EdTekWhitePaper

Building and Keeping a Positive Digital Identity

A Practical Approach for Educators, Students and Parents

June 2015

Overview

Students around the world are becoming increasingly connected and dependent on technology for communication, information and learning. According to FutureSource, 26.6 million mobile computers, including 11 million tablets were purchased in 2014, a 16 percent increase over 2013. This surge of mobile devices in K-12 environments means students are increasingly going online for learning, collaborating and connecting. In the digital age, myriad day-to-day activities have an online component, from how we consume information to how to motivate and monitor our physical activity.

Each and every time we connect, we engage in some way that creates our online identity, our profile, our persona. And it happens automatically and too often without a lot of forethought about the identity that will be created.

Many educators are savvy about the way they engage in a digital environment. They know not to post inappropriate content. They know that sharing passwords with friends is never a good idea. They know how to run frequent checks to ensure their identity hasn't been compromised.

However, as learning becomes more digital, educators at all levels are instrumental in building students' understanding about how technology impacts both their personal and future professional lives. Educators are also instrumental in helping students develop lifelong habits to create and maintain a positive online identity. This white paper outlines practical and easy-to-adopt behaviors all educators can incorporate into instruction.

What is expected of today's digital citizens?

Students are, for the most part, growing up in this digital world without any explicit or universally adopted rules about how to behave, and there is little guidance available to adults. As our digital connections and interactions grow, the lines between our education and personal lives, our career and private activities, become blurred.

Building and protecting your online identity is a critical first step. For teachers, this means understanding, advocating and modeling appropriate online behavior to help students effectively navigate this complicated landscape as well. Standard 4 of the ISTE Standards for Teachers describes how critical this step is.

Because adopting safe, legal and ethical behaviors is essential to living and learning online, this mindset is also featured across all five sets of the ISTE Standards, which are flexible enough to play a pivotal role in developing these new behaviors. These standards can be used to help guide educators and other stakeholders as they consider their approach to appropriate online behavior within their personal and professional lives. The guidance and approach outlined in this paper applies the ISTE Standards and provides educators with a simple yet effective way of understanding the steps for building and maintaining a positive online identity.

Essential questions when building digital identity

As technology and digital content become increasingly common in classrooms around the world, it is critical that educators take steps in their personal practice, as well as in daily classroom routines, to ensure that students build and maintain positive online identities.

There are five essential questions that provide a framework for thinking about digital identities whenever and wherever students are online. With these questions, educators can kick-start meaningful conversations about online behavior, help students understand the broader impact that online identity can have in their daily lives, and provide a foundation of understanding for adopting appropriate online practices:

1. What information am I sharing?

Consider what you post. You can't always trust others to treat your social media posts and text messages the way you want them to. When posting anything online, make sure you read it twice. If there's any question in your mind as to how this will impact yourself or others, sleep on it. While there can be exceptions, once that item is out there, you've lost any control over it and can't take it back. ISTE author Mike Ribble outlines a four-step process in his

book *Digital Citizenship in Schools*: Stop to collect your thoughts; think through the message to ensure it's accurate and truthful; empathize and imagine how the post will be interpreted; and post.

Check your online profile regularly. As the character Alastor "Mad-Eye" Moody in the Harry Potter books advised, "be ever vigilant." Set a time to check your profile online on a regular basis. Search yourself on several different sites and search engines, including Google and Bing, to get different results. The best way to protect yourself is to see how others see you.

Personalize your settings. Take time to make sure you know how to use the privacy and location settings for the various social media tools you use. Many social networking apps make it easy to find friends at the mall or movies. These same location finders reveal your location to anyone else on your network. Make sure the apps you use aren't broadcasting information you don't want shared with people you don't know.

2. How secure is it?

Make strong passwords. A good, strong password is the first and best defense to protecting your data and personal information. Come up with passwords that don't use information available in online databases or public records. Security questions like "What town did you grow up in?" or "What is your mother's maiden name?" can now be found easily in some basic searches. Identify a word/number/special character to use for these answers. Make sure it is something that you will remember and does not relate to something widely known in your life.

Change passwords regularly. Get into a habit of regularly changing passwords. Come up with a plan for which password scheme you are going to use (something that you will remember, but is not meaningful to others) and continue that process as you update your systems. Never allow your browser to store passwords or allow websites to remember your username and password.

Lock devices and close applications when they are not in use. Always close documents and applications when you are not using them. Lock your computer, tablet and smartphone when not in use.

3. Whom am I sharing it with?

The "front page" rule. When considering what information you share online, a good rule of thumb is to imagine it appearing on the front page of the newspaper or on everyone's home page. If you don't want to see it there, don't share. This rule applies to all forms of communications.

Need-to-know basis. Think before you share information with someone. Does this person(s) really need to know this? Retailers often ask for email addresses at the checkout counter. Stop to learn how your information will be used. Consider setting up a separate email that is not linked to any of your primary data for these types of activities

Consider secondary uses. When sharing your information with someone, don't assume you can trust them or that they won't share the information with others. Pause and think about how they might use your information: who will they share it with and how? You'd be surprised how far information can travel.

Open networks are not secure networks. Turn off the "automatically connect" feature on devices. When in a free Wi-Fi zone, take the extra step to obtain a password to connect over a secure network as opposed to accepting a "hot spot." If you must connect to an open network, the front-page rule especially applies here.

4. What am I leaving behind?

Assume that your digital footprint lasts forever. While the delete button does allow you to quickly correct action, even if you delete from the feed, a digital record is stored somewhere and could be uncovered by a super-savvy hacker. Nothing online is ever truly deleted, and things can surface many years later to haunt you. Not to mention others may have downloaded or saved information you had shared. For all purposes, you must assume anything you post online will remain online forever.

Clear your cache. Browsers automatically collect information like browsing history, personal information, and your habits and

The STEP Approach

ISTE author Mike Ribble outlines a simple, four-step process to building a positive digital identity in his book, *Digital Citizenship in Schools*.

STEP ONE

Stop. Take a moment; take a deep breath before posting, texting or sharing. Too often, not taking one's time to post, share or reply can get you in trouble.

STEP TWO

Think. Take time to create the post. THINK is also an acronym that seeks to determine if the information being posted is: True, Helpful, Inspires confidence, Necessary and Kind. If these are the focus points of a message, fewer issues will occur.

STEP THREE

Empathize. Are we interested in others and how they will react? Empathy has us think about the feelings of others, to "walk in another's shoes." Imagine how someone else might interpret your post, tweet or text and how you might feel to receive the message. Consider the Golden Rule– "Do unto others as you would have them do unto you" – before taking action online.

STEP FOUR

Post. If we have been honest and reflected on the other items above, then we can be happy with the post, reply or comment. If young users of social media can begin to learn these skills, they will be better prepared when moving into adulthood.

preferences. Schedule regular times to clear your cache on your devices to clear up history and the stored information. Not only will this make it difficult for anyone to retrace your online steps or access accidentally stored passwords, it will also improve the operation of your device by freeing up memory and improving speed.

5. What are my rights?

Know the law. There are two primary laws to protect students and their data: the Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA). FERPA protects any information that would allow someone to directly identify a student, and COPPA prohibits website operators or other online services from collecting data directly from children under the age of 13.

Review terms and conditions for devices and apps. Mobile apps for smartphones and tablets, as well as most software for computers, collect data about how, when and where you use the product or device. Before you install an app or software, take time to review the terms of service. Look for information about the type of personal information to be collected and how this information will be shared. Most devices and apps allow users to adjust the settings so that you can limit what data is automatically collected.

Some apps actually claim ownership for any content you produce while using them, so the developer can share or sell your property. Even if you close your account, any photos, video, animations or stories you created remain. Read the agreement carefully so you know how your content may be used.

Stay vigilant. Apps and software programs change the terms of service without notification. Stay abreast of the latest changes to privacy and security settings for apps, software and devices.

Data Privacy Policies

FERPA is a federal law enacted in 1974 intended to protect access to student education records and to guarantee parents and guardians access to the records and to have them corrected, if necessary. In particular, FERPA protects any information that would allow someone to directly identify the student, referred to as Personally Identifiable Information (PII). FERPA classifies protected information into three categories: educational information, personally identifiable information and directory information.

Although personally identifiable and directory information are often similar or related, FERPA provides different levels of protection for each. Personally identifiable information can only be disclosed if the educational institution obtains the signature of the parent or student (if over 18 years of age) on a document specifically identifying the information to be disclosed, the reason for the disclosure, and the parties to whom the disclosure will be made. Failure to comply with these requirements will result in a violation of FERPA.

On the other hand, with respect to directory information, FERPA does not bar disclosure by the educational institution. Directory information is defined as "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed." This includes such items as a list of students' names, addresses and telephone numbers, and also includes a student ID number (which includes electronic identifiers) provided it cannot be used to gain access to education records. Directory information, however, does not include a student's social security number, nor can the social security number be used to confirm directory information. Directory information can be disclosed provided that the educational institution has given public notice of the type of information to be disclosed, the right of every student to forbid disclosure, and the time period within which the student or parent must act to forbid the disclosure. If a student decides to "opt out" of the disclosure of directory information, the "opt out" continues indefinitely. Therefore, an educational institution cannot release such information even after a student is no longer in attendance. However, the 2011 revisions to the act prohibit a student from opting out as a way to prevent schools from requiring students to wear an identification card or badge (source: https://www.naceweb.org/public/ferpa0808.htm). An important provision of FERPA is that the school must inform parents annually of their rights under the law.

COPPA is a federal law enforced by the Federal Trade Commission that went into effect in 2000 and is intended to place parents in control over information from their young children that is collected by websites, online service providers and mobile app operators. Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools or web-based testing services. In these cases, the schools may act as the parents' agent and can consent to the collection of kids' information on the parents' behalf. However, the schools' ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose.

In order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA. In addition, the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information. As long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. However, as a best practice, schools should consider making such notices available to parents, and consider the feasibility of allowing parents to review the personal information collected. Parents have the right to ask that any information that has been collected be deleted. (Source: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools)

What educators can do to model behaviors

As described in the ISTE Standards for Teachers, Standard 4.a., it is essential that educators:

"Advocate, model and teach safe, legal and ethical use of digital information and technology, including respect for copyright, intellectual property and the appropriate documentation of sources." (ISTE, 2008)

Here's how teachers can accomplish this standard:

Model. One of the best ways to help students adopt behaviors to keep them safe when online is for the adults in their lives to model them. When adults demonstrate both the "why" and the "how," students build their knowledge about what responsible online practices look like and can take action to protect themselves, their classmates and their families. They will realize that certain practices and behaviors for engaging in online environments are as important, for example, as the rules when playing team sports, driving a car or participating in class. By repeatedly modeling the process, educators demonstrate for students how to think critically about what they are doing when they go online.

Discuss. Teachers also need to stay abreast of new developments in data security and privacy. Teachers have a responsibility to help students ask the right questions before agreeing to give up their personal information when jumping on social apps, online resources or websites. The essential questions outlined above provide educators and students with a useful foundation for meaningful discussions that can impact online living both in and out of the classroom.

Apply. Because students are growing up in a digital world, they are talented consumers of technology, but their familiarity sometimes causes them to be completely unaware of the importance of protecting their online identity and considering the implications their actions will have on their digital footprint. By integrating these new behaviors into classroom activities, daily vocabulary and expectations, teachers help students build safe habits to sustain positive digital identities.

Share. Helping students build habits to protect their identity and personal data when going online is something everyone can get behind. Parents are instrumental in supporting students of all ages to build responsible online behaviors. Teachers can also share what they know and grow within their personal and professional communities. Teachers can join a professional community to garner additional support and to expand their own learning opportunities. There are a wide range of ISTE Professional Learning Networks where educators can connect with experts from around the globe in their field to ask questions, learn from colleagues and get access to exclusive events and professional learning opportunities.

The last mile

Technology will continue to evolve and provide countless new opportunities to connect and learn. It is our responsibility to equip students with the skills they need to protect them and maintain a diligent practice of identity management to inform and facilitate greater learning. Doing so will ensure that our digital footprint is not compromised by the latest innovations.

The dangers are real, but they can be difficult to understand. Solutions require consideration and planning.

RESOURCES

Digital Citizenship in Schools, Second Edition, is an essential introduction to digital citizenship. Starting with a basic definition of the concept and an explanation of its relevance and importance, author Mike Ribble explores the nine elements of digital citizenship. He provides a useful audit and professional development activities to help educators determine how to go about integrating digital citizenship concepts into the classroom. Activity ideas and lesson plans round out this timely book.

Protecting Privacy in Connected Learning Toolkit: Consideration When Choosing an Online Service Provider for Your School System, (Version 2, September 2014). The Consortium for School Networking (CoSN) developed an excellent document that describes and recommends procedures for maintaining a secure environment while making use of networked resources.

Securing the Connected Classroom: Technology Planning to Keep Students Safe, by Abbie H. Brown and Tim D. Green (published by ISTE). Brown and Green, co-authors of this paper, are experts on classroom digital security issues. Their most recent book describes the spectrum approach to establishing school policies and procedures that work and are developed by the school community itself. The book explains in detail the steps involved in fact-finding, committee creation, developing an appropriate response, building consensus and evaluating the results of the effort.

CONTRIBUTING AUTHORS

L. Beatriz Arnillas, Director-IT, Education Technology, Houston ISD; Tammi Sisk, Instructional Technology Specialist, Fairfax County Public Schools; Rick Stegman, Instructional Technology Specialist, Fairfax County Public Schools; Bob Moore, CEO, RJM Strategies LLC; Mindy Frisbee, Senior Project Manager, ISTE Standards, and; Jodie Pozo-Olano, Chief Communications Officer, ISTE