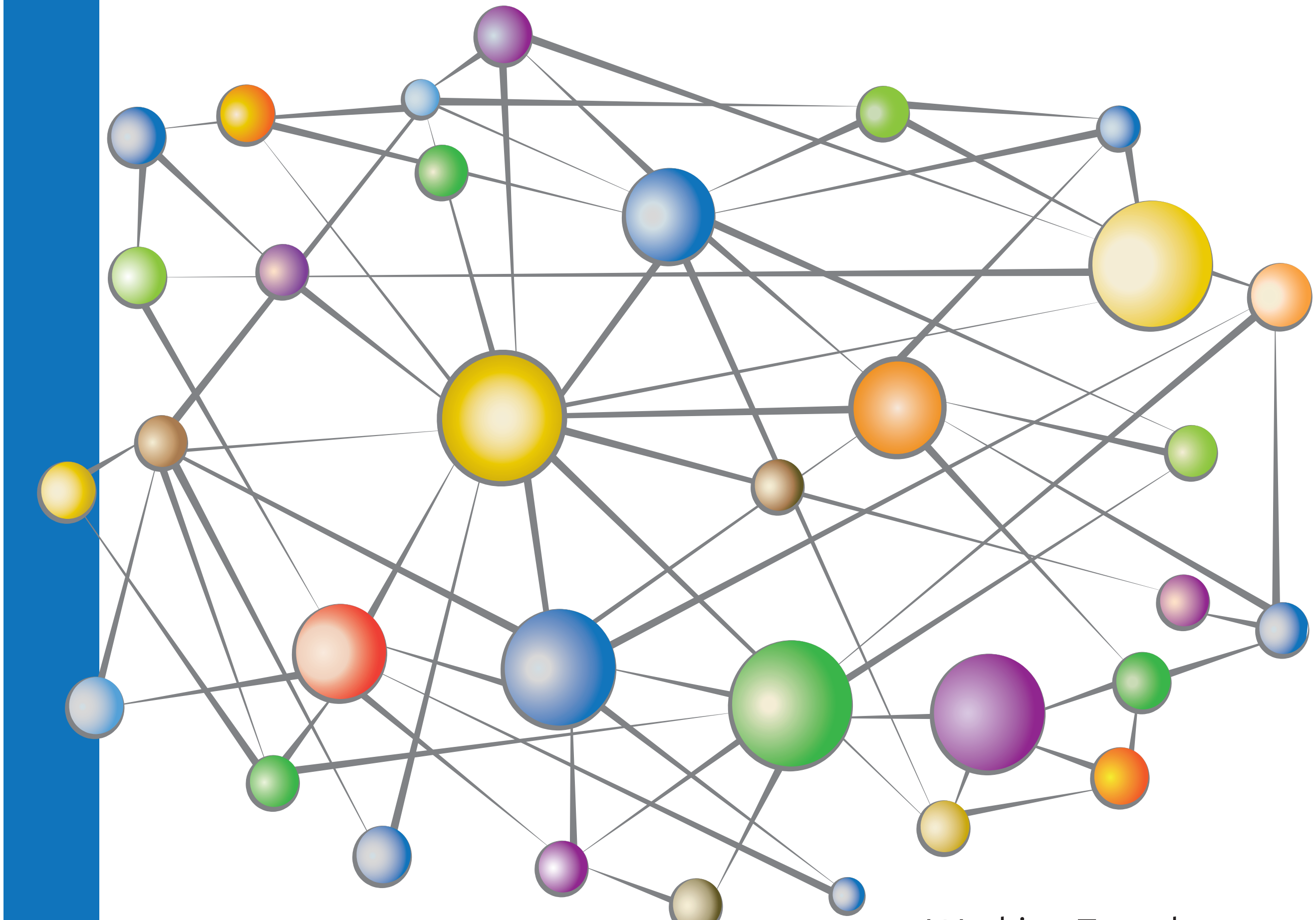
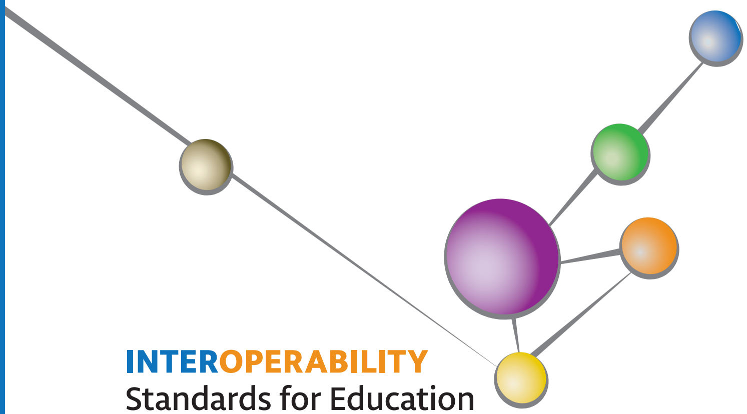
INTEROPERABILITY Standards for Education



Working Together
to Strategically Connect
the K–12 Enterprise

CoSN
LEADING EDUCATION INNOVATION



INTEROPERABILITY Standards for Education

CONTENTS

This CoSN resource is related to the IT Management and Data Management skill areas from CoSN's *Framework of Essentiall Skills of the K–12 CTO:*

Design and editorial assistance by VockleyLang

WHY INTEROPERABILITY STANDARDS MATTER IN K–12 EDUCATION

K–12 education institutions increasingly are looking to digital content and related e-learning technologies to meet evolving education needs and goals. Technology-based products, services and resources are making positive impacts on education and are improving efficiency and outcomes in teaching, learning, and classroom and school management. And yet, as educators grow more sophisticated in their use of technology, there are gaps in the integration and interfaces among disparate applications.

Historically, the case for interoperability—the seamless sharing of data, content and services among systems or applications—has not been compelling in the K–12 education market. As long as programs were restricted to individual computers or small local area networks, the costs to developers of agreeing on and implementing comprehensive, industry-wide standards were rarely justified by the benefits. Many vendors chose, instead, to focus on proprietary designs that, while solving the needs of their customers, did not allow for easy integration with systems from other vendors. Likewise, education decision makers traditionally have been more concerned with locating products that meet their immediate teaching and administrative needs than worrying about data integration as a technical requirement.

Today, however, with the advancement of the Internet and increasing reliance on digital delivery, the usability of isolated K–12 data, content and learning applications is rapidly diminishing. The growing popularity of cloud computing is amplifying the need for interoperability standards that empower school districts to combine multiple services into their IT managed portfolios, which is increasingly a combination of cloud and on-premise solutions.

Interoperability also is a logical response to the growing demand for data warehousing, sophisticated analytics, accountability reporting and performance management tools. Districts are seeking to leverage their content and data assets strategically across a number of systems and assemble best-of-breed solutions that integrate content and applications from a variety of sources and vendors. For cost efficiencies, as well as teaching and learning effectiveness, interoperability standards are a necessary component of these emerging systems.

> For cost efficiencies, as well as teaching and learning effectiveness, interoperability standards are a necessary component of emerging systems.

It is clear that vendor-customized solutions for integration are not a good solution for K–12. A more comprehensive set of industry interoperability standards is needed. The ultimate goal is to create a "plug-and-play" interoperability environment in which applications from multiple vendors can exchange information automatically and without customization. Notably, although they simplify integration, application programming interfaces (APIs)—a set of tools, programs, routines and protocols for integrating applications—usually are not plug-and-play. Instead, APIs often are specific to their application, making it harder for other vendors to adapt their products without writing a customized interface.

Over the past decade, K–12 stakeholders have been collaborating to define the underlying and architectural standards necessary for plug-and-play interoperability. These initiatives are producing useful and promising results. Although the process is far from complete, the foundation for interoperability exists today.

There are many different, overlapping categories of interoperability, each with its own challenges and evolving standards. File sharing, for example—involving common file formats such as CSV, HTML, XML, PDF and Open Document Format—is a simple form of interoperability that has matured to such a degree that many of us take for granted the ability to use our choice of tools to read, and even edit, files created in a totally separate application. Digital accessibility, on the other hand, is more complex, with laws, guidelines and standards that could be the topic of an entirely separate publication.

Eight Key Areas of Interoperability Standards

This primer focuses on eight key areas of interoperability standards:

1. Digital content
2. Data connectivity
3. Data integration
4. Authentication, authorization and identity management
5. Portals and portlets
6. File sharing
7. Network infrastructure
8. Digital accessibility

This primer also covers interoperability governance at the district level, and looks ahead with salient questions about using interoperability standards.

HOW TO USE THIS PRIMER

A conversation with **John Alawneh**, Ph.D., MBA, Chief Information Officer (CIO), Katy (TX) Independent School District and Chair, CoSN Technology Committee

Q. Who should read this primer?

A. Chief technology officers (CTOs), chief information officers (CIOs), technology directors, and other district technology leaders and education technology professionals in districts and schools.

Q. What's the purpose of this primer?

A. The intent is to educate CTOs and other education technology leaders and professionals about the standards that govern their world. We want to make sure they are familiar with the terminology and focus of these standards so they can make appropriate and effective decisions with their technology environment. And we want to make sure they understand the benefits of using interoperability standards to optimize their technology environment.

Think of this as a compilation of a comprehensive range of standards that cover almost every aspect of the technology environment in a school district, with the most important standards in key areas. You don't need to be a standards expert—but you do need to be able to discuss standards with vendors. If you don't know these standards, you're not running your IT (information technology) environment effectively—and somebody else is making decisions for you.

Q. How can education technology leaders use interoperability standards?

A. The standards can be used to develop a governance model for districts to manage interoperability strategically and effectively in their districts. By identifying and agreeing on a set of standards and specifications, districts define what is acceptable when procuring systems and platforms.

The standards also can be used to have more informed and in-depth conversations with vendors. If you're in the market for products or services, from digital content to data connectivity and integration to network solutions, focus on the appropriate standards for these areas. Vendors might approach standards that are more appropriate for them than for you—and you can do interoperability with the wrong standards. Ask vendors what standards they use, and why that standard or standards are appropriate and effective. Understand the privacy, security, network and accessibility laws and rules that govern the environment.

EIGHT KEY AREAS OF INTEROPERABILITY STANDARDS

Digital Content

Twenty-first century educational environments depend on high levels of interoperability among sources of academic content, application software and the networked computing infrastructure of an educational enterprise. Thus, educational content increasingly is developed with the presumption that it will be integrated into multiple enterprise service environments that include both new and legacy content and services.

Ensuring that districts are getting to the highest level of integration is critical for students, teachers and IT staff, as well as for publishers creating digital content. Students and teachers benefit from the availability and seamless integration within their student learning platform, where information is used continually. IT staff benefit from single sign-on (SSO) features of the student learning platform, which applies content to students and teachers based upon organizational needs. Additionally, publishers can ensure usage and that the correct students are using relevant content from the integration into back-end district systems.

Efforts to standardize content formats and interfaces emerged to connect content most efficiently to relevant users. Three main standards for content interoperability grew out of specifications established by the IMS Global Learning Consortium, an international, nonprofit community of educational institutions, suppliers and government organizations. IMS Global originally started in 1997 as an initiative of EDUCAUSE, a nonprofit association of IT leaders and professionals in higher education. Over time, the scope was broadened to include K–12, as well as corporate and government e-learning initiatives. Now a separate entity from EDUCAUSE, IMS Global developed these standards for content packaging and metadata:

1. Common Cartridge (CC)
2. Question and Test Interoperability (QTI™)
3. Learning Tools Interoperability (LTI)

The intent of Common Cartridge, LTI and QTI, which are described below, is to facilitate the development of interoperable digital content and reduce the effort to integrate or replace content in production learning environments.

In addition to these standards, IMS Global maintains a conformance certification process for content providers and delivery systems, which includes Common File Format (CFF) and Accessible Portable Item Protocol™ (APIP). IMS Global maintains a community of testers committed to resolving conformance issues, implementing revisions and retesting as needed to establish full conformance with its standards. The organization also maintains a list of products that are in conformance with the most recent versions of the standards.

Digital Content Interoperability Standards

COMMON CARTRIDGE (CC) is the IMS Global format for distributed learning environments, both online and offline. The Common Cartridge project uses IMS Global's most widely adopted specifications to define a common format for learning management systems (LMS), allowing courses from any provider—as well as content developed in-house—to be mixed and matched.

The format is flexible; a cartridge may be an assessment filled with test items, an entire set of supplementary digital content that comes along with a textbook, an online course, a lesson plan, or a specific topic or learning object complete with topics, assessments and feedback. Common Cartridge has emerged as the primary standard for digital content in K–16 education environments. It is in active development and in the process of being integrated with companion standards.

Vendor implementations of Common Cartridge are increasing—most notably with Thin Common Cartridge, where the lightweight structure supports rapid deployment of content. This is especially popular with school districts that need to integrate publishers' content into LMS with full search ability, without the need for massive data exchange. (See the case studies on Katy Independent School District on page 6 and Houston Independent School District on page 26 for examples of such implementations.)

The Common Cartridge LMS interoperability format is a package that specifies six requirements:

1. A format for exchange of content between systems, described in a manifest referenced by URL, so that there is a common way to interpret what the digital learning content is and how it is organized.
2. An authorization standard or access rules for each component of the package to protect content or applications requiring a license, so that it is contained in a cartridge in a flexible way along with unprotected content.
3. A standard for the metadata describing the content in the cartridge.
4. A standard for test items, tests and assessments. This standard allows the LMS to understand imported assessments as native so they can be manipulated as needed in the system (such as deciding which items are to be used and where in the flow of a course).
5. A standard for launching and exchanging data with external applications so they can be part of a single learning experience orchestrated through the learning system.
6. A standard for populating online discussion forums for collaboration among students. This allows such forums to be pre-populated with potential exercises, discussion threads and other elements.

For more information on Common Cartridge, see ***www.imsglobal.org/commoncartridge.html*** *and* ***www.imsglobal.org/digitallearningservices.html.***
See also diagrams of ***Common Cartridge, Common Cartridge Content Hierarchy*** *and* ***Learning Tools Interoperability.***

QUESTION AND TEST INTEROPERABILITY (QTI) is an IMS Global specification that allows assessment items, item banks, assessments and results data to be shared among construction tools, content providers, and learning and assessment delivery systems.

Related to the QTI standard is the **ACCESSIBLE PORTABLE ITEM PROTOCOL (APIP)** standard, which is very similar to QTI. APIP specifies an additional requirement that allows test items and associated accessibility information to be ported between systems. The standard focuses on accommodating the needs of the individual student, including alternate representations of test content to students with impairments. IMS Global requires vendors to join the QTI/APIP Alliance to achieve official certification of conformance to these two standards.

For more information on APIP and QTI, see ***http://www.imsglobal.org/apip/*** *and* ***http://www.imsglobal.org/question/.***
For a list of products tested and certified by IMS Global, see ***http://www.imsglobal.org/cc/statuschart.cfm****.*

LEARNING TOOLS INTEROPERABILITY (LTI) is an IMS Global standard for integrating rich learning tools (applications) with platforms such as LMS, portals or other educational environments. Learning tools are web-based applications hosted externally to the learning platform. The idea is to integrate these external tools or applications seamlessly into the learning platform in a plug-and-play fashion without any custom integration work or programming. Applications such as chats and math and science virtual labs can easily plug into learning platforms, becoming fully integrated into the user, security and content processes of the hosted platform.

Learning tools provide the way to establish the services offered through the platform and outline who has access to them, the level of security and the capabilities of each service. Through LTI, integrated content maintains single sign-on (SSO) functionality, which provides each user with a single sign-on ID and password. Most recent LTI versions provide more advanced bidirectional communications between the tools and the platform of vital data, such as user and security information.

A unique K–12 challenge in the move to digital curriculum is that content providers have a number of options to deliver content. These options can present districts with challenges in determining the best way to grant user access to these resources.

Some content providers develop SSO support. SSO allows users to log onto a system once, after which their credentials are passed to all others downstream in the content, negating the need for additional logins to different systems. However, LTI can provide a more advanced SSO functionality when integrating applications into the platform. One big advantage with LTI is that user attributes and metadata, along with the context and role, can be passed along between the platform and the application for an easier integration process.

http://www.imsglobal.org/toolsinteroperability2.cfm

SCORM (SHARABLE CONTENT OBJECT REFERENCE MODEL) is a standard developed by the Advanced Distributed Learning (ADL) Initiative. Established in 1997 by the U.S. Department of Defense, ADL has worked with multinational groups from industry, academia and government to define specifications and standards for education and training and develop tools and content to those standards. SCORM content supports informal learning, such as educational reference, on-the-job training and performance support.

A key part of the SCORM standard, now in its 2004 4th Edition, is the **CONTENT AGGREGATION MODEL (CAM)** that defines how to aggregate, describe and sequence learning objects. SCORM CAM is required in some government agency requests for proposals (RFPs) or contracts for training applications in the United States and internationally. Last released in 2006, it was updated in 2009. Conversion tools are available to make SCORM-compliant content (typically referred to as SCORM "packages") compatible with the IMS Global Common Cartridge.

http://www.adlnet.gov/scorm/

CASE STUDY

Content Integration in Katy ISD

Katy ISD is a flourishing suburban school district that encompasses 181 square miles in southeast Texas. Student enrollment is around 73,000 students served by over 60 schools. It is located in one of the fastest growing areas in the country, growing by about 3,000 students per year. Katy ISD strives to create an environment where students have an equal opportunity to be connected inside and outside the classroom.

Early on, Katy ISD pioneered the adoption of Bring-Your-Own-Device (BYOD) as a way to promote technology integration into the classroom. The district has since continued on with a more comprehensive strategy of integrating technology into the learning process by supporting more devices in the classroom, bridging the digital divide, providing access via cloud technology, training for leadership and teachers, supporting decision-making through effective data systems and building a robust network infrastructure.

The most important work in support of this strategy is the seamless integration of content into the district's online learning platform. The platform allows teachers and students as well as parents to access interactive and engaging online content and resources specific to each classroom in a standard and consistent way. Teachers are able to identify instructional materials, personalize activities, assign and prepare learning tasks inside and outside the school environment. To move away from the costly customization of content integration, Katy ISD recently has embarked on a substantial effort of streamlining the integration of digital resources into its

Continued on the next page

online learning platform.

THE CHALLENGE. Katy ISD has adopted an online learning platform that is compliant with IMS Global open standards, which are a key factor in supporting the seamless data and security integration strategy that the district is seeking.

Previously, the district purchased content from high school publishers through the state of Texas adoption process for instructional materials. Although the district's platform supports open standard integration, many providers, including textbook publishers, were not in compliance with these standards. Plus, some existing content and tools were not standards-compliant—and vendors were not eager to quickly bring those products into compliance.

THE SOLUTION. Katy ISD started work on a content integration strategy by engaging stakeholders with expertise in technology, curriculum, textbook publishing and district administration. Their first step was to build consensus and understanding as well as to identify the overall benefits, goals and objectives. The following are some of the main objectives identified early in the process:

- Preserve the long-term investment in the learning platform.
- Lower the cost of acquisition and integration of content and digital resources.
- Improve the flexibility of integrating content and digital resources.
- Allow for seamless integration of content and digital resources.

Some long-term measures to address the challenge made it a requirement of the acquisition process that all new content providers be in compliance with the IMS Global Learning Tools Interoperability (LTI) and/or Common Cartridge (CC) standards (or commit to be in compliance within a specified period of time). For the short-term—and to create more leverage with existing vendors—Katy ISD joined forces with neighboring Houston ISD to negotiate content integration.

Houston ISD was in the process of implementing its own online learning platform, a different platform than Katy ISD's, and was running into similar challenges. Because of its size, it was easier for Houston ISD to build good partnerships with willing publishers, such as Houghton Mifflin Harcourt, and negotiate for CC integrations for its science digital adoptions. Katy ISD knew of these publishers, and was able to more effectively communicate with them to deliver its own district content, specifically in the chemistry course adoption as a Common Cartridge. The Katy ISD integration effort will continue as more content and resources are added through new state of Texas instructional materials adoptions.

Katy ISD believes that conformance to open standards will lower its cost of acquisition and improve its ability to adapt to changing content and technology. When districts can "plug-and-play" content and tools from other vendors, they can adopt one platform only, with the flexibility of access to multiple sources of content. It is less costly and much more efficient. Katy ISD is committed to open interoperability standards and will continue to work with other districts and organizations such as IMS Global to promote this effort.

Katy ISD is currently a member of IMS Global and CoSN, which also supports open interoperability standards in education. This collective effort is important to the future of interoperability in education.

Data Connectivity

The main objective of data connectivity standards is to provide universal connectivity to data sources from a variety of platforms to transfer data using a standard set of commands in an efficient and cost-effective way. Data connectivity is essential for mission-critical applications, including enterprise resource planning (ERP), student information systems (SIS), learning management systems (LMS) and data warehouse applications. These systems have zero tolerance for delays or errors in accessing, processing and storing data. Unreliable data connectivity design can lead to poor performance, availability and scalability, and to data integrity issues that have direct impact on cost and risk for districts.

Unreliable data connectivity design can lead to poor performance, availability and scalability, and to data integrity issues that have direct impact on cost and risk for districts.

Application programming interface (API) refers to a set of high-level functions that can be used by an application to access low-level operating system (OS) services. An API, in the form of a data connector (or "driver"), is often required to translate from one standard database language—such as Structured Query Language (SQL) for relational databases and Multidimensional Expressions (MDX) for online analytical processing (OLAP) databases—to another, making standardized data connectivity possible.

Several connectivity standards are on the market today for accessing the most popular database platforms. Making a proactive, conscious decision to use enterprise products that support a single data connectivity standard can help greatly with production performance, reliability and scalability. When this is not possible, it is necessary to find data solutions that address the connectivity challenges offered by multiple standards.

Vendors of databases and other data-oriented solutions typically create drivers designed to meet the minimum requirement of the major standards and provide a minimal level of data connectivity for their products. Provided at no extra cost, these default drivers might appear to be cost-effective—but they can fall short of the performance requirements for critical systems and necessitate the purchase of additional, expensive drivers that increase overall support and maintenance costs. In addition, some database providers add proprietary extensions to data connectivity standards, improving performance for that particular product but, at the same time, eliminating the benefits of a standardized API and making it difficult for customers to switch to another vendor's database engine (often referred to as a "lock-in").

Third-party database connectivity products offer an alternative for critical system deployments. Such products serve a specialized purpose—facilitating data connectivity among all the components of a data system—and typically support required features without forcing lock-in to a specific database or version. Within the category of third-party solutions, developers and IT managers should look closely at the following factors before selecting a vendor for a data connectivity tool:

- **Product comprehensiveness and breadth,** including being current with specifications and providing unmatched coverage across APIs (JDBC, ODBC, ADO.NET, all described below), databases (Oracle, Microsoft SQL Server, DB2, Sybase, Informix and more) and operating systems (Windows, UNIX, Linux, iSeries, z/OS)
- **Production-proven** in a variety of environments and quality-proven through specification certification and a large customer base
- **Technical support,** with multi-channel support via phone, fax, email and web
- **Technical leadership** as an industry-trusted specification leader for JDBC, ODBC, ANSI SQL and XQuery
- **Corporate focus and strength,** with a 100% focus on database connectivity

OPEN STANDARDS VS. INTEROPERABILITY

It is important to note that there is a difference between open standards and interoperability. While open standards tend to be more inclusive and broad, interoperability is less broad and can be limited to certain vendors or products. Interoperability can be between two products or among a range of products, or driven by a dominant product. Open standard is more inclusive and a result of an open protocol adopted by a community of vendors and stakeholders. For example, Internet Protocol (IP) is an open specification that allows networks to function. Any vendor can take advantage of IP by developing hardware and software around it.

It is also important to note that open source has played a big role in the IT world. Several open source communities are developing and distributing data connectivity standards on an ad hoc basis. Although these are still in progress, the open source community—given its commitment to open standards and history of success at providing open solutions such as Apache, Linux and JBoss—can be expected to succeed at developing enterprise-viable data connectivity standards for open-source environments.

Data Connectivity Standards

OPEN DATABASE CONNECTIVITY (ODBC) interface by Microsoft allows applications to access data in database management systems using the popular Structured Query Language (SQL) as a standard for accessing the data. ODBC permits maximum interoperability, which means a single application can access different database management systems. Application end users can then add ODBC database drivers to link the application to their choice of database management system.

msdn.microsoft.com

http://www.simba.com/odbc.htm

JAVA DATABASE CONNECTIVITY (JDBC) is an API specification originally developed by Sun Microsystems for connecting applications written in Java to data in popular databases. JDBC allows encoding of access request statements in SQL, which are then passed to the application that manages the database. This API returns the results through a similar interface. JDBC is very similar to ODBC and, with a small ”bridge” program, the interface can be used to access databases through the ODBC interface—for example, writing an application designed to access many popular database products on a number of OS platforms.

http://docs.oracle.com/javase/tutorial/jdbc/basics/

ACTIVEX DATA OBJECTS (ADO) is the data access model provided for Visual Basic users to write applications for the Microsoft Windows platform. VBScript, a specialized language used primarily to program functionality for web pages, also uses ADO.

ACTIVEX DATA OBJECTS FOR .NET (ADO.NET) data standard by Microsoft provides a uniform method to access data from a number of data sources within Microsoft’s .NET Internet framework. ADO.NET encapsulates ways to connect to a database and access data—whether it is relational, XML or application-specific—and enables application developers to retrieve the results.

https://msdn.microsoft.com/en-us/library/aa286484.aspx

OBJECT LINKING AND EMBEDDING DATABASE (OLE DB) is Microsoft’s strategic, low-level API for embedding objects from different data sources. The original goal was to offer an object-oriented alternative to standards such as ODBC, but this API is mostly used today for object embedding and coexists with such other standards as ODBC and JDBC

https://msdn.microsoft.com/en-us/library/ms722784(VS.85).aspx

Data Intergration

IT environments have become more complex and educational institutions have become more reliant on data as a cornerstone to decision-making processes. This is driving the need for more reliable and timely integration of data. Integrating data across the enterprise is critical for increasing productivity, improving business efficiencies and reducing costs.

Data integration begins with data connectivity (described above), but goes beyond it to include data translation, standard data output format and other transformation services to make the data usable by each application. Data integration involves combining data residing in different sources and providing users with a unified view of these data. This process becomes complicated in a variety of situations in education. Consider these examples:

- **Data warehousing applications.** The data warehouse system extracts, transforms and loads data from several sources into a single schema. As a result of data integration, disparate data silos can be combined logically into a single and uniform data source in the data warehouse without having to migrate the physical data.
- **Integrating information systems together.** For example, most student information, learning management and assessment systems use the same data elements. A complex integration is required to streamline the sharing of student information, content and assessment data and, therefore, reduce the classroom setup time on teachers and students. Additionally, data integration is essential for ERP systems that combine finance, human resources and student information from different sources to simplify and automate business processes.

One challenge of data integration is that data structures often reside on different platforms that need to be linked together using different database solutions and computer languages. To avoid making sweeping changes to existing applications or reprogramming for every system change, integration specifications and standards have emerged to define how systems manage the exchange of information.

Data integration challenges appear with increasing frequency as the volume and the need to share existing data increases. This area—often referred to in management circles as "enterprise information integration" (EII)—has become the focus of extensive work, and numerous open problems remain unsolved. Consequently, organizations such as Ed-Fi Alliance and initiatives such as Common Education Data Standards (CEDS), both described below, have invested significant effort to develop integration standards and architectures that serve the education market. These data integration models standardize and organize data in a broad range of systems so it can be easily stored in data repositories and served through dashboards. CEDS provides the tools and a key set of data elements to streamline the data exchange between these systems, while Ed-Fi Alliance brings together standards such as XML, guidelines such as representational state transfer (REST) for creating web services and application programming interfaces (APIs) into an operational and integrated data environment.

Currently, there are many different ideas regarding what constitutes a good standard for data integration. However, there seems to be general consensus on the four components that are essential for modern data integration architecture:

1. **A broker to centrally manage security, access and communication**. The Schools Interoperability Framework (SIF) Zone Integration Server (ZIS) and the Enterprise Service Bus (ESB) provide this type of service.
2. **An independent data model** based on a standard data structure such as XML
3. **A connector** that can speak natively with the centralized broker
4. **A system model** that defines the data flow and rules of engagement to interface with it in a standardized way

Data Integration Standards and Tools

COMMON EDUCATION DATA STANDARDS (CEDS), an initiative sponsored by the U.S. Department of Education, is a national collaborative to develop common data standards for a key set of education data elements, known as a data dictionary, to streamline the exchange, comparison and understanding of data within and across P-20W (early learning through postsecondary and workforce) institutions. CEDS is a voluntary effort that will increase data interoperability, portability and comparability across states, districts and higher education organizations.

CEDS is a specified set of the most commonly used education data elements to support the effective exchange of data within and across states, as students transition between educational levels and sectors, and for federal reporting. This common vocabulary will enable more consistent and comparable data to be used throughout all education levels and sectors to support improved student achievement.

The CEDS Data Model (version 5) includes a hierarchical schema of nontechnical domains, entities, elements and option sets, among others. Entities are commonly thought of as persons, events, objects or concepts about which data can be collected. Domains provide a user-friendly structure to identify elements. The standard name of a data element in CEDS is defined for human readability and understandability, to avoid possible confusion when using an element in a different context or across domains.

http://ceds.ed.gov/

ED-FI ALLIANCE provides technology that serves as the foundation for enabling interoperability among secure education data systems designed to improve student achievement and teacher satisfaction. To achieve this goal, the community of education agencies and educational technology vendors continually improves and expands the Ed-Fi Data Standard, which is aligned with the Common Education Data Standards.

The Ed-Fi Data Standard powers IT systems and educator applications using the Ed-Fi Implementation Suite—a set of standards-based technology components that incorporate community input and field-tested solutions. The implementation suite includes an operational data store (ODS) for integrating secure real-time data from other systems, an API to easily exchange data between systems, a dashboard that puts real-time, actionable data at the fingertips of educators, and development tools that help technology leaders implement these components. All of the components are interchangeable, community-proven, and field-tested so IT leaders can choose any combination and have confidence the component(s) will solve the unique needs of their system environment to improve connectivity and data accessibility.

http://www.ed-fi.org/

LEARNING INFORMATION SERVICES (LIS) is a vendor-neutral set of standards designed around the specific data integration needs of learning environments. The specification, developed by IMS Global Learning Consortium, defines how to exchange enterprise data, such as data about learners, faculty, courses, grades and the enrollment relationship among the major systems in use at learning institutions. Typically, this data is held within a student information system (SIS). This system is then typically used to populate other systems, such as learning management and library management systems and learning object repositories.

http://www.imsglobal.org/lis/

SCHOOL INTEROPERABILITY FRAMEWORK (SIF) is an open standard for K–12 data exchange designed to enable diverse applications, such as library, student information and transportation systems, to interact and share data. SIF is comprised of the SIF-Connect Server and the Universal Agent Suite tools. Data is extracted from a variety of applications, converted into a format that meets the current SIF specifications, and placed into an operational data store. The Universal Agent sends the data to the SIF server, which determines where the data need to go.

The goal of SIF is to ensure that all SIF-compliant applications can achieve interoperability, regardless of the software and hardware used in their development. Recent developments in SIF include vertical reporting (the reporting of high-stakes test results from schools up through the hierarchy to the federal government) and the introduction of objects related to e-learning content. One feature of SIF that makes it well suited for data interoperability is its use of the XML standard, already widely used. In recent years many companies in the K–12 market have embraced the data integration standards in SIF. Several case studies have shown significant dollar savings for school districts from such standardization and many districts currently require their vendors to use SIF. Additionally, many K–12 vendors have developed SIF agents that allow their products to work within this framework.

https://www.sifassociation.org/

ENTERPRISE SERVICE BUS (ESB) is a software architecture that provides services for event-driven, complex architectures using a standards-based messaging engine (the "bus"). While SIF is more focused on data integration in general, ESB focuses more specifically on web application integration. Developers typically implement ESB using technologies found in a category of middleware infrastructure products, usually based on recognized standards.

An ESB generally provides an abstraction layer on top of an enterprise messaging system, which allows integration architects to exploit the value of messaging without writing code. In an enterprise architecture making use of an ESB, an application will communicate via the bus, where ESB acts as a message broker between applications and enables communication among them. This approach has the primary advantage of reducing the number of point-to-point connections required to allow applications to communicate.

http://en.wikipedia.org/wiki/Enterprise_service_bus

Authentication, Authorization and Identity Management

Authentication and Authorization

The majority of K–12 organizations use Microsoft Active Directory as their primary directory for authentication and authorization to digital resources. The challenge has been integrating the large number of applications used both on-premise and on the Internet to allow for a secure method of authentication and authorization from a school's primary directory.

There are two important "gatekeeper" processes involved with identity management:

- **Authentication** identifies a user through a username or ID, password, smart card, fingerprint or some other means.
- **Authorization** specifies access rights to resources. During the authorization process, the system uses a set of access control rules to decide whether requests are granted or rejected. In the K–12 world, this is generally accomplished by feeding user demographic data from human resources and/or student information systems to the identity management system. Additional information is derived from user demographics to determine authorization to various systems. For example, the system knows to automatically grant classroom teachers access to the grading system.

On-premise applications must integrate with Active Directory to allow for a single user ID and password. This can be done with direct integration to Active Directory or through open standard protocols, such as the Lightweight Directory Access Protocol (LDAP, described on page 14).

A list of all the internal systems that require username, password, rights and role information can be quite long. Student information and grading systems, special education databases and file sharing tools are just a few examples.

A variety of external systems used by schools also benefit from being able to authenticate from the same primary directory. This multitude of online systems requiring identifying information creates evolving identity management challenges. A new approach, known as federated identity management (FIM), allows users to sign on to multiple enterprise networks using the same user ID and password. Authentication and authorization over the Internet, where the types of communication are typically limited to HTTP and HTTPS, are performed through a number of communications protocols (described below).

Authentication and Authorization Protocols

SECURITY ASSERTION MARKUP LANGUAGE (SAML) is an open-standard data format used for exchanging authentication and authorization data between an identity management system and an application. The most recent update, SAML 2.0, is used in the majority of identity deployments. Its primary goal is to address the challenge of web browser single sign-on (SSO). Developed by the OASIS Security Services Technical Committee, a global consortium involved in the development, convergence and adoption of e-business and web service standards, SAML is XML-based, which offers flexibility in deployment. Federated partners can choose which identity attributes they want to share in the SAML assertion, as long as the attributes can be represented in XML. Because of SAML's interoperability, SSO connections can be established with many federated partners with a single SAML deployment. WS-Federation is a less used federation specification, but it is capable of allowing disparate security realms to broker information on identities, identity attributes and authentication.

OAUTH 2.0, an authorization framework, enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner—by creating an approval interaction between the resource owner and the HTTP service—or by allowing the third-party application to obtain access on its own behalf. This is commonly used to allow access from one web application to another based on the authentication already granted to the first application. An example of this is connecting to an Internet application, which then asks if the user would like to log in with Facebook, Google or an account from another application.

Identity Management

Identity management involves the business processes and supporting infrastructure needed for the creation, maintenance and use of digital identities. The central questions an identity management system (IDM) seeks to answer are:

- **Who are you?**
- **What are you allowed to do?**
- **How will the resources be managed to provide required access?**

The first two questions refer to authentication and authorization, discussed above. The third question relates to the administration of resources available for authenticated users. The administration of a central identity management repository across systems to create a single user account within a directory services system, such as Microsoft's Active Directory or Novell's eDirectory, can be further enhanced using open standards protocols such as LDAP (described below).

In an educational setting, one example of identity management might be a K–12 school district and local community college agreeing to federate identities so high school students can log on to the wireless system at the community college to access online resources. This would require that the community college trust the quality of the district's identity system, and agree that the district policies for ensuring authentication are acceptable for students to access the wireless system. In this scenario the risk is reasonably low, so the trust required would likely be low as well. On the other hand, if a school wanted to have its students log on to take online tests, access grades or participate in classes, the risk of poor authentication would clearly be much higher.

Identity Management Standards

SHIBBOLETH, a project of the Internet2 Middleware Initiative, is a standards-based, open source software package for web SSO across or within organizations. The system allows sites to make informed authorization decisions for individual access of protected online resources. Shibboleth uses the SAML federated identity standards to provide a federated SSO and attribute exchange framework.

Shibboleth also provides extended privacy functionality, allowing browser users and their home sites to control the attributes released to each application. With the Shibboleth software, users authenticate with their organizational credentials. The organization (or identity provider) then passes the minimal identity information necessary to the service manager to enable an authorization decision. Shibboleth is developed in an open and participatory environment, is freely available and is released under the Apache Software License.

shibboleth.internet2.edu/

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) is an application protocol for querying and modifying data from directory services implemented in Internet Protocol (IP) networks. LDAP provides for a complex level of access control instances via access control instructions (ACIs) that make it easy to securely read and modify authority. ACIs can control access depending on who is asking for the data, what data is requested, where the data is stored and so on. This access is controlled on the server side, rather than through client software, making it more secure. LDAP is an open protocol that is both cross-platform and standards-based, so applications need not worry about the type of server hosting the directory. Microsoft, IBM and other major vendors support LDAP. There is also an open source implementation (OpenLDAP).

www.tech-faq.com/ldap-lightweight-directory-access-protocol.html

OPENID authentication is a decentralized SSO service managed by the OpenID Foundation. It is simple, free and provides verification of user identity from an identity provider to a service provider. Several large providers, including AOL, Facebook, Google, MySpace, PayPal, Yahoo! and VeriSign, use OpenID. This protocol is easy to use and implement for web account access. Its decentralized and portable characteristics make it very attractive to users.

Because of its popularity as an identity system (used by popular providers such as Facebook and Google), some school districts are allowing users to associate their accounts with OpenID to simplify account creation and logins.

http://openid.net/foundation/

Portals and Portlets

The portal environment and portlets were introduced in the late 1990s as an alternative to complex Java coding in the early days of Java. IT professionals found it refreshing to work with an architecture like the portal, into which portlets could be dropped in quickly and easily with minimal coding or expertise to manage them.

However, portlets in those days lacked interoperability to make them efficient and cost-effective. Vendors developed portlets that worked well with their own portals but not with others. Interoperability standards were needed to organize this market and deliver on the original promise of portlets.

In 2003, vendors of Java-based enterprise portals responded to this market demand by building a framework to standardize the portal environment. The result was a standard known as Java Specification Request (JSR) 168, which specified an API for interoperability between enterprise portals and portlets. Software vendors began producing JSR 168-compliant portlets that could be deployed onto any JSR 168-compliant enterprise portal. The second iteration of the standard, JSR-286, was released in 2008. Because of these standards, many enterprises started developing their own portals based on their business structure and strategic focus while reusing the same architectural framework.

Enterprise portals start taking off in the late 1990s and continued to grow for the next 10 years as the best way to publish and share information with employees, the public, parents or executives. The main attraction of the portal environment was the ability to easily customize it to fit diverse user needs. This flexibility came from the interoperability standards, which enabled the use and reuse of predesigned portlets that plugged into a portal container or servlet within the portal. Portlets then responded to commands from the container to perform certain functions.

School districts began exploring this tool in a more robust way around the time the standards started taking shape. The availability of standards-compliant portlets allowed districts to take advantage of the abundance of libraries with portlets ready to plug into their portals. As a result, there was an explosion of the student portal, parent portal, employee portal and more in school environments. Although smart apps and the cloud are beginning to replace some portal concepts, portals are still a mainstream product in many districts—and this environment is not going away anytime soon.

A collection of portlets, such as email, weather, discussion and news portlets, can mesh together a web-based application hosted in a portal or on a website.

Portal and Portlet Standards

JAVA SPECIFICATION REQUEST (JSR) 168 addresses the areas of content interoperability, aggregation, personalization, presentation and security. Also known as Java Portlet Specification 1.0, this standard's primary purpose is to define the programing interface for Java portlet development. Developed with the support of the Java Community Process (JCP) and released in 2003, it defines the functionality of a portlet container and the standard interface through which it interacts with user-specific portlet code. Additionally, JSR 168 provides a URL-rewriting mechanism for creating a user interface within a portlet container and defines ways of effectively handling portlet security and personalization characteristics. Portlets adhering to this standard can run in portals regardless of the vendor.

JAVA SPECIFICATION REQUEST (JSR) 286, released in 2008, expanded JSR 186 to include portal-to-portal communication. Also known as Java Portlet Specification 2.0, its main features include inter-portlet communication, serving dynamic resources directly through portlets, serving AJAX or JSON data, and introducing portlet filters and listeners.

jcp.org/

WEB SERVICES FOR REMOTE PORTALS (WSRP), an effort of the Organization for the Advancement of Structured Information Standards (OASIS), defines a standardized interface between a portal and portlet

service that allows the plug and play of visual, user-facing Web services with portals. This standard facilitates interoperability between a WSRP-enabled container and any WSRP-compliant portal, allowing Java portlets to plug into WSRP-enabled portals.
www.oasis-open.org/committees/wsrp

Today, the market is crowded with vendors that offer standards-compliant products, which provide an architectural framework ready for standards-compliant portlets to plug in with minimum coding. SharePoint by Microsoft is one of the most popular of these products. IBM, Oracle and its subsidiary BEA Systems, and many more also have robust products in this area.

In recent years, lightweight and easy-to-deploy portlets have become popular. Typically, these portlets are built around Web 2.0 technologies such as:

- **Asynchronous JavaScript and XML (AJAX)**, a set of web development techniques deploying several technologies, such as HTML and CSS, to allow users to interact with objects on a screen while accessing data
- **Representational state transfer (REST),** a set of guidelines for creating web services
- **Web-oriented architecture/service-oriented architecture (WOA/SOA)**, a design architecture that emphasizes user interfaces

These portlets tend to provide the same functionality and interoperability as traditional ones, with the ability to easily personalize them.

File Sharing

File sharing is one of the earliest forms of electronic data and information exchange. Files are shared via the network, emails or flash drives. Files of all kinds are downloaded via the cloud or from an Internet website. In fact, the majority of information exchange happens via file sharing. There are so many file formats available that it is not practical to list them all. The focus here is on file formats typically used in enhancing systems interoperability. These formats are commonly used when uploading or downloading large amounts of data from or to systems for the purpose of exchanging data between systems.

Sharing files within a school district has many applications:

- Most commonly, multiple computers edit files in a variety of formats in **a local or common file store, or network**. This is common for office automation, where a computer will run an application, data is pulled from a common file store, edited by an end user and finally saved back to the common store. The latest iteration for this type of file sharing is the use of programs that reside on the Internet in the cloud and save data back to the cloud.
- **Peer-to-peer file sharing (P2P)**, began as a negative form of file sharing within school districts as it was widely known as a way to redistribute copyrighted material. Over the years, the connotation has changed. Programmers now use it to save bandwidth and redistribute application files by asking peers instead of downloading everything from the web.
- **Cloud-based file storage** such as Dropbox, Google Drive, iCloud Drive, OneDrive and Box

The challenge for school districts isn't so much the sharing of files, but the complex process of integrating large amounts of data stored in the files into another system. The process relies heavily on selecting the right file format, appropriate to the type of data, and data normalization, transformation and integration processes. This requires a significant investment in time and resources by district IT staff and vendors to build a comprehensive process using file transfers. This process normally ends up being a highly customized solution that isn't easily replicated by a vendor for other customers.

Data exchange is another area where file sharing plays a large role. The process involves taking data structured under one source schema and subsequently transformed into data structured under another schema. Data exchange, unlike data integration, transforms data using data exchange languages such as JavaScript Object Notation (JSON), Resource Description Framework (RDF) and Extensible Markup Language (XML).

The data exchange process is especially important when school districts populate their data warehouses with large amounts of data from operational systems such as SIS and ERP. That data often come from external sources in large files that must go through a complex process known as **EXTRACT, TRANSFORM, LOAD (ETL)**—a less common, but vitally important, file sharing process. ETL means that a file is extracted from an authoritative data source, modified as needed to work in another system and then loaded into that other system. This is especially important and widely used when moving large amount of data for data warehouses. There are limited file formats used for this purpose. The Common Education Data Standards, described on page 11, provides the tools and a key set of data elements (data dictionary) to streamline the data exchange for education institutions.

File Sharing Standards

EXTENSIBLE MARKUP LANGUAGE (XML) is a widely supported specification produced by the Worldwide Web Consortium for encoding documents as a textual data format with strong support for the representation of data structures and programming. XML-based formats have become the default for most office productivity tools, including Microsoft Office, openOffice.org and Apple's iWork.

XML FOR ANALYSIS (XMLA) is an XML extension that employs a set of XML message interfaces to define data access interaction between a client application and an analytical data provider working over the Internet. This extension allows client applications to talk to multidimensional or OLAP data sources. XMLA is designed for thin client architecture, moving analytical applications away from traditional client/server roots towards flexible web-based architecture. The result is faster response times and less intensive demand on resources. What differentiates XMLA from previous attempts at a file sharing standard is that it has gained broad support from companies, including Microsoft, Oracle Hyperion, SAP and SAS.

http://www.xml.com/

NETWORK FILE SYSTEM (NFS), developed by Sun Microsystems, is a distributed file system that lets a user mount a volume across a network and have it represented and used as a local file store. NFS is an open standard allowing anyone to implement the protocol. School districts commonly use this standard when mounting volumes using the UNIX/Linux operating systems.

http://pages.cs.wisc.edu/~remzi/OSTEP/dist-nfs.pdf

FILE TRANSFER PROTOCOL (FTP) is the most common and widely used network protocol for file sharing on the Internet. All major operating systems use this protocol. FTP is not very secure in its native format, since it uses clear (unencrypted) text for the sign-in process and data stream transmission. However, there are more secure forms of FTP available. The two main Secure FTP extensions are:

- **FTP FOR TRANSPORT LAYER SECURITY (FTPS)** adds support for the transport layer security and secure sockets layer (SSL). Both sign-in and data transmissions, or just the data transmission, can be encrypted.
- **SECURE SHELL FILE TRANSFER PROTOCOL (SFTP)** is an extension of the SSH network protocol developed by the Internet Engineering Task Force that is commonly used by districts to securely transmit a file over the Internet.

http://www.w3.org/Protocols/rfc959/

http://www.coviantsoftware.com/what-is-secure-ftp.php

COMMON INTERNET FILE SYSTEM (CIFS), an open protocol based on an enhanced version of Microsoft Server Message Block (SMB), is a standard way that computer users share files across intranets and the Internet. CIFS enables collaboration on the Internet by defining a remote file-access protocol that is compatible with the way applications already share data on local disks and network file servers. This protocol is optimized to support slower speed connections. CIFS is commonly used in districts to share between different operating systems, such as Apple OSX, Microsoft Windows and Novell Netware.

http://technet.microsoft.com/en-us/library/cc939973.aspx

WEB DISTRIBUTED AUTHORING AND VERSIONING (WEBDAV) is an extension of HTTP used to transfer files to and from web servers. Districts commonly use WebDAV because it can look like a native file share to the client operating system even though the destination could be a file store on the Internet. Since it isn't a local file store, latency can be problematic if applications require file access in a short period of time. WebDAV runs on HTTP—an important benefit, since most district proxy servers natively pass traffic on this protocol (port 80/443), so few infrastructure changes are needed to implement this solution.

http://www.webdav.org/

SIMPLE MAIL TRANSFER PROTOCOL (SMTP) is a standard for transmitting email over the Internet. SMTP uses TCP port 25 and 465 (SSL) by default, although other ports can be assigned. Almost all email servers (e.g., Microsoft Exchange, IBM (formerly Lotus) Notes, Hotmail, Gmail, Yahoo! Mail) use SMTP to send and receive email messages from outside their own systems. This protocol was last updated in 2008 by the Internet Engineering Task Force in Request for Comments (RFC) 5321. SMTPS, the secure version of this protocol, uses SSL.

http://tools.ietf.org/html/rfc5321

POST OFFICE PROTOCOL 3 (POP3) is the most recent version of a protocol for email clients, also known as webmail applications such as Gmail, Outlook and Yahoo. POP3 is used to retrieve messages over the Internet using Transmission Control Protocol/Internet Protocol (TCP/IP). These mail applications typically use SMTP only for sending messages to a mail server for relaying. Its most current publication is RFC 1939.

https://www.ietf.org/rfc/rfc1939.txt

INTERNET MESSAGE ACCESS PROTOCOL (IMAP), an enhancement over POP, is another method for email clients to retrieve messages from a mail server over the Internet. IMAP allows multiple webmail clients to connect and manage the same mailbox at the same time while maintaining the status integrity of messages on the mail server. Most webmail applications support both POP and IMAP, which is defined in RFC 3501.

https://tools.ietf.org/html/rfc3501

MULTI-PURPOSE INTERNET MAIL EXTENSIONS (MIME) is an extension of the original Internet email protocol that lets people exchange different kinds of data files—audio, video, images—and application programs on the Internet. This protocol is defined in several publications by the Internet Engineering Task Force, starting with RFC 2045 to RFC 2049.

https://tools.ietf.org/html/rfc2045

Network Infrastructure

Network infrastructure is a vital component of the learning process in school districts. There are more devices supporting a variety of standards and providing a range of services, including Voice over IP (VoIP) communications, security cameras, badge readers, tablets and phones. Access to wired and wireless networks is expected everywhere in schools—with the ability to provide high-performance services in a cost-effective way.

As districts integrate more content from many Internet, social media and video sources into their curriculum, demand on the network infrastructure is increasing. Additionally, with the recent growth in the use of personal devices across all levels in districts, expectations from the infrastructure are high. It is important to address some of the critical standards that must be considered when implementing a wireless or wired network to support a high density and mission-critical environment such as education.

This primer focuses on the technical standards of the network infrastructure. It does not address network design. However, CoSN's **Smart Education Networks by Design (SEND)** initiative provides a robust set of resources to help educators make wise decisions around network design. SEND highlights new and future technologies for network design, offers guidelines and core recommendations for school system chief technology officers, and identifies best practices and resources to assess current and long-term needs for effective network design decisions for school districts. ***http://www.cosn.org/SEND***

Network infrastructure encompasses an array of topics, typically including:

- Local or wide area network (LAN or WAN) telecommunication
- Computer hardware
- Databases
- Security and privacy
- Applications
- Cabling

Data, middleware, people, management systems and more are sometimes considered part of the infrastructure as well.

Network Architecture Standards

IEEE 802.X. The Institute of Electrical and Electronic Engineers (IEEE) is the largest technical association in the world, spanning more than 150 countries and serving more than 350,000 professional members worldwide. The IEEE 802 project encompasses many well-established LAN/WAN/MAN (local area network/wide area network/metro area network) standards that are built on the Open Systems Interconnection (OSI) model. Within IEEE 802, several working groups focus on network protocols and standards. The 802 groups are classified into 25 categories that are identified by 802.XX (802.1 to 802.25). Groups are continually added and dissolved depending on the task.

> School districts must always select from the best and most appropriate national and international standards when determining which path to follow for the network infrastructure and architecture. Such decisions are typically made early on in the design process or when major upgrades to existing infrastructure are about to take place.

The standards covered by IEEE 802 span a wide range of networking areas including architecture, bridging, ethernet, wireless, broadband and others. The most used standards are for the Ethernet family, Token Ring, wireless and virtual LANs. The best known standards include 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth and 802.16 Broadband Wireless.

http://standards.ieee.org/about/get/

Network Encryption Standards

WI-FI PROTECTED ACCESS (WPA) and **WIRED EQUIVALENT PRIVACY (WEP)** protocols are covered in details under the IEEE 802.x family of standards. Due to the tremendous growth in the deployment of wireless devices in school districts, key wireless security protocols and standards are highlighted here.

WEP is an old 802.11 security standard that is considered weak and outdated today, because it used a 40-bit encryption. WPA and, most recently, WPA2, have replaced WEP as more robust security protocols. WPA2 uses an advanced encryption with a 256-bit key, which improves security significantly over WEP. WPA, sometimes called the IEEE 802.11i standard, first became available in 2003. WPA2, sometimes called IEEE 802.11i-2004, followed almost immediately in 2004. In most cases, WPA can be implemented via firmware upgrade.

http://en.wikipedia.org/wiki/IEEE_802.11i-2004

Network Cabling Standards

EIA/TIA-568, a set of communications standards developed by the Electronic Industries Alliance (EIA) and Telecommunication Industry Association (TIA), defines the specifications for design, deployment and management of network/structured wiring systems. EIA/TIA-568 defines cabling specifications for transmitting data, video and voice for U.S. commercial buildings, including the use of fiber-optic cabling and twisted-pair cabling Enhanced Category (CAT) 5, 6, and 7 cabling, which is based on Gigabit Ethernet (IEEE 802.3ab).

http://www.linktionary.com/t/tia_cabling.html

http://www.tiaonline.org/

Network Management Standards

The **ISO FAULT, CONFIGURATION, ACCOUNTING, PERFORMANCE AND SECURITY (ISO FCAPS)** model for network management was established by the International Organization for Standardization (ISO) Telecommunication Management Network organization under the direction of the Open Systems Interconnection (OSI) group. Also known as the OSI/ISO network management model, ISO FCAPS describes a model or framework for network availability, performance and problem identification and resolution. The model focuses on the five areas indicated by the FCAPS acronym:

1. **Network Fault Management**
2. **Network Configuration Management**
3. **Network Accounting Management**
4. **Network Performance Management**
5. **Network Security Management**

It is important to note the difference between FCAPS and ITIL® (formerly known as the Information Technology Infrastructure Library). ITIL defines the organizational structure and skill requirements of an IT organization and a set of operational management practices to allow the organization to manage an IT operation and its associated infrastructure. ITIL was originally created in the United Kingdom under the auspices of the British government. FCAPS is more of a technical network management model, while ITIL (specifically ITIL v3) is more focused on service delivery, improvements and support. It is often recommended that organizations start with FCAPS and then implement ITIL v3 for service improvement.

http://en.wikipedia.org/wiki/FCAPS http://www.iso.org/iso/home.html

http://www.itlibrary.org

Network Security and Privacy Standards

ISO 27001 is considered one of the most important security standards published by ISO. Many organizations seek certification based on this standard, part of a series of ISO standards on information security management system first published in 2005. ISO has published several subsequent guidelines that provide clarifications.

ISO 27001 describes a systematic and holistic approach to information security that allows organizations to manage the confidentiality, integrity and availability of their information systems. The standards encompass people, processes and technology. The standard overlaps with other important privacy standards and allows organizations to meet legal and other regulatory compliance requirements such as the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA) and Payment Card Industry Data Security Standards (PCI DSS) (described below).

The latest version of the 27000 series of standards, ISO/IEC 27002:2013, was published in 2013. This standard outlines potential controls and control mechanisms for effective security management.

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
http://www.27000.org/iso-27002.htm

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS) were created by the PCI Security Standards Council to decrease the potential of fraud with online credit card transactions. Any organization that processes, transmits or stores credit card data must comply with this standard, which is enforced by the credit card brand or bank holder. Compliance is performed annually by a qualified assessor or by self-assessment, depending on the volume of transactions. The standards specify 12 requirements for compliance, including establishing a secured network, encrypted transmission, restricted access to credit card data, access control, security monitoring and maintaining a policy for information security.

https://www.pcisecuritystandards.org/security_standards/

SECURITY AND PRIVACY LAWS

To address privacy and security laws, it is important for districts to implement a comprehensive information security plan to protect the network and information systems from any potential threats. Security plans must include building a robust network infrastructure that adheres to the best industry standards for network connectivity and security.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) is a federal law that sets the standards for student record privacy and confidentiality for all school districts that receive federal funding. FERPA deals directly with education records of students in terms of privacy and security. It gives parents and students the right to inspect and review educational records, request a correction on records if incorrect and decide to whom the records can be released. Network security plays a crucial role in ensuring compliance with privacy and security requirements dictated by this law. FERPA imposes certain requirements on how confidential data is stored and transmitted throughout a network. It also has ramifications on the destruction of data as well as the management of user access to student education records. Additionally, sharing information internally through district systems and externally via websites must be examined against FERPA requirements to avoid privacy violations of staff and students.

http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

CHILDREN INTERNET PROTECTION ACT (CIPA) is a federal law to protect students from accessing offensive content while on school computing systems. It imposes requirements on school systems that receive funding for Internet access or network support from the federal E-rate program. The requirements include establishing an Internet safety policy that defines technology measures to deal with filtering and blocking of inappropriate content, including images and video through emails, chats or Internet.

http://www.fcc.gov/guides/childrens-internet-protection-act

Continued on the next page

CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA) is a federal law that regulates the collection of personal information about children under the age of 13 via websites through school district Internet connections. The law requires that all websites post a clear and comprehensive privacy policy that states the requirement of parental permission before collecting personal information about a student under the age of 13. Personally identifiable information (PII) includes full name, home address, email address, telephone number or any other information that would allow someone to identify or contact a child. COPPA also addresses other kinds of information, such as hobbies and interests collected through website tracking mechanisms such as cookies, that can connect information to an individual.

There are some exceptions to this law that allow a website operator to collect certain identifiable information without parent permission. For example, an operator can collect an email address to provide a notice or seek consent or respond to a one-time request from a child and then delete it. An exception is made for multiple communications of the same type via email with a child in the case of a newsletter subscription. In this case, the operator must notify the parent of such regular communication and allow the parent to opt out if desired.

http://www.coppa.org/

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) is a federal law that regulates individual student health records and other identifiable health information in schools and districts. Although HIPPA seems to overlap with FERPA, since many consider student health records to be educational records, the U.S. Department of Health and Human Services and the U.S. Department of Education require that both laws be applied in districts.

http://www.hhs.gov/ocr/privacy/index.html

CoSN's Protecting Privacy in Connected Learning toolkit is an excellent resource for educators and policymakers involved in decision making related to student privacy issues. The toolkit is organized in the form of a decision tree that addresses FERPA and COPPA compliance and provides smart suggested practices that reach beyond compliance. The toolkit also includes definitions, checklists, examples and key questions to ask.

The toolkit was created with the help of Harvard Law School's Cyberlaw Clinic, which is based at the Berkman Center for Internet and Society, sponsored by Microsoft, and endorsed by the Association of School Business Officials International.

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

Digital Accessibility

School districts are about educating all children regardless of their physical or mental ability. It is important for technology to be accessible to all students with diverse abilities. Digital accessibility standards address a host of impairments that include visual, hearing, physical or learning disabilities.

In many districts, the assistive technology department provides assistance and training to the more severely impaired students through specialized technology and staff. Some students needing assistance are in the low impairment category, requiring lower-level accommodations when it comes to accessing mainstream technology tools for their learning. For example, students with vision impairment should be able to easily enlarge screen size, listen to content or distinguish color for color blindness.

There may be legal implications to districts that do not provide reasonable accommodations to students with disabilities. Several federal laws explicitly address accessibility for information technology—and prohibit any federally funded entity from discriminating on the basis of disability.

Digital Accessibility Laws, Guidelines and Standards

SECTION 508, originally enacted as an amendment to the Rehabilitation Act of 1973, requires federally funded organizations to provide technology that is accessible to people with disabilities. Clarified and strengthened in 1998, Section 508 clearly outlines what the federal government means by accessible electronic and information technology. All federally funded entities must provide disabled members access to information that is equivalent to that of others who are not disabled. This means that information must be accessible in a variety of ways that is specific to each disability. While WCAG (described below) serves as a guideline and includes more details for accessibility compliance, Section 508 consists of requirements.

http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards

WEB CONTENT ACCESSIBILITY GUIDELINES (WCAG) is a series of accessibility guidelines published by the World Wide Web Consortium (W3C). WCAG 1.0, adopted in 1999, consists of 14 accessibility guidelines focused on accessible design of web pages. The guidelines generally apply to content on a web page or web application, such as text, images and sounds, as well as presentation and structure of web pages.

WCAG 2.0, published in 2008, consists of 12 guidelines with a more comprehensive focus on accessibility. These guidelines address issues such as text alternatives for non-text content, captions for multimedia, full functionality via a keyboard, ease of navigation and easier ways to see and hear content.

http://www.w3.org/WAI/WCAG20/glance/

http://www.w3.org/WAI/intro/wcag.php

W3C also has developed the **WEBSITE ACCESSIBILITY CONFORMANCE METHODOLOGY (WCAG-EM)**, an approach to conformity to WGAC 2.0.

http://www.w3.org/WAI/eval/conformance

ACCESSIBLE PORTABLE ITEM PROTOCOL (APIP) standard, discussed on page 5 under the IMS Global standards, allows digital tests and test items to be ported across item banks. APIP also provides an interface to make tests and items accessible by students with disabilities.

ACHECKER is a tool that reviews accessibility of single web pages for conformity to number of standards and guidelines, including WGAC 2.0 and Section 508.

http://achecker.ca/checker/index.php

More recently, accessibility is being addressed as a **UNIVERSAL DESIGN FOR LEARNING (UDL)** question. In other words, content is made available in multiple formats to address all the needs and preferences of all learners. Spearheaded by the Center for Applied Special Technology (CAST), UDL is a framework for curriculum design that addresses learners with diverse abilities to provide equal opportunities for learning. UDL provides a blueprint for creating instructional goals, methods, materials and assessments that work for everyone—not a single, one-size-fits-all solution but rather flexible approaches that can be customized and adjusted for individual needs. While UDL is not a technically defined as a standard, it does provide principles and guidelines that can be used to assess and evaluate materials.

http://www.cast.org/udl/index.html

NATIONAL INSTRUCTIONAL MATERIALS ACCESSIBILITY STANDARD (NIMAS) is a technical standard used by publishers to produce source files that may be used to develop multiple specialized formats (such as Braille or audio books) for students with print disabilities.

The source files are prepared using XML to mark up the structure of the original content and provide a means for presenting the content in a variety of ways and styles. For example, once an NIMAS fileset is produced, the XML and image source files can be used not only for printed materials, but also to create Braille, large print, HTML, Digital Accessible Information System (DAISY) digital talking books using human voice or text-to-speech, audio files derived from text-to-speech transformations, and more.

http://www.education.nh.gov/instruction/special_ed/nimas.htm

INTEROPERABILITY GOVERNANCE

IT interoperability and standards have become a strategic issue for technology leaders and school districts. In a technology environment where cloud computing, virtual servers, desktops and mobility are transforming learning and the working of districts, the demand for a more strategic approach to interoperability for the whole organization is becoming increasingly important.

At the heart of interoperability is the ability for all systems and platforms to work together and deliver services seamlessly and efficiently across the district. When systems work well together, so will the organizational ability to collaborate, deliver services, cut costs, improve system security and privacy, drive transformation and serve customers efficiently.

However, to achieve effective interoperability, districts must first identify and agree on a set of standards and specifications that should define what is acceptable when procuring systems and platforms. In other words, there must be a governance model established by the whole organization to manage interoperability strategically.

There are inherent efficiencies for adopting interoperability standards. The most significant is the impact on teachers and students. Using open and adaptable standards provides them with access to current content and curriculum resources, and ensures continued access if the technology delivery platform or the learning management (LMS) system change over time. Such changes should not result in loss of access for students or teachers. An additional benefit could be fiscal savings to districts. If content can be easily moved among systems, this means less cost and loss of productivity for staff.

When K–12 content providers each deliver digital material in their own proprietary formats, teachers, students, parents and district administrators encounter significant challenges. Managing data in multiple locations creates additional IT management cost, user access complexity and user experience problems—and it limits or eliminates the possibility of personalizing learning and data-driven decisions. Lack of standardization also poses a challenge to vendors who have to integrate other content into their platforms by investing in creating one-time APIs that can't be replicated for other customers.

> There must be a governance model established by the whole organization to manage interoperability strategically.

Developers of open standards strive to provide universal language for digital integration so that all content, activities, assessments, practices and data associated with digital resources can be accessed in a single, content-agnostic platform. The significance of open standards integration packages is that they are non-proprietary, meaning that platform or management systems remain open to multiple sources of digital resources and vendors. The integration scripts are reusable with other platforms or LMS. Districts that adopt open interoperability standards retain their right to replace an LMS or platform without losing all the content integrations they have built with content providers over the years. Digital interoperability standards allow purchased or developed content to be reintegrated into a new platform.

Teachers, students and parents can access day-to-day student activities and performance data, enhancing their ability to intervene or adjust their strategies in a timely fashion. Learners benefit from choices or and access to different formats for a given topic, such as audio, visual or written data; organizers, case studies and projects; languages, Lexile levels and other accommodations needed or desired. Districts and schools retain their right to replace or change their LMS without losing digital content. Digital content providers need to build only one integration package, which can be reused in other LMS or platforms.

CASE STUDY

Interoperability Governance at Houston ISD

Houston Independent School District (ISD) is the largest school district in Texas and the seventh largest in the United States, with more than 215,000 students and 283 schools. Located in southeast Texas, the district serves the city of Houston and several nearby communities. Houston ISD prides itself on providing students with rigorous academic courses designed to prepare them for college and meaningful careers.

THE CHALLENGE. Houston ISD purchases instructional resources from more than 200 different content and tools providers. In addition, the district wants to leverage the collective knowledge and experience of its best teachers by supporting their ability to develop content. To make all of this content and tools available to teachers, students, parents and administrators, Houston ISD needed a platform that could house all curriculum planning guides, content and tools.

Like other K–12 districts, Houston ISD has taken a stand on students' right to effective and even transformational use of technology in teaching and learning environments, so students can be prepared for the careers and/or college degrees of their choice. This means that students must have the ability to choose the content and tools that best suit their learning needs and preferences, with teachers, parents and administrators providing guidance in support of these choices and needs. In addition, students, teachers and parents should be able to access user and performance data in one single platform. This situation forced the district to reconsider how it purchases, produces and delivers content, and which digital communication, collaboration and productivity tools it needed.

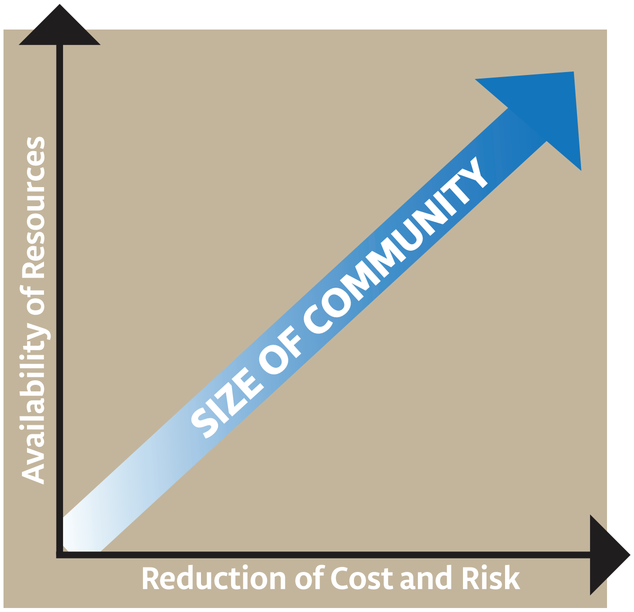
THE SOLUTION. Before making decisions, Houston ISD learned that some curriculum, content and learning management systems (platforms) are compliant with digital content interoperability standards—and some were not. The same is true of digital content providers. This difference determines whether or not a platform can provide, in a single location, searchable and discoverable content from multiple sources, from a large number of content producers, in a wide range of formats to accommodate learners' interests, preferences and needs. This is a critical component for personalized instruction.

To meet this vision, Houston ISD chose a platform compliant with IMS Global digital content interoperability standards. The district also:

- Announced to all its vendors and partners that it now requires Common Cartridge, Thin Common Cartridge, and/or LTI and QTI integrations, depending on the best fits for each adopted digital material.
- Provided informational sessions about digital content interoperability for district leaders and procurement staff
- Modified its instructional materials purchasing process. Every digital content or resource, no matter who the purchasing agent is in the district, goes through the scrutiny of a digital content interoperability standards committee, which determines the ideal type of integration required, based on the nature of the digital material, before the contract goes through the procurement and legal departments.

LOOKING AHEAD

There is no one-size-fits-all approach to realizing the benefits of standardization. The development of robust, reliable industry standards is a complex and time-intensive process involving costs as well as benefits. How do you know when a set of interoperability standards is worth adopting?



To some degree your decision should be based on a realistic assessment of the maturity and empirical support for any standard. The more mature the approach or standard, the more likely it is to have support in the form of a community of practitioners, available documentation, examples, training and a pool of skilled staff members. On the other hand, a newer standard may be supported by enthusiastic pioneers and offer professional development and collaboration opportunities that compensate for the lack of industry maturity.

Even more important is determining how well the standard meets your needs. Will adopting it enable a critical user activity or high-priority enterprise capability? Will it lower costs, shorten development time or facilitate the maintenance and evolution of crucial systems? If the need is there, then carefully researching the different options to invest in products and approaches that support a chosen standard will be well worth the time.

With the rising importance of cloud computing, online learning, portals, modularity, data warehousing and performance management, interoperability standards have become more crucial than ever before. As the IT world shifts from a product-oriented to a service-oriented environment and schools struggle to make ends meet, it is essential for K–12 technology leaders to learn how to maximize the benefits of existing enterprise systems while adding new solutions that are cost-effective and scalable. None of this is possible without interoperability.

REFERENCES

DIGITAL CONTENT AND INTEROPERABILITY STANDARDS

Common Cartridge (CC)
www.imsglobal.org/commoncartridge.html
www.imsglobal.org/digitallearningservices.html

Diagrams:
Common Cartridge
Common Cartridge Content Hierarchy
Learning Tools Interoperability

Question and Test Interoperability (QTI)
http://www.imsglobal.org/question/

Accessible Portable Item Protocol (APIP)
http://www.imsglobal.org/apip/

Learning Tools Interoperability (LTI)
http://www.imsglobal.org/toolsinteroperability2.cfm

Sharable Content Object Reference Model (SCORM)
http://www.adlnet.gov/scorm/

SCORM Content Agreement Model (CAM)
http://www.adlnet.gov/scorm/

DATA CONNECTIVITY STANDARDS

Open Database Connectivity (ODBC)
msdn.microsoft.com
http://www.simba.com/odbc.htm

Java Database Connectivity (JDBC)
http://docs.oracle.com/javase/tutorial/jdbc/basics/

ActiveX Data Objects (ADO)
https://msdn.microsoft.com/en-us/library/aa286484.aspx

Object Linking and Embedding Database (OLE DB)
https://msdn.microsoft.com/en-us/library/ms722784(VS.85).aspx

DATA INTEGRATION STANDARDS AND TOOLS

Common Education Data Standards
http://ceds.ed.gov/

Ed-Fi Alliance
http://www.ed-fi.org/

Learning Information Services (LIS)
http://www.imsglobal.org/lis/

School Interoperability Framework (SIF)
https://www.sifassociation.org/

Enterprise Service Bus (ESB)
http://en.wikipedia.org/wiki/Enterprise_service_bus

IDENTITY MANAGEMENT STANDARDS

Shibboleth
shibboleth.internet2.edu/

Lightweight Directory Access Protocol (LDAP)
www.tech-faq.com/ldap-lightweight-directory-access-protocol.html

OpenID
http://openid.net/foundation/

PORTAL AND PORTLET STANDARDS

Java Specification Request (JSR) 286
jcp.org/

Web Services for Remote Portals (WSRP)
www.oasis-open.org/committees/wsrp

FILE SHARING STANDARDS

XML for Analysis (XMLA)
http://www.xml.com/

Network File System (NFS)
http://pages.cs.wisc.edu/~remzi/OSTEP/dist-nfs.pdf

File Transfer Protocol (FTP)
http://www.w3.org/Protocols/rfc959/
http://www.coviantsoftware.com/what-is-secure-ftp.php

Common Internet File System (CIFS)
http://technet.microsoft.com/en-us/library/cc939973.aspx

Web Distributed Authoring and Versioning (WebDAV)
http://www.webdav.org/

Simple Mail Transfer Protocol (SMTP)
http://tools.ietf.org/html/rfc5321

Post Office Protocol 3 (POP3)
https://www.ietf.org/rfc/rfc1939.txt

Internet Message Access Protocol (IMAP)
https://tools.ietf.org/html/rfc3501

Multi-Purpose Internet Mail Extensions (MIME)
https://tools.ietf.org/html/rfc2045

NETWORK ARCHITECTURE STANDARDS

IEEE 802.x.
http://standards.ieee.org/about/get/

NETWORK ENCRYPTION STANDARDS

Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP)
http://en.wikipedia.org/wiki/IEEE_802.11i-2004

Network Cabling Standards
EIA/TIA-568
http://www.linktionary.com/t/tia_cabling.html
http://www.tiaonline.org/

NETWORK MANAGEMENT STANDARDS

ISO Fault, Configuration, Accounting, Performance and Security (ISO FCAPS)
http://en.wikipedia.org/wiki/FCAPS
http://www.iso.org/iso/home.html
http://www.itlibrary.org

NETWORK SECURITY AND PRIVACY STANDARDS

ISO 27001
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
http://www.27000.org/iso-27002.htm

Payment Card Industry Data Security Standards (PCI DSS)
https://www.pcisecuritystandards.org/security_standards/

SECURITY AND PRIVACY LAWS

Family Educational Rights and Privacy Act (FERPA)
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Children Internet Protection Act (CIPA)
http://www.fcc.gov/guides/childrens-internet-protection-act

Children's Online Privacy Protection Act (COPPA)
http://www.coppa.org/

Health Insurance Portability and Accountability Act (HIPAA)
http://www.hhs.gov/ocr/privacy/index.html

DIGITAL ACCESSIBILITY LAWS, GUIDELINES AND STANDARDS

Section 508
http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards

Web Content Accessibility Guidelines (WCAG)
http://www.w3.org/WAI/WCAG20/glance/
http://www.w3.org/WAI/intro/wcag.php, http://www.w3.org/WAI/eval/conformance

Universal Design for Learning (UDL)
http://www.cast.org/udl/index.html

National Instructional Materials Accessibility Standard (NIMAS)
http://www.education.nh.gov/instruction/special_ed/nimas.htm

COSN TECHNICAL COMMITTEE

John Alawneh
Chair
Chief Information Officer
Katy Independent School District (TX)

Steve Langford
Co-chair
Chief Information Officer
Beaverton School District (OR)

Dan Armstrong
Assistant Superintendent for Technology Services
Plano Independent School District (TX)

L. Beatriz Arnillas
Senior IT Manager, Instructional Technology
Houston Independent School District (TX)

Joe Christoffersen
Director, Technology Operations
Katy Independent School District (TX)

Bob Collie
Private-sector Liaison
Vice President
Education Networks of America

Gisela Field
Administrative Director, Assessment, Research, and Data Analysis
Miami-Dade County Public Schools (FL)

Jorge Fernandez
Executive Director, Client & Business Services
Miami-Dade County Public Schools (FL)

Luke Fox
CoSN Board Member Liaison
Executive Director of Information Technology
Richland County School District One (SC)

Ricardo Garmendia
Manager, IT Customer Services/Print Shop
Renton School District (WA)

Karin Holz
Director, Business Development and Sales, Public Schools
InfoSnap, Inc.

Jamey Hynds
Director, Business Intelligence
Katy Independent School District (TX)

Tom Ingram
Director, Information Technology
Escambia County School District (FL)

Mike Jamerson
CoSN Board Member Liaison
Director of Technology
Bartholomew Consolidated School Corporation (IN)

Keith Krueger
CoSN Staff Liaison
Chief Executive Officer
Consortium for School Networking

Ron Mayberry
Executive Director of Instructional Technology
Federal Way Public Schools (WA)

Judith "Kristy" Oran
Educational Specialist
Technology Express

Darlene Rankin
Director, Technology Innovations
Katy Independent School District (TX)

Steve Smith
Chief Information Officer
Cambridge Public Schools (MA)