Effective Social Learning for K12

Finding the Right Balance Between Security and Collaboration to Reach Today's Students

September 2011

Introduction

In recent years, social media in all of its forms has captured the world's attention. Tools such as blogs, wikis and online communities have made online communication and collaboration a daily activity for hundreds of millions of people, students included.

In turn, schools are now leveraging social media tools to engage their classrooms, enriching traditional teaching methods and building the communication and collaboration skills students need for 21st century success. According to the U.S. Department of Education, "21st century competencies and such expertise as critical thinking, complex problem solving, collaboration, and multimedia communication should be woven into all content areas [for education]"[1] For schools facing budget constraints, many collaboration tools can even help cut costs.

Having pushed collaboration to the forefront, consumer offerings like Facebook and Google Docs have taught us that collaboration tools for classroom use must be modified and appropriately managed in order to ensure safety that meets local, state and federal educational standards. A recent study by Columbia University found that the privacy settings of many consumer-based social networks are "fundamentally flawed and cannot be fixed."[2]

Leveraging social media tools for K12 education creates a unique tension between true collaboration and student safety—a tension not found in the context of ordinary consumer tools. How do we bring students into an online network for authentic collaboration while adequately protecting student information and staying compliant with federal child safety regulations? There is no "one size fits all" solution to this problem, and security technology by itself cannot act in a vacuum to solve it. Security technology must be used as a means to an end and implemented with the flexibility that schools need to extend their real-world policies for student safety into a digital environment.

In this respect, most of today's education technology companies miss the mark. Companies heavily promote collaboration capabilities (many of them offered for "free") while obscuring the issue of security with ambiguous, unsubstantiated claims of "safe and secure." The noncommittal language even extends into their Terms of Service agreements. One company's privacy policy openly states, "…we cannot and do not guarantee that Content you post on the Website will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Website."[3]

Online security cannot be a gamble—it's an important issue for student safety and is required by federal law in the Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), and Children's Internet Protection Act (CIPA). Proper security needs to be in place to protect students from risks such as predators, bullying and having their still-developing views used against them now and in the future. Schools that implement solutions that lack adequate security run the risk of possible lawsuits from angry parents as well as losing their E-Rate funding.

This paper lays out the major components of online security—all of which must be required in cloud-based educational technologies. It then explains how ePals extends these components throughout a flexible, safe and secure, policy-managed environment that schools can then govern with their own real-world rules and policies for safe and authentic collaboration.

Components of Security

In order to fully understand the security issues facing classrooms, it is important to first establish the main components that make up online security. The following list establishes a good base level:

Firewalls – Firewalls act to protect the physical perimeter of a network from outside threats. This acts much like a security guard keeping unauthorized people out of a restricted area.

Encryption – Data stored on a network can be converted into code using a digital key in order to protect the data from unauthorized users. Many people have encountered encryption when doing such tasks as online banking.

Authentication – This type of security usually relates to ensuring that the people entering the network are authorized users. Assigning each person a username and password, similar to measures taken for consumers making online purchases, is a typical form of authentication.

Domain-based Security – As the name implies, this can pertain to the security of a domain or website. This is important for schools that access their networks or cloud-based applications through a main website portal. Many people have enacted their own form of domain-based security at home by setting a WEP key to secure their wireless network.

Capabilities Security – Covering a wide range of applications, the most popular measures include: spam filters, virus protection, and content filtering for inappropriate language. Most people have encountered these when using web-based email accounts.

Information Security – This covers the way information is stored and protected in a network. The International Organization for Standardization (ISO) has set important standards for information security to protect the privacy of users.

Each of these security initiatives plays an important part in protecting a network, but no one technology can act effectively alone. For example, a number of products in the education market employ authentication as the only security measure. This means that simply acquiring a user name and password gets someone inside the community walls, with unfettered access to any of its members. Some companies couple authentication with content filters for message traffic. But in a school context where teachers, parents and students of varying age groups regularly communicate, a universally applied filter will either be flooded with false positives, or set to insufficient protection. When authentic collaboration in either scenario cannot succeed, none of the individual measures are sufficient. This approach makes compliant collaboration all but impossible.

All of these security measures must not only be in place—but also work in concert with each other in a holistic manner that recognizes the unique communication requirements for students vs. parents vs. teachers. This is because each person within the system plays a different role. For online security to genuinely work for schools, the technology must understand the role of each person as well as the school policies that apply to that person. This is not just important for compliance with federal regulations—it is fundamental to a context where collaborative learning can thrive.

ePals Policy-Managed Security

ePals starts by integrating all of the listed security measures into its cloud-based solutions, recognizing that this should only be the beginning. Independently, these technologies only work at the perimeter to keep unauthorized people out of the network—much like a school safety officer works to keep unauthorized people out of a school building. But what happens if an unauthorized person has already made his way into the network? What if a student from within the system is using the technology to try and harm others? What happens when schools want to let certain people into the network, such as parents or international students collaborating on group projects? Should third graders be treated differently than high school students when safety and privacy are involved?

In the physical world, schools have policies in place to handle these situations, but most technology solutions have a hard time replicating such policies in the digital context. Nonetheless, online security without real-world policies creates an all or nothing scenario. For collaboration and security to coexist in an effective, meaningful way, schools need a more sophisticated solution that recognizes and allows for real-world dynamics.

Policy Management

Based on more than 10 years in the industry experience evaluating the ways in which students, educators and parents interact, ePals has created a patent-pending policy management solution that successfully brings these real-world policies into the network, not only at the edge, but throughout the entire system. Using this solution, schools have the ability to implement their own unique policies to meet their needs. Indeed, a Christian elementary school in Pennsylvania might have very different policies than a public high school in Northern California.

It starts with role-based permissions: ePals assigns each user a role within the network such as student, teacher or parent. The system then goes further to apply real-world relationships between users. For example, Nancy is a student at Centennial Elementary. While her role is "student," her relationship might be "third-grade student in Ms. Kay's class." Ms. Kay's role is "teacher," but her relationship might be "teacher to Nancy at Centennial Elementary." Jane might have the role of "parent," but her relationship is "Nancy's mom." There could also be a fellow third grade "student" from across the district with the relationship of "Nancy's collaboration partner in the district-wide science fair."

Accounting for real world-relationships is vital to security, as the role people have within a network may stay the same, but their real-life relationships are constantly changing. For example, changes may occur with respect to Jane's parental rights. Teachers' relationships to specific students change each year as students advance a grade.

Just like the physical world, ePals' policy management can account for dynamic relationships and automatically apply school policies—in any of these scenarios—at the appropriate enforcement point. The ePals solution even recognizes the difference between incoming and outgoing communications as they pertain to a user, and outcomes of actions will differ depending on sender and recipient roles and relationships. If Ms. Kay sends an email to Nancy, a content filter might be enacted to check the appropriateness of the email, while an email Ms. Kay receives from another teacher would not. Similarly, ePals can determine if the source of the email is inside or outside of the district and apply an appropriate action. For example, an email from an eMentor outside the district might get monitored by Ms. Kay before it reaches Nancy.

ePals makes it easy for users to know their rights and restrictions by assigning each user policy badges—similar to parental controls used on popular Internet sites—that explicitly state what a user can and cannot do based on their roles and relationships within the network. Just like parental controls, policy badges also serve as a deterrent, enforcing school context-appropriate behavior.

Real-world Deployment

Policy management is the necessary first step toward ensuring that collaboration tools safely account for the community's complex dynamics. But just as the architecture allows for relationships in the real world, the technology's implementation must account for deployment in the real world. The solution needs to be efficient and effective for teachers, enhancing the classroom rather than burdening it with additional maintenance. The solution has to let teachers manually control the parts they need to—e.g. restrict permission levels on demand for a suddenly insubordinate student—and automatically manage the parts they do not. With technologies such as hierarchical controls and system automation, the ePals solution is designed for both comprehensive security and easy, everyday use.

Hierarchical Controls

Working with ePals through a simple step-by-step process, a district sets overarching policies for the network during the initial system implementation. But just like in real life, educators have the ability to make a policy more stringent at the school, classroom, group or individual level. For instance, the district may set a policy that elementary school students can communicate and collaborate with each other throughout the district. James, a sixth-grade student, is sending emails teasing students in Ms. Kay's class. The ePals solution gives Ms. Kay the ability to change the policy to keep James from communicating with her students. By enabling hierarchical controls, teachers can keep the same authority over student behavior as in the physical classroom, while also having the same abilities to encourage learning and collaboration.

Hierarchical controls can also enhance collaboration by allowing teachers to create customized learning environments that help keep students focused on the subject matter at hand. Teachers can enhance classroom curriculum by setting up temporary or permanent policy-managed collaboration groups to get students discussing a topic or working through a problem. The technology can also give students the opportunity to use several forms of social media on assignments—such as wikis, and blogs—to keep students engaged even after normal school hours.

Automation and Auto-population

While policy-managed security offers unique depth and flexibility, little additional work is needed on the part of educators and school administrators to make the solution work. This is accomplished through sophisticated system automation that is able to take real-world changes to policies and automatically enforce them, in real-time, throughout the network.

For example, if a policy is in place that says elementary school students cannot communicate with high school students, the system will automatically enforce this. If the policy is changed to allow Nancy to communicate with her brother who attends high school, the system automatically makes the policy change and enforces it without the need for further human intervention.
This same automation technology also stimulates collaboration by auto-populating a user's contact list with all the people with whom they are allowed to communicate. As policies change, the ePals solution automatically adds and deletes contacts as necessary to comply with the new policies. This saves teachers valuable time by making sure each student has the contacts they need for group discussions without the need to compile the information themselves.

Commitment to Service

An education technology company's accountability for service is also significant to student safety. ePals is committed to providing high levels of service to schools and districts, and to ensuring that schools can trust ePals to maintain school policies and student privacy throughout the entire learning experience. This means creating a safe and secure educational ecosystem that applies the same school policies across all email communications and social media interactions, and obtaining third party verification to prove it.

Terms of Use Agreements

One of the best ways to initially discover a company's commitment to accountability is to carefully read its Terms of Use or Terms of Service agreements. Unfortunately, many education technology companies drastically limit their commitments to liability as mentioned earlier in the paper. For example, one company's Terms of Service state, "You will indemnify and hold Company, its parents, subsidiaries, affiliates, officers, and employees harmless (including, without limitation, from all damages, liabilities, settlements, costs and attorneys' fees) from any claim or demand made by any third party due to or arising out of your access to the Services [or] use of the Services."[i] Some consumer offerings go so far as to hold the school or district liable to the company for such breaches in security. This is a major distinction between products that are made available for free, and products that are premium (even as many premium offerings are eligible for substantial subsidies by E-rate).

ePals stands behind its technology and acts as a partner with schools and districts. The company works closely to help districts choose and integrate policies into the system during implementation and then works with the schools to monitor the system for potential problems. If a problem arises, ePals provides comprehensive support to quickly resolve the issue.

Third Party-Verified Privacy

Providers that take student safety seriously understand that when schools and districts do their due diligence, they need more from collaboration products than a face value claim of privacy. Online privacy verification vendors like TRUSTe provide services that help schools identify the vendors that employ the highest standard of online privacy practices. Every product ePals has released has undergone a rigorous TRUSTe Certification process and obtained verification of its privacy protocols, making ePals one of the only collaboration platform providers in the education space to earn TRUSTe Certification. The TRUSTe badge is published across the ePals' suite of websites, so schools and districts can easily identify that ePals security measures stand apart as vetted and compliant.

Conclusion

As school administrators assess educational technologies for the classroom, they must take into account the security measures of each solution in order to provide privacy for students now and into the future. When evaluating cost, administrators should consider "total cost of ownership," not just licensing.[5] Where some products offer "free" user licenses, the school can end up shouldering a tremendous amount of the work to configure the product for the educational environment, deploy it across the district, maintain it over a period of years and obtain necessary services with respect to use. This can substantially increase the total investment well beyond the cost of education-specific technologies.

Our experience has shown that the best results occur where schools ask six vital questions when assessing a communication or collaboration product:

1. Can real-world policies be implemented into the technology?
2. Can the technology's security decipher real-world relationships?
3. Does the solution automate actions to save districts and schools valuable time?
4. Does the company stand behind its solution?
5. What is the total cost of ownership?
6. Is the solution compliant with education-based regulations?

By answering these questions during the discovery period, schools and districts can save valuable time and effort, and ensure that students are properly protected while staying in compliance with state and federal requirements. Perhaps most important, however, is the question of whether the solution integrates elements that aid its use and adoption by educators and students for learning purposes. Too often, social learning technologies merely shift the burden on an already overburdened staff to "make the tool useful," largely defeating its purposes.

Resources:

[1]"Transforming American Education: Learning Powered by Technology," by U.S. Department of Education: http://www.ed.gov/technology/netp-2010

[2]"The Failure of Online Social Network Privacy Settings," by Michelle Madejski, Maritza Johnson, and Steven M. Bellovin: http://academiccommons.columbia.edu/catalog/ac:135406

[3]Edmodo Privacy Policy: http://www.edmodo.com/corporate/privacy-policy

[4]Edmodo Terms of Service: http://www.edmodo.com/corporate/terms-of-service

[5]"A Holistic View of the Total Cost of Technology," by Rich Kaestner: http://www.cosn.org/Initiatives/ClassroomTotalCostofOwnership/CoSNResources/tabid/5120/Default.aspx

"Social Networking Sites and Teens," by Amanda Lenhart and Mary Madden: http://www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens.aspx

International Society for Technology in Education (ISTE): http://www.iste.org/AM/Template.cfm?Section=NETS

Project Tomorrow: http://www.tomorrow.org/speakup/speakup_reports.html

Children's Online Privacy Protection Act (COPPA): http://www.ftc.gov/ogc/coppa1.htm

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

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

TRUSTe: http://www.truste.com/privacy_seals_and_services/enterprise_privacy/childrens-online-privacy-seal.html

Appendix: Security Comparison Checklist

Collaboration and Communication Features[ii]	Free Consumer Solutions*	Edu-Tech Companies°	ePals Solution
SAFETY/POLICY MANAGEMENT			
Safe for Students under 13 Easy, automated COPPA, CIPA, FERPA compliance	⛔	⚠	✚
Group and Role-based Policies and Controls Granular ability to set and delegate access controls, policies and outcomes by role and group	⛔	⚠	✚
User-Specific Content Filtering and Moderation	⛔	⚠	✚
LEARNING INFRASTRUCTURE			
Highly Collaborative Ability to connect locally or globally with other learning networks	⛔	⛔	✚
DEPLOYABILITY			
Enterprise-Grade Services, Training and Support More than just a "self-service" option	⚠	✚	✚
Infrastructure Flexibility Including support for LAN for local access as well as multiple cloud deployments	⛔	⚠	✚
Automation and Auto-population Integrates with Student Information Systems, applies "discoverability" matrix	⛔	⚠	✚
SERVICE COMMITMENT			
Contracting Provides meaningful Service Level Agreements	⛔	⚠	✚
3rd Party-Verified Privacy TRUSTe Certified	⛔	⚠	✚

* Mass-market consumer email and social media offerings not specifically designed for education
° Products from current companies geared for K-12 use

✚ **Rich, flexible capabilities, customized and set by the school/district**

⚠ **Limited/inflexible capabilities**

⛔ **Little to no capability**

[1] Based on ePals research and customer feedback as of July 2011.