Access 4 Learning Community

Powered by: SIF

Simple. Secure. Scalable. Standard.

Data Privacy Task Force Artifacts

www.A4L.org

March 2015 – Volume 1, version 1.1

Table of Contents

About the Task Force

Threats to student data privacy have received considerable attention recently, and it is generally recognized that while data security and data privacy issues overlap to some degree, there are enough differences that data privacy concerns can effectively be treated separately.

Educational solutions at the school and district levels are increasingly deployed in the cloud, and that introduces a set of new concerns about who might be granted (or otherwise obtain) access to student health records, discipline actions or other identification (ex: name, address and phone) information. Conversely, there is potential data available in these applications including performance, student developed content, etc. that would be valuable to collect as part of a larger portfolio for the learner.

The *Access 4 Learning Community* is a unique blend of schools, regional support entities, government agencies, and vendors coming together to discuss and develop technical "blueprints" for marketplace solutions to better enable management and usage of educational data. At the 2014 Community Annual Meeting at a session called "Who owns the data?", there was a consensus of attendees to form a Work Group focused exclusively on privacy issues surrounding access to and use of sensitive student related data.

The *Student Privacy Task Force* concentrates on end user issues (i.e. educational agency) relating to ensuring data privacy primarily for student data, but encompassing staff and possibly parental data privacy as well. In this first volume, the volunteer group has created:

- **Student Data Classifications:** Various data points carry with them various levels of privacy concerns. The Task Force has collected the most common student data points and proposed levels of data privacy sensitivity. Since this group is international in representation, the areas of classification include those utilized in North America, Australia and the United Kingdom.
- **Data Privacy Use Cases:** Many times the security of a particular data point is contingent on the context in how it is being utilized. Presented is a collectively developed template for Use Case development and examples of its usage in various real-world data privacy scenarios.
- **Administrative Data Privacy "Best Practices":** The Task Force is also focused on providing actionable guidance to allow end users to implement strategies and practices to effectively manage their data demands. In this first volume, the group presents a *"Data*

Breach Template" to be used by end users with their vendors ideally to provide clarity around roles and responsibilities if a breach occurs.

The group has already begun the planning for additional Artifacts versions which may include:

- ✓ *Data Privacy Profiles* corresponding to one or more use cases identifying a unique collection of data elements to be including and excluded in objects conforming to that profile.
- ✓ *Data Privacy Profile Verification* for marketplace solutions to specify exactly how compliant solutions can be administrated to enforce selected Object Data Privacy Profiles in a real world solution.
- ✓ *Checklist of Data Privacy Recommendations* to address the privacy policies of Cloud Service providers and enable education agencies to meet or exceed federal and local data privacy mandates.

The Task Force is not interested in "re-inventing the wheel". Numerous organizations have provided outstanding data privacy policy, tools, guidance, etc. and this group will continue to identify and partner with those organizations to support the complicated data privacy landscape.

I. Student Data Areas and Sensitivity Levels

Data sensitivity levels seek to provide an easily recognizable and understood privacy label for data to both highlight those uses that may require extra attention, but to also alleviate fears that more sensitive data is being shared. It is expected that the use of sensitivity levels will serve as a tool for schools, government jurisdictions, vendors, educators, students and parents to readily ascertain which use cases have data exchanges with a 'low' privacy sensitivity and which have an 'extreme' privacy sensitivity. For example, compromising information in a student's "core identity" is probably more serious than compromising that same student's "learning profile".

As a result, the following "Sensitivity Levels" are proposed, the last three of which could be applied to the named areas within Student Data.

Data Privacy Sensitivity Level	Meaning	U.S. Government Equivalent
Low	Confidentiality of information should not be assumed by data owner (i.e. in public domain)	Public
Medium	Unauthorized access may result in potential (non-physical) harm to student	Sensitive
High	May involve legal liability if compromised by the data steward	Confidential
Extreme	Privacy requirements may be specifically protected by law	Confidential requiring special handling

The "Extreme" (special handling) level might be applicable only to a set of specific elements typically National IDs, Social Security numbers and possibly credit card information. If any of these elements are included in a data exchange, the entire exchange should be flagged as having an Extreme Data Privacy sensitivity level.

Currently data privacy constraints typically operate at the level of "no student data may be shared with application X". This is too broad and needs finer granularity. The "Student Data Areas" (Health Care, Discipline, Identity, etc.) presented here allow this to be narrowed further to address "…no student core identification data elements (address, phone #, name, etc.) may be shared with application X". Also provided is a brief description and types of objects and to address that Student Data Area.

Student Data Area	US Sensitivity Level	AU Sensitivity Level	UK Sensitivity Level	Brief Description	Types of Objects
Student Retrieval	Depends upon other data	Medium	Depends upon other data – Medium	Identifies a student record.	State Surrogate ID, RefId, District Student ID
Student Other	Low	Low	Low	Elements that do not fit into one of the other Areas	Library Card #, Assigned School Bus route, Student Promotion Info, Projected Year Graduation
Imagery	Low	Medium	Medium	Student/other profile photos, student activity photos	PersonPicture
Student Demographics (relatively static)	Low	Medium	Low	Qualifiers on student used to place them in groups with "similar" students	Race, Gender, Nationality, languages spoken, ESL, socio-economic, family "types"
Student Learning Profile	Low	Low	Low	Learning Management System - type generic information	Learning preferences, motivations, "type" of learner
Special Programs	Medium	Medium	Medium	Qualifiers on student used to identify them for special programs	Free or reduced price lunch, Special Ed
Student Achievement	Medium	Medium	Low	Transcript information	Details of performance on assessment tasks including awards
Student Assignments	Medium	Low	Low	Classwork or programs	Assignment and due dates, grades, competency marking
Student Categorization Indicators (variable)	Medium	High	Medium	May be based upon details that are hidden from applications accessing "indicators"	Risks: Bullying, suicide, attendance problems, dropout, Gifted and Talented
Schedule / Timetable	Medium	Low	Medium	Current schedule of classes	Timetable information including structure and class lists, calendars
Student Attendance	Medium	Extreme	Medium	Attendance in current classes and / or current year	Attendance details including present/absent, time of arrival/ departure, reason codes and notes
Student Finance	Medium	Medium	Medium	Details of student financial transactions	Outstanding or paid invoices, receipts, credit notes, scholarships and subsidies
Student Discipline	High	High	High	Detail of discipline incidents including follow-up actions	Date, times, locations, and types of Discipline incidents

Student Healthcare	High	Extreme	High	Details regarding a student's current or pre-existing conditions including medication	Inoculations, allergies, medical incidents (accidents, seizures)
Core Student Identity	High If SS# used Extreme	Extreme	Extreme	The basic set of elements from which a Student can be identified	Name, Facebook & other web accounts, SS#
Student Contact	High	Extreme	High	Usually detached from other student data. Typical use: emergency situation	Address(es), Phone #(s), Email Address(es), Parents or Guardian info
Other Areas				**Brief description**	**SIF Objects / Elements**
School Setup	Low	Low	Low	Details of rooms, term information	RoomInfo, TermInfo
Staff Teaching Areas	Low	Low	Low	The allocation of staff to a school/subject matter	StaffAssignment
Staff Contact Details	High	Extreme	High	Any contact information on staff member	Address, phone, email information
Core Staff Identity	High. If SS# present, Extreme	Extreme	Extreme	The basic identifying features of a staff member	StaffPersonal
Core Parent / Guardian Identity	High. If SS# present, Extreme	Extreme	Extreme	The basic identifying features of a parent or guardian	StudentContactPersonal, StudentContactRelationship
Staff Credentials	High	High	High	Level of education, degree areas, certification areas	Degree, certifications, providing institutions, year provided

II. Student Data Privacy Use Case Template

A valuable set of questions for any conversation around student data privacy and the issues that surround its identification, management, sharing and usage are not new – Who, What, Where, How and Why. To collect information to answer these questions, conversations tend to focus on the "Use Cases" around the identified data. In the technical world, "Use Cases" outline the interactions between roles and a system to reach a goal.

For Task Forcer usage, a Student Data Privacy Use Case defines "who" is and/or is not authorized to query and/or update a specific area of student data, and why. A template for defining these use cases is presented here:

Aspect	Sample Value(s)
Name	• *Work Study Access* • *Health Provider Access and Update*
Type	• *Per program* • *Per cloud service product* • *Per external organization*
Assigned Data Steward	• *School* • *District/ Local Authority* • *State / Territory / Province*
Data Sensitivity *(How sensitive is the most sensitive data involved in this use case)*	• *Extreme (Requires special handling)* • *High (Confidential)* • *Medium (Sensitive)* • *Low (Public)*
Actors (what applications / users / groups would exchange the data) Application Types (IDM, LMS, SIS) User Types (Superintendent, Teacher, Parent) System Types (local IT Data Center, local Cloud, Vendor Cloud, foreign hosted Vendor Cloud)	• *External Work Study Apps (UK use case)* • *Federal Program (ex: Free School Lunch)* • *State level Data Warehouse / SLDS* • *District Data Warehouse Cloud Service* • *Identity management Applications in other districts* • *Learning Management application in this district*
Data (what area(s) of education-related data are of concern in this Privacy Use case) and what is the scope (School, District, State, all or subset)	• *Student Health Care* • *Student Identification Information* • *Student Discipline* • *Student Transcript* • *Student Schedule*

	• *Student Demographics (race, gender, etc.)* • *Student General Info*
Access (Query, Create, Change, Delete)	*The typical limitation is that no data changes are allowed and only certain elements will be returned on a successful query. However other alternatives are possible:* • *Food Service System can retrieve only student ID information, but can update "Free Lunch" indicator.* • *Application cannot update attendance elements but can set "At Risk" indicator.*
Intent (why is information being shared)?	*State needs student information to support data analytics…*
Concerns Addressed (why is some subset of that information being restricted)?	*District Data Steward responsibilities require maintaining student anonymity outside the organizational boundaries of the District.*
Restrictions: These restrictions (some of which may be introduced by existing policies and legislation) could apply to: Who has physical possession of the data? How is it protected (ex: encryption)? Who can access it? For how long? Who can aggregate it? Who can change it? Who can give others access to it? Who enforces these rules?	*State level applications should not be allowed to update any District level student data elements unless specifically enabled.* *State level applications should not be allowed access to any information that would enable them to identify an individual student and associate that student with specific records in the detailed data they contain.*

(A) Data Sharing Use Case - U.S. State Longitudinal Data System Example

Better decisions require better information. This principle lies at the heart of the U.S. Federal Statewide Longitudinal Data Systems (SLDS) Grant Program. Through grants and a growing range of services and resources, the program has helped propel the successful design, development, implementation, and expansion of K12 and P-20W (early learning through the workforce) longitudinal data systems (US Department of Education).

Aspect	Sample Value(s)
Name	*State level SLDS and District Student Data*
Assigned Data Steward	*District*
Actors (what applications / users / groups would exchange the data)	• *State level Data Warehouse / SLDS* • *District SIS* • Application Type (IDM, LMS, SIS) • User Type (Superintendent, Teacher, Parent) • System Type (local IT Data Center, local Cloud, Vendor Cloud)
Data (what area(s) of education-related data are of concern in this Privacy Use case)	• *Student Identification Information* • *Attendance* • *Discipline* • *Performance* • *Program Participation* • *Assessment*
Intent (why is information being shared)?	*State needs student information to support data analytics.*
Concerns Addressed (why is some subset of that information being restricted)?	*District Data Steward responsibilities require maintaining student anonymity outside the organizational boundaries of the District.*
Restrictions (what data areas should identified actors be restricted on, as to access or update). These restrictions could apply to: • Who has physical possession of the data? • Who can access it? • Who can aggregate it? • Who can change it? • Who can give others access to it? • Who enforces these rules?	*State level applications should not be allowed to update any District level student data elements unless specifically enabled.* *State level applications should not be allowed access to any information that would enable them to identify an individual student and associate that student with specific records in the detailed data they contain.*

(B) Data Sharing Use Case: UK Social Care/ Looked After Children (LAC)

The term "Children Looked After" has a specific legal meaning based on the UK Children Act. A child is looked after by a local authority if he or she has been provided with accommodation for a continuous period of more than 24 hours or is placed in the care of a local authority by virtue of an order made under the Act. The majority of children who are looked after by the local authority are placed with foster care providers but for some children, residential care may be more appropriate

Aspect	Sample Value(s)
Name	• *LAC (Looked After Children)*
Type	• *Per Local Authority*
Assigned Data Steward	• *Local Authority*
Data Sensitivity (How sensitive is the most sensitive data involved in this use case)	• *Extreme (Requires special handling)*
Actors (what applications / users / groups would exchange the data)	• Applications: Schools MIS, LA MIS. • Users: Social Workers (LA), Senior LA Staff, School Head Teachers. • Systems: School Servers (Local/Cloud), LA Servers (Local/Cloud). • Application Types (IDM, LMS, SIS) • User Types (Superintendent, Teacher, Parent) • System Types (local IT Data Center, local Cloud, Vendor Cloud, foreign hosted Vendor Cloud)
Data (what area(s) of education-related data are of concern in this Privacy Use case) and what is the scope (School, District, State, all or subset)	• *Student Health Care* • *Student Identification Information* • *Student Discipline* • *Student Attendance* • *Student Schedule* • *Student Demographics (race, gender, …)* • *Student General Info* • *Student Contact Info* • *Student Categorizations* • *Student Imagery* • *Student Achievement*
Access (Query, Create, Change, Delete)	• *Query only from School MIS.*

Intent (why is information being shared)?	*To have all up-to-date and relevant information about a student, their current situation in school and any information known about the student from the school.*
Concerns Addressed (why is some subset of that information being restricted)?	*Only relevant/required information is passed to the LA, however this covers most information needed, rather than being restricted to a subset.*
Restrictions (what data areas should identified actors be restricted on, as to access or update)? These restrictions (some of which may be introduced by existing policies and legislation) could apply to: • Who has physical possession of the data? • How is it protected (ex: encryption)? • Who can access it? For how long? • Who can aggregate it? • Who can change it? • Who can give others access to it? • Who enforces these rules?	*Limited staff within the LA can access all the information, particularly information regarding social care (added post extraction usually). Those staff have full access to read, change and modify information within local LA system, no information is written back to school directly. Rules are enforced by LA, and follow national laws on social care responsibilities and data protection, and child protection.*

(C) Data Sharing Use Case - U.S. Free and Reduced Lunch Example

The U.S. National School Lunch Program is a federally assisted meal program operating in public and nonprofit private schools and residential child care institutions. It provides nutritionally balanced, low-cost or free lunches to children each school day. The program was established under the National School Lunch Act, signed by President Harry Truman in 1946 (US Department of Agriculture).

Aspect	Sample Value(s)
Type	*Internal to District*
Assigned Data Steward	*District*
Data Sensitivity (How sensitive is the most sensitive data involved in this use case)	*High (Confidential)*
Actors (what applications / users / groups would exchange the data)	• *Student Information System (recipient)* • *Food Service System (provider)*
Data (what area(s) of education-related data are of concern in this Data Sharing Use case)	• *Core Student Identity* • *Demographics (race, gender, etc.)* • *Student General Info* • *Free and Reduced Lunch Data*
Access (Query, Create, Change, Delete)	*Food Service System can retrieve only student ID information, but can update "Free Lunch" indicator in Student Information System.*
Intent (why is information being shared)?	*District and State needs student free and reduced lunch information to support data analytics required by Federal Programs.*
Concerns Addressed (why is some subset of that information being restricted)?	*District Data Steward responsibilities require maintaining student anonymity outside the organizational boundaries of the District. Not all District staff should have access to information.*
Restrictions (what data areas should identified actors be restricted on, as to access or update)? These restrictions (some of which may be introduced by existing policies and legislation) could apply to:	*State level applications should not be allowed to update any District level student data elements unless specifically enabled.* *State level applications should not be allowed access to any information that would enable them to identify an*

• Who has physical possession of the data? • How is it protected (ex: encryption)? • Who can access it? For how long? • Who can aggregate it? • Who can change it? • Who can give others access to it? • Who enforces these rules?	*individual student and determine whether that student obtains free or reduced student lunch.*

III. Student Data Privacy Stewardship and Data Breach Example

Local education organizations (or their equivalents) act as the data "steward" for all information relating to one or more of the schools / institutions under its jurisdiction. Different types of information may have different ownership restrictions (ex: a staff member may own some of the information concerning their personal assessment and attendance records, but as an employee, may have a different set of ownership rights than a student or parent over that data). There may be more than one data steward for a given student (ex: a student has attended schools in multiple districts). Each has an equivalent responsibility to the owner for the data under its control.

The Data Steward's role is to:

- Ensure data security: Data is secure only when it inaccessible to unauthorized 3rd parties. Only secure data can be made private.
- Ensure Data Privacy: Secure data is private only when its access and use by authorized 3rd parties is restricted and fully controlled by the Data Steward, in accordance with (where possible) the stated wishes of the Data Owner.

Steward and Supplier Interrelationship

The assumption is made that the marketplace suppliers (vendors, providers, corporations, etc.) are treated as using the information to provide a service for the Data Steward (usually the school). In this case the Steward maintains control over who can view the information it supplies, and for what purposes.

The definition of "control" varies but might include some or all of the following use cases:

- The Data Steward gives the personal information to the supplier to use for a limited purpose that assists or benefits the Data Owner;
- An agreement between the Data Steward and the supplier binds the supplier not to use or disclose any personal information except for the specified limited purpose. If any data is exposed to its sub-contractors, at a minimum these sub-contractors must also agree to the same obligations, and be specified by name in any contracts or agreements with the Data Steward.
- An agreement between the Data Steward and the supplier gives the Steward the right to be notified of and pre-approve any additional 3rd party accessing the data, or

alternatively a reasonable opportunity to retrieve all information and request it be scrubbed from supplier storage.

10 General Data Privacy RFP Considerations (modified from Fordham)

1. Reserve the right to audit and inspect supplier compliance to stated Data Privacy requirements
2. Restrict suppliers unilaterally amending the agreed upon Data Privacy Policies without sufficient notice and without right to refuse.
3. Specify whether or not (and if so how) students / parents can access their own data.
4. Ensure that the Data Steward retains exclusive control over who can access and mine any "identifiable" student data
5. Specify the types of data transferred or collected (i.e. from previously mentioned areas and sensitivity levels), mode of transfer and implications of transferring data with these sensitivities.
6. Prohibit or limit the sale or marketing of student information without express parental consent
7. Include explicit prohibition or limitations (such as right of refusal) on re-disclosure / transfer of entrusted data to other business areas, companies or trusts related to the primary contracted business entity (where intended use should be disclosed during procurement):
8. Specify "conditions of storage" (location, encryption, backups, destruction, etc.) and require specific procedures to ensure alternative data storage services can be found, data can be re-hosted, and all sensitive data will and can be deleted upon contract termination.
9. Specify data security requirements, and notification responsibilities if a data breach occurs
10. In case of bankruptcy or vendor acquisition, ensure access is available to data for a limited time after notice of bankruptcy, and/or ESCROW provision must be made to continue service

STUDENT DATA/DATA BREACH SPECIAL TERMS AND CONDITIONS - US Version

Breach Agreement provided and edited from Cambridge Public Schools.

This Student Data/Data Breach Special Terms and Conditions dated _____ (hereinafter "Agreement") is by and between XXX Schools ("XXX") and _____ ("Contractor"), a contractor performing institutional services and functions that will require student data to perform those services and functions.

1. Contractor and XXX have contracted for the Contractor to provide _____ ("the Services"), which are institutional services and functions, to XXX. In the course of performing the Services, Contractor will obtain confidential student records and/or confidential student record information that contain personally identifiable student records, data and/or information ("Data Files"). XXX and Contractor acknowledge and agree that this Agreement is for the purpose of sharing Data Files between the parties in a manner consistent with the Family Education Records Privacy Act of 1974 ("FERPA") and XXXXX student record regulations, XXX ("State Regulations"). The Data Files will be used by the Contractor's employees to populate student data for the purpose of delivering these Services. Contractor further acknowledges and agrees that all copies of such Data Files, including any modifications or additions to data from any source that contains personally identifiable information regarding individual students, are subject to the provisions of this Agreement in the same manner as the original Data Files. The ability to access or maintain Data Files and/or any personally identifiable student data contained therein under this Agreement shall not under any circumstances transfer from Contractor to any other party.
2. Contractor acknowledges and agrees that it is providing institutional services or functions for XXX and that it is under direct control of XXX with respect to the use and maintenance of Data Files in connection with these Services. Contractor additionally acknowledges and agrees that at no point in time is the Contractor the owner of the Data Files. Ownership rights are maintained by XXX and XXX reserves the right to request the prompt return of any portion of the Data Files and/or all Data Files at any time for any reason whatsoever. Contractor further acknowledges and agrees that it shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of the Data Files, including without limitation, any student data and/or personally identifiable information contained within the

Data Files. Contractor also acknowledges and agrees that it shall not make any re-disclosure of any Data Files, including without limitation, any student data and/or personally identifiable information contained in the Data Files, without the express written consent of XXX. Additionally, Contractor agrees that only authorized employees of the Contractor directly involved in delivering the Services shall have access to the Data Files and that it and its employees shall protect the confidentiality of the Data Files in such a way that parties other than officials of XXX and their authorized agents cannot identify any students.

3. Contractor also acknowledges and agrees to:

   (i) use personally identifiable student data shared under this Agreement for no purpose other than in connection with and through the provision of the Services.

   (ii) use reasonable methods, consistent with industry standards, to protect the Data Files and/or any personally identifiable student data contained therein from re-disclosure, and to not share the Data Files and/or any personally identifiable student data received under this Agreement with any other entity without prior written approval from XXX.

   (iii) not copy, reproduce or transmit the Data Files and/or any personally identifiable student data contained therein, except as necessary to fulfill the Services.

   (iv) notify the Chief Information Officer for XXX in writing within three (3) days of its determination that it has experienced a data breach, breach of security or unauthorized acquisition or use of any Data Files and/or personally identifiable student data contained therein. Contractor agrees that said notification shall include, to the extent feasible, the date or approximate dates of such incident and the nature thereof, the specific scope of said breach (i.e., what data was accessed, used, released or otherwise breached, including the names of individual students that were affected by said breach) and what actions or steps with respect to the incident that Contractor plans to take or has taken in response to said breach.

   (v) not provide any Data Files or any personally identifiable data contained therein to any party ineligible to receive student records and/or student record data and information protected by FERPA and State Regulations or prohibited from receiving personally identifiable from any entity under 34 CFR 99.31(a)(6)(iii).

   (vi) to maintain backup copies, backed up at least daily, of Data Files in case of Contractor system failure or any other unforeseen event resulting in loss of Data Files.

   (vii) to, upon receipt of a request from XXX, immediately provide XXX with any specified portion of the Data Files within three (3) days of receipt of said request

(viii) to, upon receipt of a request from XXX, immediately begin the process of returning all Data Files over to XXX and subsequently erasing and/or otherwise destroying any Data Files, be it digital or physical form, still in Contractor's possession such that Contractor is no longer in possession of any student work belonging to XXX and to provide XXX with any and all Data Files in Contractor's possession, custody or control within seven (7) days of receipt of said request.

(ix) to, in the event of the Contractor's cessation of operations, promptly return all Data Files to XXX in an organized, manageable manner and subsequently erasing and/or otherwise destroying any Data Files, be it digital or physical form, still in Contractor's possession such that Contractor is no longer in possession of any student work belonging to XXX.

(x) to delete XXX Data Files that it collects or receives under this Agreement once the Services referenced in this Agreement lapses.

(xi) to, upon receipt of a litigation hold request from XXX, immediately implement a litigation hold and preserve all documents and data relevant identified by XXX and suspend deletion, overwriting, or any other possible destruction of documentation and data identified in, related to, arising out of and/or relevant to the litigation hold.

4. Contractor certifies under the penalties of perjury that it complies with all federal and state laws, regulations and rules as such laws may apply to the receipt, storing, maintenance or access to personal information, including without limitation, all standards for the protection of personal information of residents of XXX and maintaining safeguards for personal information. Contractor hereby further certifies under penalties of perjury that it has a written comprehensive information security program that is in compliance with the provisions of 201 C.M.R. 17.00 *et seq*. Further, the Contractor hereby certifies under the penalties of perjury that it shall fully comply with the provisions of the federal Family Educational Rights Privacy Act, 20 U.S.C. §1232g and regulations promulgated thereunder and XXXX student records law and regulations, including without limitation., and to fully protect the confidentiality of any student data and/or personally identifiable information provided to it or its representatives. Contractor further represents and warrants that it has reviewed and complied with all information security programs, plans, guidelines, standards and policies that apply to the work it will be performing, that it will communicate these provisions to and enforce them against its subcontractors and will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information and/or student record information from unauthorized access, destruction, use, modification, disclosure or loss. Contractor also represents and warrants that if personal information and/or student record information is to be stored on a laptop or

other mobile electronic device, that such electronic devices are encrypted and that all such devices will be scanned at the completion of any contract or service agreement and/or research study or project to ensure that no personal information and/or student record information is stored on such electronic devices. Furthermore, Contractor represents and warrants that it has in place a service that will allow it to wipe the hard drive on any stolen laptop or mobile electronic device remotely and have purchased locks for all laptops and mobile electronic devices and have a protocol in place to ensure use by employees.

5. Contractor represents, warrants and agrees that its terms of service/terms and conditions of use and/or privacy policies dated _____shall be amended as it relates to the Services as follows:

   (i) Any indemnification provision contained in the Contractor's terms of service, terms and conditions of use and/or privacy policies are hereby deleted in their entirety.

   (ii) Any provision in the Contractor's terms of service, terms and conditions of use and/or privacy policies that require that the City and/or XXX, as a user, to carry insurance coverage are hereby deleted in their entirety.

   (iii) Any provision in the Contractor's terms of service, terms and conditions of use and/or privacy policies which specifically disclaim all implied warranties or merchantability, non-infringement and fitness for a particular purpose, the implied conditions of satisfactory quality and acceptance as well as any local jurisdictional analogues to the above and other implied or statutory warranties are hereby deleted in its entirety.

   (iv) Any provision in the Contractor's terms of service, terms and conditions of use and/or privacy policies by which the City and/or XXX is specifically releasing the Contractor from liability are hereby deleted in their entirety.

   (v) Any changes that the Contractor may make, from time to time, to its terms of service, terms and conditions of use and/or privacy policies, shall not apply to the terms of these Services unless the Contractor and City and/or XXX agree to such changes in writing.

6. Contractor represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Data Files and any personally identifiable student data contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data Files and/or any personally identifiable student data contained therein, or may own, lease or control equipment or facilities of any kind where the Data Files and any personally identifiable student data contained therein is stored, maintained or used in any way.

IN WITNESS WHEREOF, and in consideration of the mutual covenants set forth herein and for other good and valuable consideration, and intending to be legally bound, each party has caused this Agreement to be duly executed as a XXXX [State] instrument under seal as of the day and year first written above.

INSERT NAME OF CONTRACTOR	XXX SCHOOL
_____	_____
Name XXX	Name XXX
Title	Superintendent of Schools

DATA BREACH AND STUDENT RECORD CERTIFICATION

The Contractor hereby certifies under the penalties of perjury that it complies with all state laws, regulations and rules as such laws may apply to the receipt, storing, maintenance or access to personal information about residents of XXX, including without limitation, all standards for the protection of personal information of residents of XXX and maintaining safeguards for personal information. Contractor hereby further certifies under penalties of perjury that it has a written comprehensive information security program that is in compliance with the provisions of XXX. Further, the Contractor hereby certifies under the penalties of perjury that it shall fully comply with the provisions of the federal Family Educational Rights Privacy Act, 20 U.S.C. §1232g and regulations promulgated thereunder and XXX student record s law and regulations, and to fully protect the confidentiality of any student data and/or personally identifiable information provided to it or its representatives. The Contractor additionally acknowledges that it is under the direct control of the XXX Schools with respect to the use and maintenance of all education records and shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of student data and/or personally identifiable information and shall not make any re-disclosure of any student data and/or personally identifiable information without the express written consent of the XXX Schools.

Signed at _____ this _____day of _____20___ by the duly authorized representative of the Contractor.

Name _____

Title _____

Contractor _____

DATA BREACH CERTIFICATION

The Contractor hereby certifies under the penalties of perjury that it complies with all state laws, regulations and rules as such laws may apply to the receipt, storing, maintenance or access to personal information about residents of XXX, including without limitation, all standards for the protection of personal information and maintaining safeguards for personal information. Contractor hereby further certifies under penalties of perjury that it has a written comprehensive information security program that is in compliance with the provisions of XXX. Ownership rights are maintained by XXX in any data XXX has stored with Contractor (hereinafter "Data Files") and XXX reserves the right to request the prompt return of any portion of the Data Files and/or all Data Files at any time for any reason whatsoever. Contractor further acknowledges and agrees that it shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of the Data Files, including without limitation, any personnel record data, health record data and/or personally identifiable information contained within the Data Files. Contractor also acknowledges and agrees that it shall not make any re-disclosure of any Data Files, including without limitation, any personnel record data, health record data and/or personally identifiable information contained in the Data Files, without the express written consent of XXX. Additionally, Contractor agrees that only authorized employees of the Contractor directly involved in delivering the Services shall have access to the Data Files and that it and its employees shall protect the confidentiality of the Data Files in such a way that parties other than officials of XXX and their authorized agents cannot identify any individuals (whether students or employees).

Contractor also acknowledges and agrees to:

(i) use Data Files for no purpose other than in connection with and through the provision of its service to XXX.

(ii) use reasonable methods, consistent with industry standards, to protect the Data Files and/or any personally identifiable data, personnel record data and/or health record data contained therein from re-disclosure, and to not share the Data Files and/or any personally identifiable data, personnel record data and/or health record data received from XXX with any other entity without prior written approval from XXX.

(iii) not copy, reproduce or transmit the Data Files and/or any personally identifiable data, personnel record data and/or health record data contained therein ,except as necessary to fulfill its services to XXX.

(iv) notify the Chief Information Officer for XXX in writing within three (3) days of its determination that it has experienced a data breach, breach of security or unauthorized acquisition or use of any Data Files and/or any personally identifiable data, personnel record data and/or health record data contained therein. Contractor agrees that said notification shall include, to the extent feasible, the date or approximate dates of such incident and the nature thereof, the specific scope of said breach (i.e., what data was accessed, used, released or otherwise breached, including the names of individual students that were affected by said breach) and what actions or steps with respect to the incident that Contractor plans to take or has taken in response to said breach.

(v) to maintain backup copies, backed up at least daily, of Data Files in case of Contractor system failure or any other unforeseen event resulting in loss of Data Files.

(vi) to, upon receipt of a request from XXX, immediately provide XXX with any specified portion of the Data Files within three (3) days of receipt of said request.

(vii) to, upon receipt of a request from XXX immediately begin the process of returning all Data Files over to XXX and subsequently erasing and/or otherwise destroying any Data Files, be it digital or physical form, still in Contractor's possession such that Contractor is no longer in possession of any Data Files belonging to XXX and to provide XXX with any and all Data Files in Contractor's possession, custody or control within seven (7) days of receipt of said request.

(viii) to, in the event of the Contractor's cessation of operations, promptly return all Data Files to XXX in an organized, manageable manner and subsequently erasing and/or otherwise destroying any Data Files, be it digital or physical form, still in Contractor's possession such that Contractor is no longer in possession of any Data Files belonging to XXX.

(ix) to delete XXX Data Files that it collects or receives once its contractual relationship with XXX has ended.

(x) to, upon receipt of a litigation hold request from XXX, immediately implement a litigation hold and preserve all documents and data relevant identified by XXX and suspend deletion, overwriting, or any other possible destruction of documentation and data identified in, related to, arising out of and/or relevant to the litigation hold.

Further, the Contractor hereby certifies under the penalties of perjury that it shall fully comply with the provisions of the federal and state laws regarding the protection of the confidentiality of any personally identifiable information, including without limitation, personnel record data and/or health record data, provided to it or its representatives. The Contractor additionally

acknowledges that it shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of personally identifiable information and shall not make any of any such personally identifiable information without the express written consent of the XXX Schools.

Signed at _____ this _____day of _____ 20___ by the duly authorized representative of the Contractor.

Name _____

Title _____

Contractor _____

IV. Data Privacy FAQ

1. What are the recognized "types" of Student information

- **Education Records (from U.S. FERPA)**

  Materials that are "maintained by an educational agency or institution or by a person acting for such an agency or institution," and contain information directly related to a student.

- **De-Identified Data (from U.S. FERPA):**

  The School System has removed all personally identifiable information and there is a reasonable determination that the student is not identifiable.

- **Personal Information (from CoSN – extends U.S. FERPA PII)**

  Name, home address, email address, telephone number, social security number, photo, video, audio files containing child's voice, geo-location information, persistent identifier that can be used to recognize use over time and across different websites, and any other information that permits physical or online contact of a specific individual.

2. What are the subareas of Educational Records that might be utilized in defining and enforcing a Data Privacy Policy for identifiable students?

The complete list depends upon the Student Data Model. It is an area currently under discussion, and includes:

- Aggregates (Gender, ethnicity, etc.)
- Academic Transcript (courses taken)
- Attendance
- Grades and class ranking
- Assessment
- Health
- Discipline
- Current Schedule of classes
- Program Participation
- Program Eligibility

3. Who is the Data Owner?

- The students and their parents/guardians are the ultimate "owners" of Student-related data.

- The Data Owner, subject to legal constraints (approved State policies, court orders, federal reporting, etc.), is the default arbitrator of who gets to create, update and delete information in educational record "subareas" for an identified student, and who gets to access that information.
- Parents/guardians should be informed that they are the data owners and can exercise the associated rights.

4. Who are the Data Stewards?

- The local School District, Local Authority, or equivalent)acts as the data "steward" for all information relating to one or more of the schools / institutions under its jurisdiction.
- Different types of information may have different ownership restrictions (ex: a staff member may own some of the information concerning their personal assessment and attendance records, but as an employee, may have a different set of ownership rights than a student or parent over that data).
- There may be more than one data steward for a given student (ex: a student has attended schools in multiple districts). Each has an equivalent responsibility to the owner for the data under its control.

5. What are the set of responsibilities of a Data Steward?

- **Ensure Data Security**
    - Data is secure only when it inaccessible to unauthorized 3rd parties. Only secure data can be made private.
- **Ensure Data Privacy**
    - Secure data is private only when its access and use by authorized 3rd parties is restricted and fully controlled by the Data Steward, in accordance with (where possible) the stated wishes of the Data Owner.
- **Ensure Data Accuracy**
    - Data not only needs to be secure but of high quality for its effective management and ultimately usage. The Data Steward must play the role,

via effective policies and procedures, that quality checks occur with the various data owners.

6. How exactly does a Data Steward ensure data privacy?

- **Create and maintain** a comprehensive data privacy "policy" which specifies which external organizations get access to which part of the data it is entrusted with. Only the Data Steward (acting within possible Data Owner constraints) should determine who these organizations are.
- **Share** this "external organization" data privacy policy with Data Owners, offering individual "opt outs" where appropriate or required.
- **Define** a separate, clear and enforceable Data Privacy agreement with every vendor within the organization that is allowed access to sensitive data. Only the Data Steward should determine who these vendors are.
    - There should be additional "data hosting" requirements included in the agreements with vendors who provide their services from the cloud rather than from the organizational IT data center (ex: data must be physically hosted in the U.S. as an example).
    - It should be clearly stated that no new 3rd party partner or purchaser should ever be given access to any data without:
        - A required notification being sent to the Data Steward
        - A reasonable time given to transfer the data from the vendor control to storage approved by the Data Steward.
        - Legally enforceable scrubbing of the data from the vendor controlled storage
- **Deploy** educational solutions which:
    - Can be configured to support these policies
    - Provide the necessary functionality for administrators to ensure that these policies are being enforced … whether the data ultimately resides in a local network or in the cloud.

7. What is the unique role of the Access 4 Learning Community *in ensuring the privacy of sensitive student data?*

- **We are an organization of vendors and end users** who have worked together to deliver secure educational solutions for over 18 years. The Community is ideally positioned to find a middle ground between addressing data privacy concerns on one hand and delivering required solution functionality on the other.
- **We are an educational systems interoperability standards organization**. The Community doesn't delve into the details of how a particular vendor can use data (ex: an eProfile or an XYZ Account) because we don't standardize such use. What the Community DOES standardize is:
    - The information that can be shared between 2 or more interoperating applications.
    - Exactly how that information is conveyed "over the wire".
- **A SIF-compliant solution is an administrable solution**
    - Architects can determine data profiles for the information which can be exchanged (ex: a U.S. FERPA acceptable subset of a de-identified Student).
    - Local Site Administrators can configure the set of specific applications which are permitted to see it.
    - Data Privacy Policies can thus be defined and enforced without requiring the adjusting / reconfiguring of deployed applications

V. Resources

Family Policy Compliance Office, U.S. Department of Education, Model Notice for Directory Information: http://www.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html

National Institute of Standards and Technology, Computer Security Resource Center: http://csrc.nist.gov/publications/

National Institute of Standards and Technology, Guidelines on Security and Privacy in Public Cloud Computing (2011): http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publications (FIPS) 199 (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Privacy Technical Assistance Center, U.S. Department of Education: http://ptac.ed.gov

Privacy Technical Assistance Center, U.S. Department of Education, Checklist–Data Breach Response (2012): http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

Privacy Technical Assistance Center, U.S. Department of Education, Written Agreement Checklist (2012): http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf

U.S. Federal Trade Commission, Complying with COPPA: Frequently Asked Questions- COPPA AND SCHOOLS (2013): http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools

U.S. Federal Trade Commission, FTC Strengthens Kid's Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Protection Rule (2012): http://www.ftc.gov/opa/2012/12/coppa.shtm

RFP Suggestions

Fordham http://ir.lawnet.fordham.edu/clip/2/:

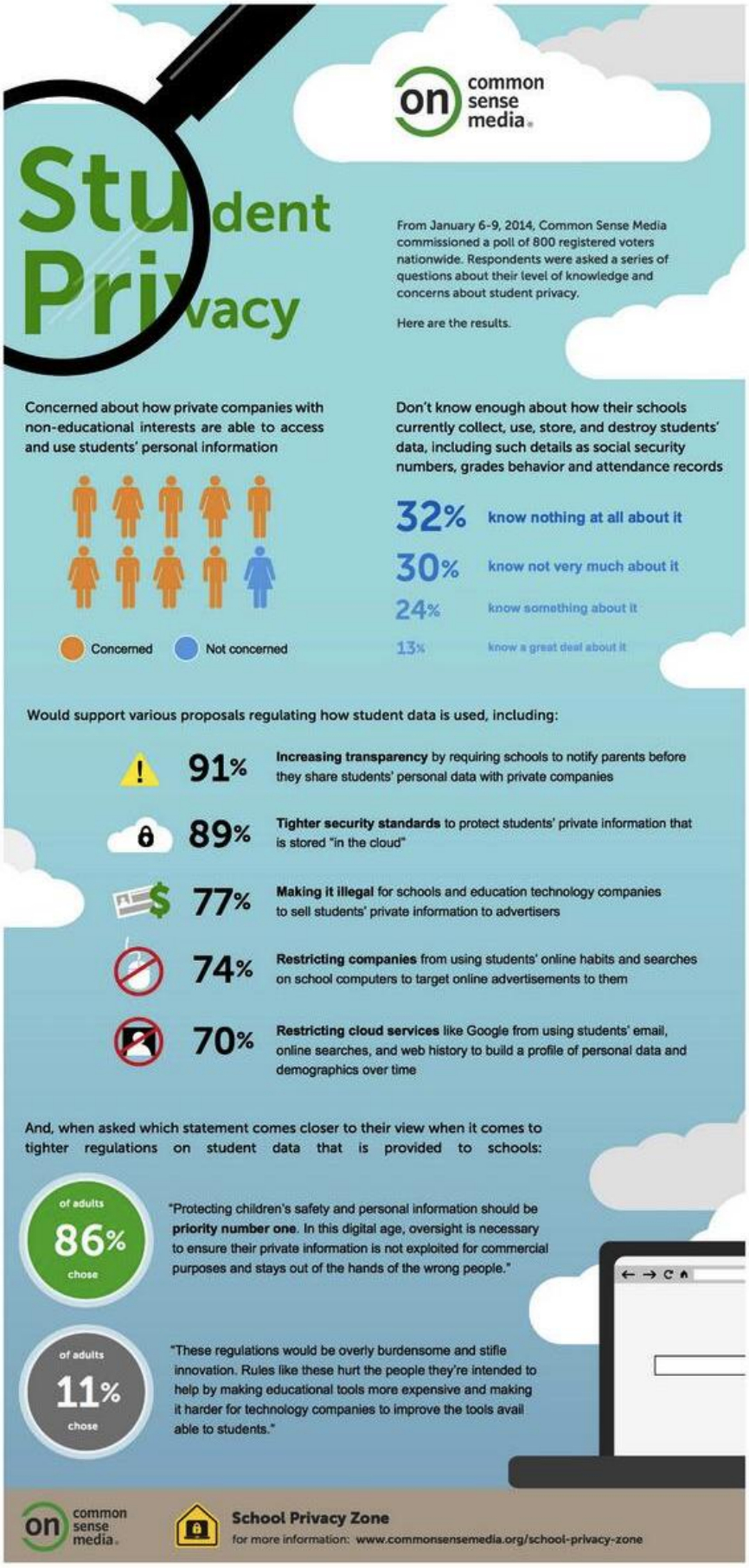
CoSN http://cosn.org/focus-areas/leadership-vision/protecting-privacy

UK Data Protection Resources

https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices - Specific to schools, privacy notices are ways of notifying parents on how student data will be used, and does not require permission.

https://www.gov.uk/data-protection/the-data-protection-act – General Data Protection Act information

https://ico.org.uk/for-organisations/guide-to-data-protection/ - Another source on Data Protection Act, this time from the Information Commissioner Office, the ultimate authority on data protection in the UK.


common sense media
Student Privacy
From January 6-9, 2014, Common Sense Media commissioned a poll of 800 registered voters nationwide. Respondents were asked a series of questions about their level of knowledge and concerns about student privacy.
Here are the results.
Concerned about how private companies with non-educational interests are able to access and use students' personal information
Concerned
Not concerned
Don't know enough about how their schools currently collect, use, store, and destroy students' data, including such details as social security numbers, grades behavior and attendance records
32% know nothing at all about it
30% know not very much about it
24% know something about it
13% know a great deal about it
Would support various proposals regulating how student data is used, including:
91% Increasing transparency by requiring schools to notify parents before they share students' personal data with private companies
89% Tighter security standards to protect students' private information that is stored "in the cloud"
77% Making it illegal for schools and education technology companies to sell students' private information to advertisers
74% Restricting companies from using students' online habits and searches on school computers to target online advertisements to them
70% Restricting cloud services like Google from using students' email, online searches, and web history to build a profile of personal data and demographics over time
And, when asked which statement comes closer to their view when it comes to tighter regulations on student data that is provided to schools:
of adults 86% chose
"Protecting children's safety and personal information should be priority number one. In this digital age, oversight is necessary to ensure their private information is not exploited for commercial purposes and stays out of the hands of the wrong people."
of adults 11% chose
"These regulations would be overly burdensome and stifle innovation. Rules like these hurt the people they're intended to help by making educational tools more expensive and making it harder for technology companies to improve the tools avail able to students."
common sense media
School Privacy Zone
for more information: www.commonsensemedia.org/school-privacy-zone