE REMEDIES ARE FOUND TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE. THE TOTAL LIABILITY, IF ANY, OF SERVICE PROVIDER (INCLUDING ITS SUBSIDIARIES, ITS MEMBERS AND SUBSIDIARIES OF ITS MEMBERS, ITS SERVICE PROVIDERS AND LICENSORS, AND THE EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS THEREOF) IN THE AGGREGATE OVER THE TERM OF THIS AGREEMENT FOR ALL CLAIMS, CAUSES OF ACTION OR LIABILITY WHETHER SOUNDING IN CONTRACT, TORT OR OTHERWISE ARISING UNDER OR IN ANY WAY RELATED TO THIS AGREEMENT AND/OR THE SERVICES PROVIDED HEREUNDER (COLLECTIVELY, "CLAIMS'), SHALL BE LIMITED TO THE LESSER OF: (a) CUSTOMER'S DIRECT DAMAGES, ACTUALLY INCURRED; OR (b) $100,000 ("AGGREGATE CAP"); PROVIDED HOWEVER THAT THE AGGREGATE CAP SHALL NOT APPLY TO: (1) SERVICE PROVIDER'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 12 (INDEMNIFICATION); (2) CLAIMS WHICH ARISE OR RESULT FROM FRAUDULENT ACTS, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF THE SERVICE PROVIDER OR ITS SUBCONTRACTORS; (3) SERVICE PROVIDER'S BREACH OF ITS OBLIGATIONS UNDER SECTION 10.6 (COMPLIANCE WITH LAWS), AND (4) CLAIMS FOR PERSONAL INJURY AND DAMAGE TO TANGIBLE PERSONAL PROPERTY OR REAL PROPERTY ARISING OUT OF THE NEGLIGENCE OF SERVICE PROVIDER. WITH RESPECT TO ANY BREACH BY SERVICE PROVIDER OF ITS OBLIGATIONS UNDER SECTION 10.6 (COMPLIANCE WITH LAWS) SUCH TOTAL LIABIILTY IN THE AGGREGATE OVER THE TERM OF THIS AGREEMENT FOR CLAIMS SHALL BE LIMITED TO THE LESSER OF: (x) CUSTOMER'S DIRECT DAMAGES, ACTUALLY INCURRED; OR (y) $1,000,000. NOTWITHSTANDING THE FOREGOING, SERVICE PROVIDER'S SOLE OBLIGATION FOR A BREACH OF WARRANTY UNDER SECTION 11.1 SHALL BE LIMITED TO REPROCESSING APPLICABLE CUSTOMER DATA OR REPERFORMING THE SERVICES. SERVICE PROVIDER (INCLUDING ITS SUBSIDIARIES, ITS MEMBERS AND SUBSIDIARIES OF ITS MEMBERS, ITS SERVICE PROVIDERS AND LICENSORS, AND THE EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS THEREOF) SHALL HAVE NO LIABILITY, EXPRESS OR IMPLIED, WHETHER ARISING UNDER CONTRACT, TORT OR OTHERWISE, FOR ANY CLAIM OR DEMAND: (i) TO THE EXTENT RESULTING DIRECTLY OR INDIRECTLY FROM CUSTOMER'S INTERNAL OPERATIONS, EQUIPMENT, SYSTEMS OR SOFTWARE OWNED OR LICENSED BY CUSTOMER; OR (ii) BY THIRD PARTIES, EVEN IF SERVICE PROVIDER WAS ADVISED OF THE POSSIBILITY OF SUCH CLAIMS OR DEMANDS, EXCEPT AS EXPRESSLY PROVIDED OTHERWISE HEREIN.

12. **Indemnification.**

12.1 Indemnification of Customer by Service Provider. Subject to the limitations of liability in Section 11, Service Provider shall indemnify and hold harmless Customer, its officers, agents, employees, affiliates, subsidiaries, assigns and successors in interest (collectively, the "Customer Indemnitees" and individually each a "Customer Indemnitee") from and pay any final judgments awarded against Customer, and pay Customer's reasonable costs and attorneys' fees resulting from any claims, liabilities, losses, suits, and damages asserted by a third party based on Service Provider's alleged infringement of any patent, copyright, trademark, trade secret, or other intellectual property or proprietary rights of such third party under the laws of the United States arising out of the Service Provider Materials, unless and except to the extent that such infringement is caused by Service Provider's compliance with Customer's unique specification or instructions or Service Provider's use of trademarks, Customer Data, or other materials supplied by Customer or Authorized Users.

12.2 Indemnification Procedures. If any third party makes a claim covered by Section 12.1 against a Customer Indemnitee with respect to which such Customer Indemnitee intends to seek indemnification under this Section, Customer shall give prompt written notice of such claim to Service Provider, including a brief description of the amount and basis therefor, if known. Upon giving such notice, Service Provider shall have the right to defend such Customer Indemnitee against such claim, and shall be entitled to assume control of the defense of the claim with counsel chosen by Service Provider, reasonably satisfactory to the Customer Indemnitee. Customer and the Customer Indemnitee shall cooperate fully with and assist Service Provider in its defense against such claim in all reasonable respects. Notwithstanding the foregoing, the Customer Indemnitee shall have the right to employ its own separate counsel in any such action, but the fees and expenses of such counsel shall be at the expense of the Customer Indemnitee. Service Provider shall not be liable for any settlement of action or claim effected without its consent.

13. **Insurance.** Service Provider, at Service Provider's expense, will procure and maintain during the Initial Term, a minimum $2,500,000 per occurrence/$5,000,000 aggregate limit of Professional Liability, covering technology errors and omissions, privacy liability, network security and liability, and network extortion. Insurance coverage will be issued by a fiscally sound insurance carrier. Service Provider will make available certificates or other evidence of satisfaction of the above insurance requirements upon the request of Customer. Such forms will name Customer as additional insured under Professional Liability, and shall specify that, in the event of cancellation, material change, potential exhaustion of the aggregate limit, or non-renewal of insurance coverage, notice will be given to Customer in accordance with the policy provisions.

14. **General.**

14.1 Assignment, Successors. Service Provider may freely assign this Agreement, in whole, to a not-for-profit entity that expressly assumes the Service Provider's rights and obligations hereunder arising after the date of assignment; provided however that Service Provider's successors and permitted assigns may not thereafter assign, transfer, convey, sublet or otherwise dispose of this Agreement or its right, title or interest therein or its power to execute such Agreement, to any other person or corporation without the previous written consent of Customer, not to be unreasonably delayed, condition, or withheld. No right or license under this Agreement may be assigned or transferred by Customer, nor may any duty be delegated by Customer without Service Provider's prior written consent. Any assignment, transfer or delegation in contradiction of this provision will be null and void. Subject to the foregoing, this Agreement will bind and inure to the benefit of the successors and assigns of Customer and Service Provider.

14.2 Audit.

(a) Customer shall have the right, at Customer's expense, to conduct independent code and network security reviews following each major release (i.e., Alpha Release, Release 1.0, etc.), and no more than once every six (6) months thereafter, upon reasonable notice to Service Provider and at reasonable times. Notwithstanding the foregoing, if Customer has reasonable cause to believe Service Provider is not in compliance with this Agreement, Customer may perform an independent code and network security review up to once every three (3) months.

(b) Service Provider shall establish and maintain records pertaining to Customer's use of the SLI Service including, without limitation, logs of disclosures of Personally Identifiable Information to third parties meeting all FERPA requirements pertaining to records of disclosures, and security and audit logs (collectively, "Records"). Customer shall have the right, at Customer's expense, to audit, review and copy such Records upon reasonable notice to Service Provider and at reasonable times; provided, however, that such Records will be made available to Customer at no cost provided that such Records be made available to Customer at no cost in a format that can be downloaded or otherwise duplicated.

14.3 Subcontracting. Service Provider may freely subcontract its duties and obligations under this Agreement. In the event that Service Provider subcontracts any of its duties and obligations, Service Provider agrees that: (i) the third party contractor shall execute an agreement regarding confidentiality consistent with the terms of this Agreement to the extent that such third party contractor has access to Confidential Information of Customer and an agreement relating to any other obligations of such contractor as required to comply with Data Privacy and Security Laws, the Data Privacy and Security Policy and FERPA, and (ii) any such permitted subcontracting shall not release Service Provider from any of its obligations under this Agreement.

14.4 Force Majeure. Notwithstanding any other provision of this Agreement, no party to the Agreement shall be deemed in default or breach of this Agreement or liable for any loss or damages or for any delay or failure in performance (except for the payment of money) due to any cause beyond the reasonable control of such party.

14.5 Governing Law. The validity, construction, and interpretation of this Agreement and the rights and duties of the parties hereto shall be governed by the internal laws of the State of Washington, excluding its principles of conflicts of laws.

14.6 Notice. All notices required or permitted under this Agreement will be in writing and sent by certified mail, return receipt requested, or by reputable overnight courier, or by hand delivery. The notice address for Service Provider is Stacey Childress, Chair, SLC Board of Managers, In care of: Bill & Melinda Gates Foundation, PO Box 23350, Seattle, WA 98102; and the notice address for Customer is Ken Wagner, Associate Commissioner for the Office of Curriculum and Assessment, Room 863 Education Building Annex, 89 Washington Avenue, Albany, NY 12234. Any notice sent in the manner set forth above shall be deemed sufficiently given for all purposes hereunder (i) in the case of certified mail, on the third business day after deposited in the U.S. mail, and (ii) in the case of overnight courier or hand delivery, upon delivery. Either party may change its notice address by giving written notice to the other party by the means specified in this Section.

14.7 Independent Contractor. Service Provider is acting as an independent contractor in its capacity under this Agreement. Nothing contained in this Agreement or in the relationship of the Customer and Service Provider shall be deemed to constitute a partnership, joint venture, or any other

relationship between the Customer and Service Provider except as is limited by the terms of this Agreement.

14.8 Entire Agreement; Amendments; Memorandum of Understanding.

(a) This Agreement, together with the attachments hereto, constitutes the entire agreement between Service Provider and Customer with respect to the subject matter hereof. There are no restrictions, promises, warranties, covenants, or undertakings other than those expressly set forth herein and therein. Except as provided in Section 14.8(b), this Agreement supersedes all prior negotiations, agreements, and undertakings between the parties with respect to such matter. This Agreement, including the exhibits hereto, may be amended only by an instrument in writing executed by the parties or their permitted assignees.

(b) If Customer is a School District, the MOU is attached for reference purposes only. If Customer is the State Educational Agency that is party to the MOU, Customer and Service Provider agree that: (i) notwithstanding Section B.6 of the MOU to the contrary, the term of the MOU shall survive execution of this Agreement and expire on December 31, 2014; and (ii) the terms of this Agreement, together with its other attachments, shall prevail over any conflicting terms contained in the MOU, including but not limited to MOU Paragraphs B.2.c (Privacy and Security), B.3.d (Test Data), B.3.e (Notice), B.3.f (SLI Implementation), B.6 (Term), and B.7 (Confidentiality and Publicity), and MOU Exhibit C (Data Privacy and Security Plan).

14.9 Construction of Agreement; Headings. No provision of this Agreement shall be construed against or interpreted to the disadvantage of any party hereto by any court or arbitrator by reason of such party having or being deemed to have structured or drafted such provision. The headings in this Agreement are for reference purposes only and shall not be deemed to have any substantive effect.

14.10 Severability. If any provision of this Agreement is held by a court or arbitrator of competent jurisdiction to be contrary to law, then the remaining provisions of this Agreement will remain in full force and effect.

14.11 Publicity.

(a) Service Provider will use reasonable efforts to notify Customer by email to tdunn@mail.nysed.gov (Tom Dunn) prior to referencing Customer in any press releases, media statements, press or media interviews, or presentations about this Agreement, the Technology Build, the SLI Pilot, or the SLI Service. In any event, a copy or recording of such materials, if any, will be promptly provided to the Customer after the release.

(b) Customer will use reasonable efforts to notify Service Provider by email to slcteam@waggeneredstrom.com prior to referencing Service Provider, this Agreement, the Technology Build, SLI Pilot, or the SLI Service in any press releases, media statements, press or media interviews, or presentations. Customer will use all reasonable efforts to provide Service Provider with an advance copy of any press releases, media statements, presentations, or other written material intended for public release in order to allow Service Provider to review and provide comment. In any event, a copy or recording of such materials, if any, will be promptly provided to the Service Provider after the release.

14.12 No Third Party Beneficiaries. Except as expressly provided herein, this Agreement is entered into solely between, and may be enforced only by, Customer and Service Provider. This Agreement will not be deemed to create any rights or causes of action in or on behalf of any third parties,

including employees, students, suppliers and customers of a party, or to create any obligation of a party to any such third parties.

14.13 Waiver. The failure of either party at any time to require performance by the other party of any provision of this Agreement shall not affect in any way the full right to require the performance at any subsequent time. The waiver by either party of a breach of any provision of this Agreement shall not be taken or held to be a waiver of the provision itself. Any course of performance shall not be deemed to amend or limit any provision of this Agreement.

14.14 Counterparts; Signatures. This Agreement may be signed in counterparts with the same effect as if the signatures were upon a single instrument, and all such counterparts together shall be deemed an original of this Agreement. For purposes of this Agreement, a facsimile copy of a party's signature shall be sufficient to bind such party.

ATTACHMENT B

SLI Service

The Shared Learning Infrastructure is a web-based software (SaaS: Software as a Service) system. The Shared Learning Infrastructure and the SLI Service will include the following components:

- A multi-tenant data store, a portion of which is provisioned for use solely by Customer, securely partitioned from portions made available to other customers, to store and retrieve Customer Data.
- A secure landing zone, provisioned for use solely by Customer to upload Customer Data to the SLI Service.
- A data ingestion service, which populates the data store from correctly-formatted Customer Data by uploading to the secure landing zone.
- A data validation service, which provides error reports to Customer, upon completion of the data ingestion service acting upon Customer Data. Validation may include determination of file completeness, correct file structure, adherence to data constraint requirements and referential integrity, as described in User Materials.
- An application program interface (API), providing authentication and controlled access to Customer Data in the data store. Access will include reading, creating, deleting and updating Customer Data in the data store.
- A data browser, which may be used for troubleshooting and viewing Customer Data in the data store. Viewable on any web-enabled device.
- A dashboard application, which Authorized Users may access to view various representations of Customer Data. Viewable on any web-enabled device.
- A user and application authentication and authorization service, which supports authentication and authorization of applications and users in a single sign-on (SSO) manner, for Third Party Application Providers that conform to User Materials.
- Support for federated identity integration using SAML 2.0, which allows Customer to maintain a list of Authorized Users, and assignment of Authorized Users to Roles, using an identity provider (directory service) hosted by Customer. Customer must allow Service Provider access to such directory service via the SAML 2.0 protocol and trust relationship.
- A portal service, sufficient to demonstrate functionality of applications made available by Service Provider, allow single sign-on (SSO) using the OAuth 2.0 authentication protocol, and display of Third Party Application Providers that conform to User Materials. The portal service is not intended for high-volume usage, as defined in the industry and the User Materials.
- A learning registry index service and associated API that provide storage and retrieval of information about learning standards and objectives, learning resources, and learning standard-aligned content, including resource location, description and usage-related metadata.

User Materials for the SLI Pilot can be found here: http://slcedu.org/technology/technical-specifications/slc-pilot-phase-project-documents.

ATTACHMENT B
APPENDIX A

SLI Service Related to Customer-Specific Implementations

As part of the SLI Service, Customer may request, and Service Provider may agree to provide, additional applications and source code, itemized below, that may be used as the basis for Customer-specific implementations.

- Content tagging tool, used to associate location, description, learning standard alignment, and usage metadata with learning resources.
- Search application, used to locate learning resources within the learning registry index service and the Bing search engine.
- Learning map authoring tool, used to create learning maps by associating learning objectives with each other to create learning paths.
- Learning map visualizations, used to create graphical representations of a learning map.
- One or more additional teacher- or administrator-facing sample applications that address the needs of two or more of the State Educational Agencies or School Districts participating in the SLI Pilot.

ATTACHMENT C

Support Services

Support Requests. Service Provider will provide support for SLI Services (not including SLI Services related to Customer-specific implementations described in Attachment B, Appendix A) during Normal Business Hours in response to telephone and email queries from Customer as described in this Attachment.

Error Resolution. If Customer identifies an Error, Customer will report the Error to Service Provider in accordance with Service Provider's support procedures. Customer will provide all information reasonably requested by Service Provider and will give Service Provider assistance and co-operation to enable Service Provider to properly perform the activities included in this Attachment. An "Error" is an event where the SLI Service does not perform substantially as described in the User Materials.

Service Provider will assign a category and work to resolve reported Errors as follows:

Error Severity	Resolution	First Response Time	System Components
Severity 1 Error Critical System Failure	SLC will work continuously until Error is resolved	1 hr 24x7x365	Critical SLC Service components only, which include: Landing zone; data input/output API; data ingestion; authentication / authorization; security related issues
Severity 2 Error Non-Critical System Failure	SLC will work during Normal Business Hours until Error is resolved	2 hrs during Normal Business Hours	All other non-critical SLC Service components
Severity 3 Error System Failure but Work-around Available	Error will be placed in backlog	1 day during Normal Business Hours	All SLC Service components
Severity 4 Error Minor or Aesthetic Issue	Error will be placed in backlog	1 day During Normal Business Hours	All SLC Service components

Service Provider will give first priority to resolving Severity 1 Errors. If Service Provider provides a workaround for a Severity 1 Error, it will be downgraded to a Severity 3 Error. Resolution of higher severity errors is given priority over the resolution of lower severity errors.

Errors may be classified as issues with the Customer Data uploaded into the SLC Service. Customer will be responsible for correcting issues in the Customer Data. Incorrectly transformed Customer Data may have to be reloaded by Customer.

Business Continuity Objectives. "Recovery Time Objective" (tolerable duration of time that the system can be down after a failure or disruption) is 24 hours. "Recovery Point Objective" (tolerable age of data that must be reloaded after a system failure or disruption) is 24 hours.

System Administrator. Customer will provide Service Provider a designated system administrator / support contact with all relevant contact information to respond to questions from Service Provider regarding the SLI Service and Service Provider's provision of Services.

Support Exceptions. Service Provider will not be responsible or liable with respect to any problems or issues arising from (i) unauthorized or improper use of the SLI Service; (ii) modification, alteration or

configuration of the SLI Service by or for Customer that has not been authorized in writing by Service Provider, (iii) hardware, software, technology or intellectual property which has not been provided by or on behalf of Service Provider pursuant to this Agreement, (iv) communications facilities; (v) any breach of this Agreement by Customer, or any act or omission of any Authorized User which, if performed or omitted by Customer would be a material breach of this Agreement, and/or (vi) any act or omission of Customer or any Authorized User that prevents, delays, disturbs or interferes with Service Provider's performance of its obligations hereunder.

ATTACHMENT D

Reserved

ATTACHMENT E

Additional Terms Applicable to SEAs

A State Educational Agency that participates by accessing the SLI Service in accordance with this Agreement and discloses Personally Identifiable Information derived from student records to the SLI to assist it in performing evaluation and compliance activities related to federal- and state-supported education programs is subject to the following additional terms:

1. The State Educational Agency hereby designates the Service Provider (and its contractors that perform services to carry out this purpose) as its authorized representative to assist it in carrying out evaluation and compliance activities related to federal- and state-supported education programs, within the scope of this Agreement.

2. The State Educational Agency will disclose Personally Identifiable Information to the SLI Service from source systems maintained by the New York State Education Department and its authorized representatives including (i) student demographic, enrollment, program service, and assessment data; and (ii) educator assignment, certification, performance, and other related data (collectively, "SEA Data"). The State Educational Agency will only disclose SEA Data: (i) when the SEA is the authoritative source of data needed for applications that School District Customers have elected to utilize; (ii) when utilization of SEA Data will avoid or limit redundant data entry or verification on behalf of School District Customers; or (iii) when necessary to support an evaluation or compliance activity by an authorized representative of the State Educational Agency related to federal- and state-supported education programs.

3. The State Educational Agency intends for the SLI Service to serve as a technology platform to support its overall evaluation and compliance activities. SEA Data maintained within the SLI Service may be utilized to support state evaluation or compliance activities to the fullest extent permitted by state and federal law. However, the State Educational Agency will not utilize Personally Identifiable Information, other than SEA Data, for evaluation or compliance activities without the prior authorization of the School District Customer(s) who submitted such data to the SLI Service.

4. Consistent with the Data Privacy and Security Policy, Personally Identifiable Information disclosed to the SLI Service shall be disclosed only to authorized representatives designated or approved by the State Educational Agency with a legitimate interest in the indicated evaluation or compliance purposes and protected from further disclosures beyond those authorized in this Agreement and the participating School District's agreement with the Service Provider.

5. Personally Identifiable Information provided to the Service Provider and to its sub-contractors shall be destroyed when the Agreement is terminated or when the Personally Identifiable Information is no longer needed for services to the State Educational Agency.

6. The State Educational Agency shall use "reasonable methods," consistent with provisions of this Agreement and the Data Privacy and Security Policy, to ensure to the greatest extent practicable that its authorized representatives use Personally Identifiable Information only for the indicated evaluation/compliance purposes and protect it from further disclosure.

   The State Educational Agency may not grant access to the SLI Service to Third Party Application Providers (as defined in Attachment A, section 1.31 of the Agreement) for purposes of providing services directly to students, unless specifically authorized to do so by a School District or as otherwise authorized by FERPA. However, a State Educational Agency may be a Third Party Application Provider of a School District that is a customer of SLI Service for such purposes, and, if so, may grant access to another Third Party Application Provider to assist it in performing these services.

ATTACHMENT F

Memorandum of Understanding

Attached

THE STATE EDUCATION DEPARTMENT / THE UNIVERSITY OF THE STATE OF NEW YORK / ALBANY, NY 12234

EXECUTIVE DEPUTY COMMISSIONER
(518) 473-8381
E-mail: vgrey@mail.nysed.gov

April 13, 2012

Mr. Henry Hipps
Senior Program Officer
College Ready: Next Generation Models
Bill & Melinda Gates Foundation
P.O. Box 6176, Ben Franklin Station
Washington, DC 20044-6176

Dear Mr. Hipps:

Enclosed for signature are two copies of a Memorandum of Understanding ("MOU") between the Shared Learning Collaborative, LLC (Company) and the New York State Education Department (NYSED). This MOU memorializes the Company's and NYSED's shared vision for the Shared Learning Infrastructure (SLI), their understanding regarding the purpose of the SLI Pilot, and each organization's role during the SLI Pilot.

Please return one original signed copy of the MOU to:

Anne Campbell
New York State Education Department
Bureau of Fiscal Management
Room 410, EB
89 Washington Avenue
Albany, NY 12234

If you have any questions regarding this MOU, please contact Ken Wagner at 518-473-7880.

Sincerely,

Valerie Grey

Enclosure
c: Ken Wagner
bc: Ken Slentz
Joanne Morelli
Bureau of Budget Coordination
Bureau Fiscal Management
Office of Counsel

MEMORANDUM OF UNDERSTANDING
Between the Shared Learning Collaborative, LLC
And
New York State Education Department

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 New York State Education Department ("NYSED") so that NYSED 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, Education Data Portal (EDP) / Student Information Repository System (SIRS) (hereinafter "State Ed Infrastructure").

3. This Memorandum of Understanding ("MOU") memorializes the Company's and NYSED'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 NYSED'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 NYSED each acknowledges the purpose of the SLI Pilot is to develop, test and implement the SLI in a limited number of states including NYSED. The Company and NYSED 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 NYSED 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. NYSED 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 NYSED to help it secure commitments from education content application and technology services vendors, of particular interest to NYSED, 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 NYSED to complete a technology landscape of NYSED's State Ed Infrastructure and to determine the appropriate level of integration and relationship between the SLI and NYSED's State Ed Infrastructure. The Company and NYSED intend for that landscape to assist NYSED in identifying i) the interdependencies between the SLI and the State Ed Infrastructure, and ii) the opportunities for NYSED to leverage the SLI and reduce the scope of NYSED's investments in State Ed Infrastructure. Additional interdependencies of the State Ed Infrastructure on the SLI may be identified by NYSED from time to time, and, if so, the Company and NYSED intend to make good faith efforts to address such interdependencies. The Company intends to assist NYSED, for example by reviewing any RFP language, providing documentation related to the SLI to support NYSED'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, NYSED 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 NYSED acknowledge that prior to NYSED 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, NYSED 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 though B.2.c and B.3.a through B.3.d and the referenced Exhibits, it will promptly notify NYSED in writing to the address set forth below:

Ken Wagner / Assistant Commissioner for Data Systems
New York State Education Department
Information and Reporting Services
Room 863 Education Building Annex
89 Washington Avenue
Albany, NY 12234

In the event that NYSED 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 NYSED 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 NYSED 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 NYSED.

4. **The Parties' Joint Acknowledgments of Risk and Mitigation**. The Company and NYSED 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 NYSED's shared vision for the SLI.

The Company and NYSED 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 NYSED's state and the opportunity to extend the functionality and value of NYSED's current and future investments in State Ed Infrastructure.

To contribute to the mitigation of risk, the Company and NYSED 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. *NYSED's Project Team:*
   - Ken Wagner, Project Owner
   - Kathleen Moorhead, Project Manager
   - David Walsh, CIO
   - Doug Jaffe, Regents Fellow
   - Sandeep Chellani, Pilot District Project Owner
   - Sapna Moudgil-Shah, Pilot District Team
   - Lisa Goldschmidt, Pilot District Curriculum Expert
   - David Price, Pilot District Team

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 NYSED, 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 NYSED of a service level agreement governing implementation of the SLI, whichever is earlier.

7. **Confidentiality and Publicity**.

a. The Company and NYSED 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 NYSED 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 NYSED in evaluating and making internal decisions about its State Ed Infrastructure.

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

c. NYSED 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. NYSED 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, NYSED 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 NYSED 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 NYSED; **except for the confidentiality obligations set forth in Section B.7, which the Company and NYSED 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 NYSED, notwithstanding that both are not signatories to the original or to the same counterpart.

SHARED LEARNING COLLABORATIVE, LLC

By: Stacey Childress

Name: Stacey Childress

Title: Member and Chair, Board of Managers

Date: April 19, 2012

NEW YORK STATE EDUCATION DEPARTMENT

By: Valerie Grey

Name: Valerie Grey

Title: Executive Deputy Commissioner

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 NYSED'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 NYSED feature design, and prioritization decisions, project timelines, and draft/final technical and functional design documents for the Technology Build and solicit NYSED'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 **NYSED's Participation in the SLI Pilot.** Consistent with paragraph B.3.a of the MOU, NYSED 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.* NYSED 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.

NYSED has identified the following as its technical point of contact for the SLI pilot: Kathleen Moorhead, Project Manager, kmoorhea@mail.nysed.gov.

b. *SLI Pilot and Local Education Agencies.* NYSED intends to identify Local Education Agencies ("LEAs") within NYSED's state that will participate in the SLI Pilot with NYSED ("Participating LEAs"). NYSED 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. NYSED 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.* NYSED 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.* NYSED, 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.* NYSED 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 NYSED, Participating LEAs, or schools within those LEAs. NYSED intends to establish, or has established, and utilize a unique, stable identifier to tag each teaching, learning and assessment object that NYSED 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, NYSED 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.* NYSED recognizes that any enhancements made by or on behalf of NYSED to open source licensed SLI code will be made available consistent with the terms of such license. The Company and NYSED agree that software and applications developed by or on behalf of NYSED 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 NYSED'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, NYSED 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 NYSED'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	StudentObjectiveAssessement
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 Figures

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:

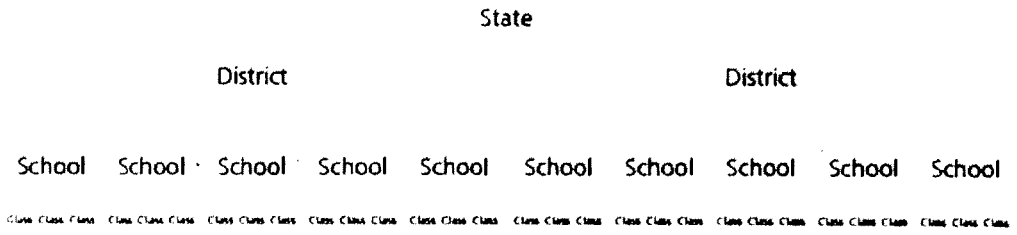

Figure 1 - State/District/School/Class Hierarchy

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.

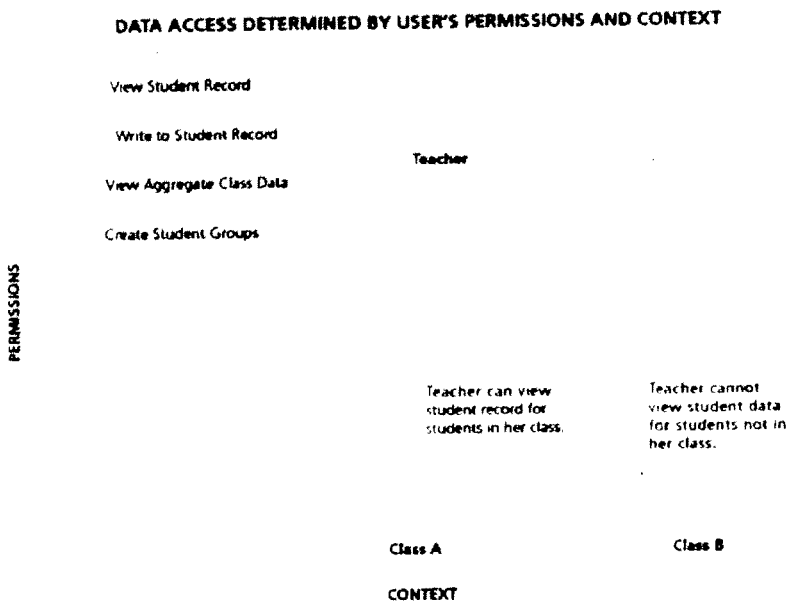

Figure 2 – Example of User Permissions and Context

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.

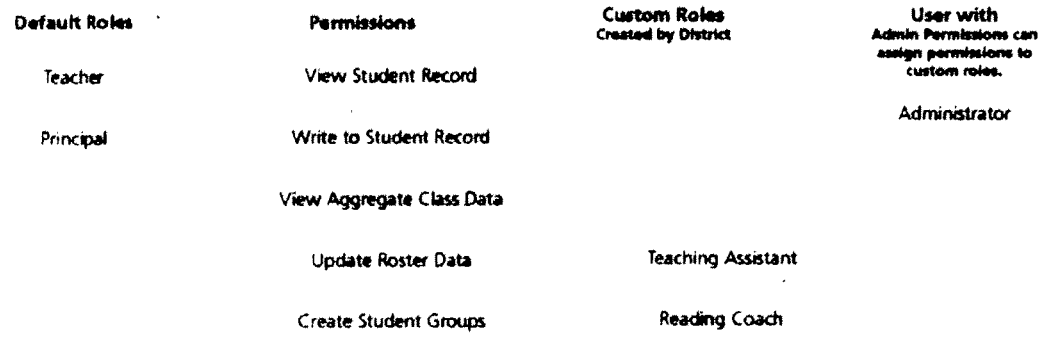

Figure 3 – Example of Default Roles, Custom Roles, and Assigning Permissions

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.

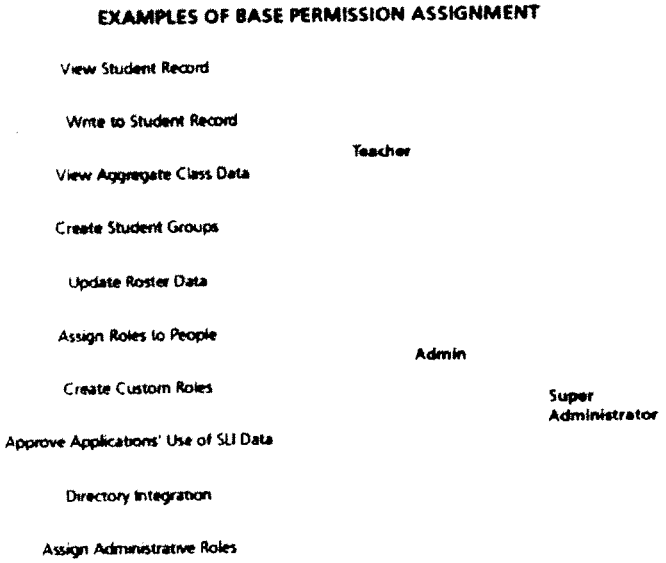

Figure 4 - Examples of Base Permission Assignment

3.3 Authentication and Authorization

Usernames, 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.

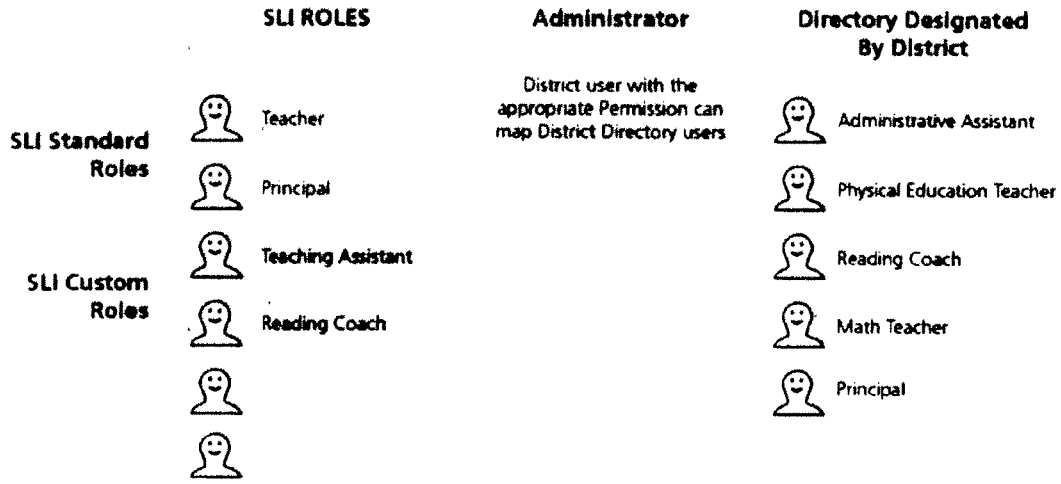

Figure 5 – Example of Mapping an External Directory

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.

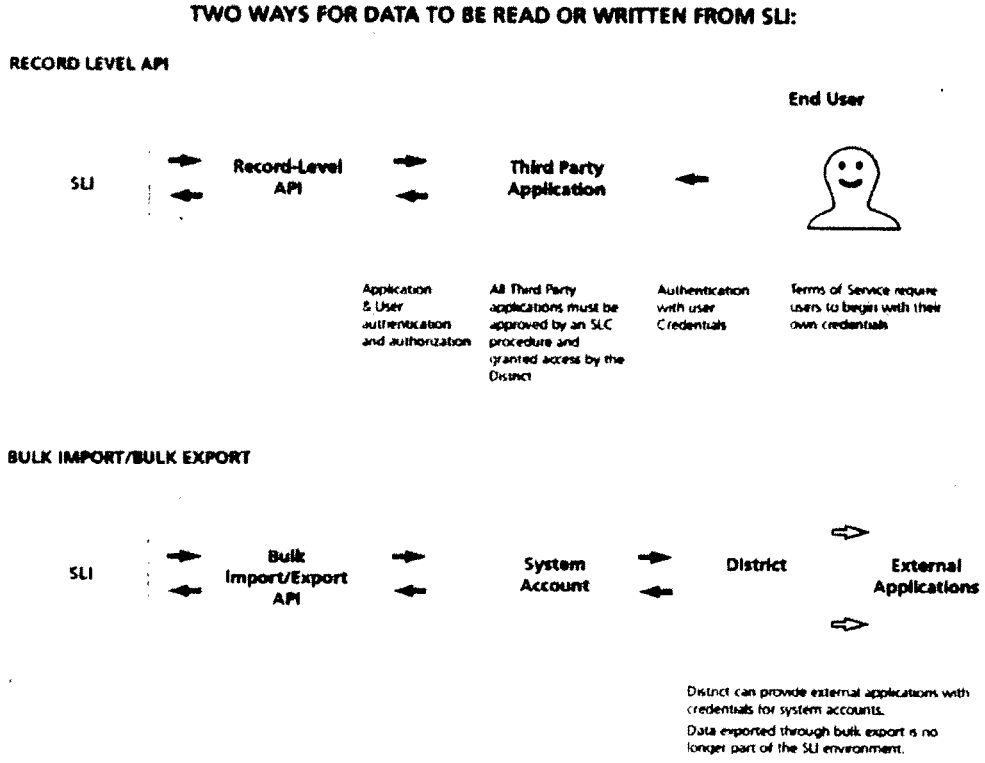

Figure 6 - Two Ways for Data to be Read or Written

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:

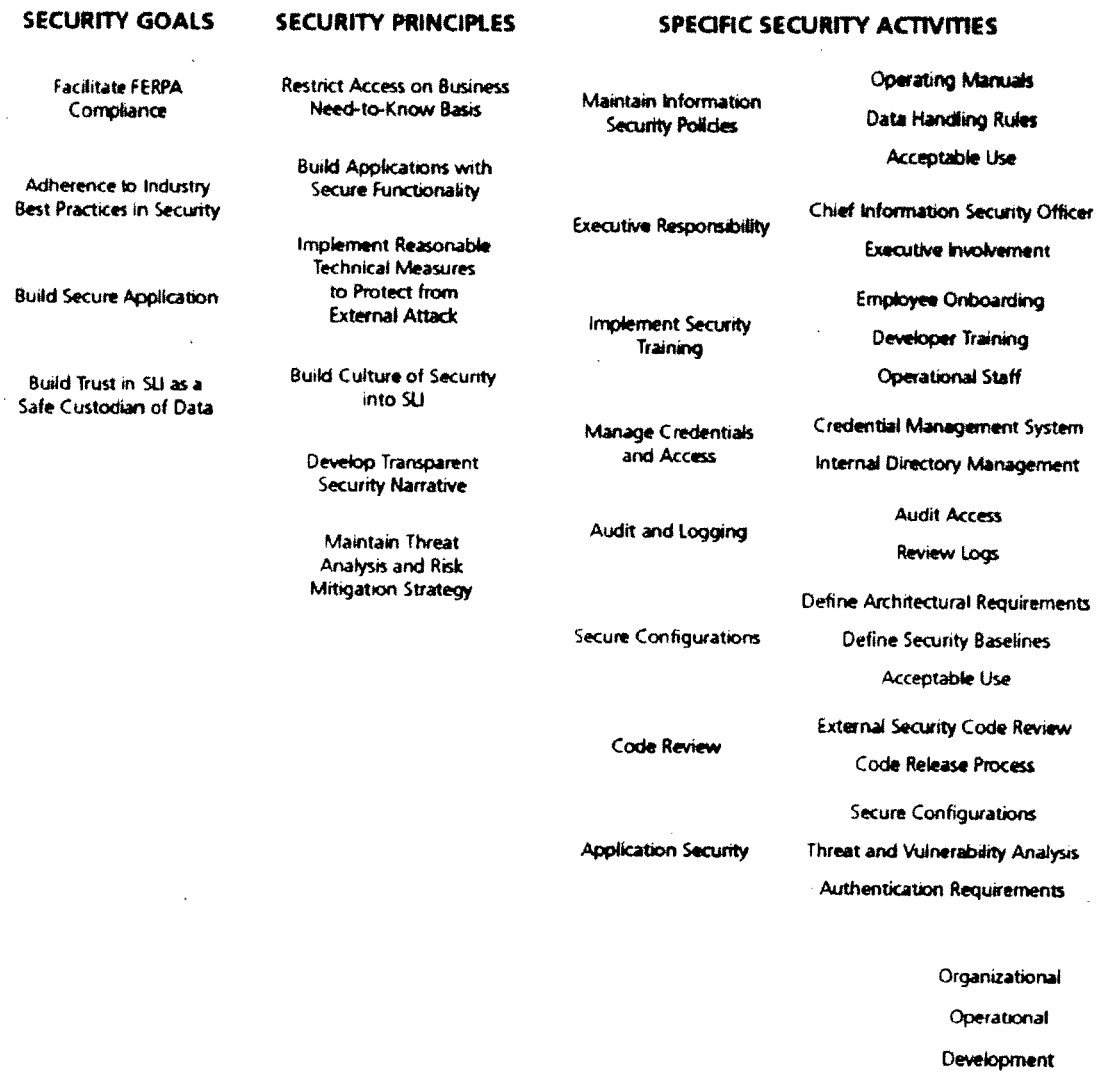

Figure 7 - Information Security Approach

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
A. Restrictions and authentication processes limiting access to Student PII only to: a. the School District that provided the data and to other recipients authorized by the School District; and b. employees of the host of SLI and to other recipients based on pre-defined roles.	a. Role-based solution that will use user identity data and enrollment data to provide access only to users authorized by the District. b. Documented processes for restricting and recording any necessary access by Wireless Generation.
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;	For v.1, the only access the SLI provides to third-party users is through applications approved by School Districts. 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. 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.
C. Electronic acceptance by participating School Districts of terms of use agreements required for participation in SLI;	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.
D. Electronic agreements between participating School Districts and organizations conducting research for or on behalf of the School Districts; and	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. 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
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.	Districts will be able to stop sending data or request destruction or return of data at any time.

ATTACHMENT G

Super Administrator(s)

Ken Wagner

ATTACHMENT H

Additional Terms Applicable to Customer

Service Provider and Customer agree to the following additional terms:

1. **Cloud Hosting Region; Cloud Hosting Warranty**

1.1 Customer Data shall be hosted within the continental United States.

1.2 In addition to the warranties provided in Section 11.1 of Attachment A, effective September 2013, Service Provider warrants that the SLI Service will comply with the Federal Risk and Authorization Management Program ("FedRAMP") requirements applicable to cloud service providers as developed by the Federal Cloud Computing Initiative at the US General Services Administration, or such other standard as mutually agreed in writing by Service Provider and Customer.