Digital Citizenship - Be Internet Awesome

Content Area: **Generic Content Area**
Course(s): **Generic Course**
Time Period: **Generic Time Period**
Length: **On going**
Status: **Published**

Unit Overview

This unit will teach students to make their own safe and thoughtful decisions as they navigate their digital lives. It will teach students the skills they need to be safe and smart on-line. Through browser-based games the students will learn these essential skills.

Transfer

• Think critically and evaluate websites, email, and other content online.

• Protect themselves from online threats, including bullying and scams.

• Get smart about sharing: what, when, how, and with whom.

• Be kind and respectful toward other people online, including respecting their privacy.

• Ask for help with tricky situations from a parent or other trusted adult.

For more information, read the following article by Grant Wiggins.

http://www.authenticeducation.org/ae_bigideas/article.lasso?artid=60

Meaning

Understandings

Students will understand how...

- To think critically and evaluate websites, email, and other content on-line.
- Protect themselves from on-line threats, including bullying and scams.
- Get smart about sharing: what, when, how, and with whom.
- Be kind and respectful toward other people on-line, including respecting their privacy.
- Ask for help with tricky situations from a parent or other trusted adult.

Essential Questions

Students will keep considering...

what practices can they use to keep themselves and others safe while living in the digital world.

Application of Knowledge and Skill

Students will know...

Students will know...

- when know to share and when to keep their information private.
- how to determine if something on the Internet if fake.
- what makes a good and safe password.
- how their words can affect others. As well as their actions on-line are as important as their real life.
- when to ask for help from adults (teachers, parents, guardians).

Students will be skilled at...

Students will be skilled at...

- managing a positive reputation both online and off.
- determining the validity of websites and other sources of information and be wary of manipulation, unsubstantiated claims, fake offers or prizes, and other online scams.

- creating strong passwords.
- identifying situations in which a trusted adult should be consulted.

Academic Vocabulary

Online privacy: A broad term that usually means the ability to control what information you share about yourself online and who can see and share it

Digital footprint (or digital presence): Your digital footprint is all the information about you that appears online. This can mean anything from photos, audio, videos, and texts to "likes" and comments you post on friends' profiles. Just as your footsteps leave prints on the ground while you walk, what you post online leaves a trail as well.

Reputation: The ideas, opinions, impressions, or beliefs that other people have about you; something that you can't be totally sure about but that you usually want to be positive or good

Personal information: Information that identifies a specific person – for example, your name, street address, phone number, Social Security number, email address, etc. – is called personal (or sensitive) info. Really think carefully before sharing this kind of information online.

Oversharing: Sharing too much online – usually this is about sharing too much personal information or just too much about yourself in a certain situation or conversation online.

Settings: This is the area in any digital product, app, website, etc., where you can define or adjust what you share and how your account is handled – including your privacy settings.

Bot: Also called a "chatbot" or "virtual assistant," this is a piece of software that operates online or on a network to automatically answer questions, follow commands (like giving directions to your new friend's house), or do simple tasks (like play a song).

Phishing: An attempt to scam you or trick you into sharing login information or other personal information online. Phishing is usually done through email, ads, or sites that look similar to ones you're already used to.

Spearphishing: A phishing scam where an attacker targets you more precisely by using pieces of your own personal information

Scam: A dishonest attempt to make money or gain something else of value by tricking people Trustworthy: Able to be relied on to do what is right or what is needed

Authentic: Real, genuine, true, or accurate; not fake or copied Verifiable: Something that can be proven or shown to be true or correct

Deceptive: False; an action or message designed to fool, trick, or mislead someone

Manipulation: Someone controlling or influencing another person or situation unfairly, dishonestly, or under threat. Alternatively, things you find online may be manipulated, such as a photo that has been edited to make you believe something that isn't true.

Fraudulent: Tricking someone in order to get something valuable from them

Firewall: A program that shields your computer from most scams and tricks

Malicious: Words or actions intended to be cruel or hurtful. Can also refer to harmful software intended to do damage to a person's device, account, or personal information.

Catfishing: Creating a fake identity or account on a social networking service to trick people into sharing their personal information or into believing they're talking to a real person behind a legitimate account, profile, or page

Clickbait: Manipulative online content, posts, or ads designed to capture people's attention and get them to click on a link or webpage, often to grow views or site traffic in order to make money

Privacy: Protecting people's data and personal information (also called sensitive information)

Security: Protecting people's devices and the software on them

Two-step verification (also called two-factor verification and two-step authentication): A security process where logging in to a service requires two separate steps or two "factors," such as a password and a one-time code. For example, you may have to enter your password and then enter a code that was texted to your phone or a code from an app.

Password or passcode: A secret combination used to access something. It may take different forms; for example, you may have a four-digit number-only code that you use for your phone lock and a much more complex password for your email account. In general, you should make your passwords as long and complex as you can while still being able to remember them.

Encryption: The process of converting information or data into a code that makes it unreadable and inaccessible

Complexity: The goal when creating a secure password. For example, a password is complex when it has a mix of numbers, special characters (like "$" or "&"), and both lowercase and uppercase letters.

Hacker: A person who uses computers to gain unauthorized access to other people's or organizations' devices and data

Bullying: Purposefully mean behavior that is usually repeated. The person being targeted often has a hard time defending themselves.

Cyberbullying: Bullying that happens online or through using digital devices Harassment: A more general term than bullying that can take many forms – pestering, annoying, intimidating, humiliating, etc. – and can happen online too

Conflict: An argument or disagreement that isn't necessarily repeated

Aggressor: The person doing the harassing or bullying; though sometimes called the "bully," bullying prevention experts advise never to label people as such.

Target: The person being bullied or victimized

Bystander: A witness to harassment or bullying who recognizes the situation but chooses not to intervene

Upstander: A witness to harassment or bullying who supports the target privately or publicly, sometimes including trying to stop and/or report the incident they witnessed

Amplify: To increase or widen participation or impact

Exclusion: A form of harassment or bullying used online and offline; often referred to as “social exclusion”

Block: A way to end all interaction with another person online, preventing them from accessing your profile, sending you messages, seeing your posts, etc., without notifying them (not always ideal in bullying situations where the target wants to know what the aggressor is saying or when the bullying has stopped)

Mute: Less final than blocking, muting is a way to stop seeing another person’s posts, comments, etc., in your social media feed when that communication gets annoying – without notifying that person or being muted from their feed (not helpful in bullying)

Anonymous: An unnamed or unknown person – someone online whose name or identity you don’t know

Trolling: Posting or commenting online in a way that is deliberately cruel, offensive, or provocative

Report abuse: Using a social media service’s online tools or system to report harassment, bullying, threats, and other harmful content that typically violates the service’s terms of service or community standards

Courageous: Brave; not necessarily fearless, though, because people are especially brave when they’re scared or nervous but take positive action anyway

Compromised account: An online account that has been taken over by someone else so that you no longer have complete control of it

Student agency: A step beyond a student using their voice to speak up, student agency is the capacity to act or make change; including protecting or standing up for oneself and others; often seen as a necessary part of citizenship

Trust: Strong belief that something or someone is reliable, truthful, or able

Learning Goal 1

Students will be able to make their own safe and thoughtful decisions as they navigate their digital lives. Students will have the skills they need to be safe and smart on-line.

Digital Citizenship Learning Goal 1 Proficiency Scale

TECH.8.1.5.D	Digital Citizenship: Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.
TECH.8.1.5.D.1	Understand the need for and use of copyrights.
TECH.8.1.5.D.2	Analyze the resource citations in online materials for proper use.
TECH.8.1.5.D.3	Demonstrate an understanding of the need to practice cyber safety, cyber security, and cyber ethics when using technologies and social media.

TECH.8.1.5.D.4	Understand digital citizenship and demonstrate an understanding of the personal consequences of inappropriate use of technology and social media.
TECH.8.1.5.D.CS1	Advocate and practice safe, legal, and responsible use of information and technology.
TECH.8.1.5.D.CS2	Demonstrate personal responsibility for lifelong learning
TECH.8.1.5.D.CS3	Exhibit leadership for digital citizenship.
TECH.8.1.5.E.1	Use digital tools to research and evaluate the accuracy of, relevance to, and appropriateness of using print and non-print electronic information sources to complete a variety of tasks.
TECH.8.1.5.E.CS2	Locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media.
TECH.8.1.5.E.CS3	Evaluate and select information sources and digital tools based on the appropriateness for specific tasks.

Target 1 - Share with Care

✓ Create and manage a positive reputation both online and off.

✓ Respect the privacy boundaries of others, even if different from one's own.

✓ Understand the potential impact of a mismanaged digital footprint.

✓ Ask for adult help when dealing with sticky situations.

Target 2 - Don't Fall for a Fake

✓ Understand that just because something is online doesn't mean it's true.

✓ Learn how phishing works, why it's a threat, and how to take steps to avoid it.

✓ Determine the validity of websites and other sources of information and be wary of manipulation, unsubstantiated claims, fake offers or prizes, and other online scams.

Target 3 - Secure Your Secrets

✓ Learn why privacy matters, and how it relates to online security.

✓ Practice how to create strong passwords.

✓ Review the tools and settings that protect against hackers and other threats.

Target 4 - It's Cool to Be Kind

✓ Define what being positive means and looks like online and offline.

✓ Lead with positivity in online communications.

✓ Identify situations in which a trusted adult should be consulted.

Summative Assessment

Be Internet Awesome Test

21st Century Life and Careers

CRP.K-12.CRP1.1	Career-ready individuals understand the obligations and responsibilities of being a member of a community, and they demonstrate this understanding every day through their interactions with others. They are conscientious of the impacts of their decisions on others and the environment around them. They think about the near-term and long-term consequences of their actions and seek to act in ways that contribute to the betterment of their teams, families, community and workplace. They are reliable and consistent in going beyond the minimum expectation and in participating in activities that serve the greater good.
CRP.K-12.CRP2.1	Career-ready individuals readily access and use the knowledge and skills acquired through experience and education to be more productive. They make connections between abstract concepts with real-world applications, and they make correct insights about when it is appropriate to apply the use of an academic skill in a workplace situation.
CRP.K-12.CRP5.1	Career-ready individuals understand the interrelated nature of their actions and regularly make decisions that positively impact and/or mitigate negative impact on other people, organization, and the environment. They are aware of and utilize new technologies, understandings, procedures, materials, and regulations affecting the nature of their work as it relates to the impact on the social condition, the environment and the profitability of the organization.
CRP.K-12.CRP8.1	Career-ready individuals readily recognize problems in the workplace, understand the nature of the problem, and devise effective plans to solve the problem. They are aware of problems when they occur and take action quickly to address the problem; they thoughtfully investigate the root cause of the problem prior to introducing solutions. They carefully consider the options to solve the problem. Once a solution is agreed upon, they follow through to ensure the problem is solved, whether through their own actions or the actions of others.
CRP.K-12.CRP9.1	Career-ready individuals consistently act in ways that align personal and community-held ideals and principles while employing strategies to positively influence others in the

	workplace. They have a clear understanding of integrity and act on this understanding in every decision. They use a variety of means to positively impact the directions and actions of a team or organization, and they apply insights into human behavior to change others' action, attitudes and/or beliefs. They recognize the near-term and long-term effects that management's actions and attitudes can have on productivity, morals and organizational culture.
CRP.K-12.CRP11.1	Career-ready individuals find and maximize the productive value of existing and new technology to accomplish workplace tasks and solve workplace problems. They are flexible and adaptive in acquiring new technology. They are proficient with ubiquitous technology applications. They understand the inherent risks-personal and organizational-of technology applications, and they take actions to prevent or mitigate these risks.

Formative Assessment and Performance Opportunities

Be Internet Awesome Interactive Games

Differentiation/Enrichment

Games can be played at their own pace and level.

Many discussions are teacher guided and information can be leveled according to class/student needs.

- IEP/504 Modifications
- Self and peer reflection and collaboration
- Small Group Instruction
- Independent review of Video Instruction
- Reveiw and Practice

Unit Resources

Be Internet Awesome Curriculum

Be Internet Awesome Website

BIA Google Slides