K-5 Computer Science

Teacher Notes

Domain Standard (Competency): Digital Citizenship

The Teacher Notes were developed to help teachers understand the depth and breadth of the standards. In some cases, information provided in this document goes beyond the scope of the standards and can be used for background and enrichment information. Please remember that computer science encompasses both fundamental skills, such as computational thinking and digital citizenship, that all students should be introduced to in order to be viable citizens in a digital society as well as discrete skills that are endemic to specific career clusters.

1762 Twin Towers East • 205 Jesse Hill Jr. Drive • Atlanta, GA 30334 • www.gadoe.org
Table of Contents

Related Standard(s)
Overview
K-2 Elements
3-5 Elements
Related Vocabulary
Citations
Grade-by-grade Progression
Digital Citizenship

CSS.DC.K-2.3: Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

1. Identify personal information, understand the need to keep it private, and engage in activities for keeping personal information private.
2. Participate in systems for keeping personal information private and protected (for example: passwords, biometric sensors).
3. Understand shared information on the Internet can be permanent.
4. Recognize and avoid harmful behaviors in online environments (e.g. viruses, in-app purchases, cyber-bullying, etc).
5. Follow safety rules and exhibit responsibility when using a device.
6. Create an artifact that shows the use of positive safe behavior when using technology.
7. Recognize work that is created by others.
8. Recognize that credit is given for the work of others found online.
9. Create an artifact that demonstrates a positive personal digital identity.

CSS.DC.3-5.3: Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

1. Discuss real-world cybersecurity problems (e.g. viruses, phishing attacks, click bait, etc) and how personal information can be protected.
2. Understand, demonstrate, and encourage respect for intellectual property of print and digital media.
3. Create and manage digital identity through positive, safe, and ethical online interactions.
Digital Citizen – Overview

CSS.DC.K-2.3: Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

CSS.DC.3-5.3: Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

Click this link for an animated version of this introductory section. [https://youtu.be/untCgT3_wxg](https://youtu.be/untCgT3_wxg)

Digital Citizen is a domain which is reflected in the way all of the other domains are implemented as it guides students’ responsible use of that technology. The Digital Citizen standards imply that students are citizens in a digital world and therefore students and their teachers should strive to be good, positive citizens of that world. Currently, most people use some form of interconnected technology in many aspects of society and daily life. When using such technology, students must be able to recognize when their actions will lead to positive or negative outcomes. Furthermore, students need to comprehend how those actions will affect themselves and others. As citizens in the digital world, everyone retains certain rights, responsibilities, and opportunities as they live, learn, and work with digital tools. Of these, the most relevant to students at the K-5 level are safety, intellectual property, and positive interaction.

Students must learn how to keep themselves safe in online environments. The foundation for keeping students safe is for them to be cognizant of the personal information they share digitally. From entering personal information into a web page to chatting while gaming, students must consider the information they share online. Another important aspect to internet safety is being mindful of the digital identity they create with almost every choice they make, from creating publicly viewable usernames to posting information, photos, or videos online. Recognizing dangers to themselves and to their devices as well as making safe choices are important parts of being a good digital citizen.
Practicing the legal and ethical use of technology is an important part of being a good digital citizen. Protecting creative ideas and technological advances is key to intellectual and technological growth in society. The U.S. Constitution lays the foundation for this protection in Article One, Section 8, “To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries” which lead to the development of current copyright laws. When students create artifacts for learning or entertainment, it is easy for them to use information or audio/visual elements without permission. The simple act of copying and pasting an image from a Google search takes just a few seconds with very little effort. It is important that teachers instill the understanding that those words, ideas, graphics, etc. were not created by the student and thus they don’t have implicit permission for their use. Teaching citation of sources is only a part of the solution as it merely addresses the plagiarism side of the issue. It is also important to direct students to sources of images, etc. that have granted certain usage rights and to spark conversations and thought surrounding the use of others’ creative work. Learning the basics of plagiarism and copyright responsibility at an early age points students in the right direction as they grow.

We create the digital world in which we live. The positive interactions that students experience as they contribute creatively and connect with others build a positive digital world for everyone. As students begin to build a digital identity, teachers should provide opportunities that lead to developing positive and safe interactions with others through discussions and practice. Most students know of or have experienced negative online interactions and need strategies and understanding of ways to manage those situations.

The Digital Citizen domain is the foundation for encouraging safe and positive use of technology in an interconnected world.
As an educator, if you want to learn more about digital citizenship consider using these resources.

Become a Common Sense Media Educator:
https://www.commonsense.org/education/recognition

Complete the Google Citizenship and Safety Course:
https://teachercenter.withgoogle.com/digital_citizenship/preview
CSS.DC.K-2.3.1

Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

1. Identify personal information, understand the need to keep it private, and engage in activities for keeping personal information private.


This element is about students learning how to keep personal information private by teaching them what personal information is, to be aware when that information is being asked for, and the dangers of providing that information.

Personal Information is any data that specifically identifies a person which includes: student names, family names, home address, phone numbers, school, birthday, age, current or future locations, photos of themselves, etc. These items are not safe for students to share without adult supervision.

Websites, apps, and messages from others in games or chat functions may ask for various forms of personal information. Some websites or apps ask for this information as part of the account creation process, and even these requests could be fraudulent. These sites may or may not be safe environments for students at this level. It is important that students know that any time their personal information is requested they should immediately alert a trusted adult. Even when playing games, some students are confronted with requests for information which is unsafe to share and it is important for them to know how to handle those situations. Regardless of the context, students need to be able to recognize that they are being asked to provide information that should be kept private.

Providing personal information can be dangerous. In May 2019, the GBI reported that through a recent operation 31 people were arrested in Georgia for internet crimes against children. Several
of these arrests were directly related to online predators obtaining children's personal information for the purpose of harming them (Georgia Bureau of Investigation 2019). It is important that children know that even though they believe they are communicating with someone that shares their interests, it could be someone that means them harm. Not only can providing personal information be used to harm them physically, it can also cause digital identity or financial harm to themselves or their families.

Teachers can provide activities in which students are asked for various pieces of information in different situations. Conduct discussions about what to do in those situations and proper responses such as asking an adult for help. Students work through the thought process so that when a real problem arises, they know how to react.

Resource Links

BrainpopJr. - Internet Safety (free lesson)  
https://jr.brainpop.com/artsandtechnology/technology/internetsafety/

Code.org - Course E: Lesson 8 - Private and Personal Information Lesson  
https://curriculum.code.org/csf-19/coursee/8/

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common sense media updated their lessons. Below are former and current lessons that focus on privacy.

Common Sense Media - Digital Citizenship Curriculum  
https://www.commonsense.org/education/digital-citizenship/curriculum  
Look for these lessons that focus on privacy and security at the K-2 level. 
Kindergarten - Safety in My Online Neighborhood  
1st Grade - Internet Traffic Light  
2nd Grade - That's Private!  
(Previous privacy lesson from Common Sense Media)  
K-2 Keep It Private  
https://www.commonsense.org/education/lesson/keep-it-private-k-2

Article - Protect Your Students and Data Privacy (Note: lessons here are directed to grades 3 and up but this site contains up-to-date privacy information for everyone.)

Teaching Privacy (K-12) (Note: this resource provides lessons that may be too advanced for the K-2 level, but it contains valuable and up-to-date privacy information for everyone.)
https://teachingprivacy.org/teachers-portal/
Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

2. Participate in systems for keeping personal information private and protected (for example: passwords, biometric sensors).


This element is about making students aware that they participate at home and at school in systems that can help keep their information private and protected. Teachers should conduct discussions with students which create the awareness that when they log into various applications or websites for educational or gaming purposes, they are using a system designed to keep their data secure (or the expectation thereof). At school, students log into resources using a username and password that provides access only to themselves and school personnel. At home they may log into gaming systems or other platforms as well. It is important to note that creating usernames and passwords is also a privacy issue. When appropriate, students should be taught how to create usernames and passwords that do not include personal information. Teachers should also have discussions of different ways that accounts and devices can be protected: usernames and passwords, biometric methods such as fingerprint sensors, face ID or PIN numbers and more.
Resource Links

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons. Below are former and current lessons that focus on passwords.

Digital Passport - Password Protect activity (online interactive game)
https://www.digitalpassport.org/

K-2 Powerful Passwords
https://www.commonsense.org/education/lesson/powerful-passwords-k-2

3-5 Password Power-Up
https://www.commonsense.org/education/digital-citizenship/lesson/password-power-up

Biometrics and how they work
https://www.elprocus.com/different-types-biometric-sensors/
CSS.DC.K-2.3.3

Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

3. Understand shared information on the Internet can be permanent.


This element is about understanding that anything shared on an online device has the potential to be recorded permanently. A digital footprint is made up of messages and pictures that have been shared via email, texting, social media, etc. as well as a record of websites visited and searching history. This footprint can affect relationships and later in life, education and career opportunities. Therefore, students need to think about what they do online even at a young age.
Resource Links

Code.org - Your Digital Footprint - Course B - Lesson 1 (K-2)
https://curriculum.code.org/csf-19/courseb/1/

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons. Below are former and current lessons that focus on digital footprints.

   Common Sense Media - Digital Citizenship Curriculum
   https://www.commonsense.org/education/digital-citizenship/curriculum
   Look for this lesson that deals with digital footprint and identity at the K-2 level.
   2nd Grade - Digital Trails
   (Previous digital footprint lesson from Common Sense Media)
   K-2 Follow the Digital Trail lesson and video
   Teaching Channel - video of implementation of this lesson

   For teachers - Young Children & Digital Footprints

   How to Teach Students About their Digital Footprint
   https://www.eschoolnews.com/2014/01/20/kids-digital-footprint-937/

   Teaching Children about Digital Footprints and Online Reputations

   Young Children & Digital Footprints
CSS.DC.K-2.3.4

Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

4. Recognize and avoid harmful behaviors in online environments (e.g. viruses, in-app purchases, cyber-bullying, etc).


This element is about recognizing and avoiding dangers in the digital world.

**Viruses, Malware, Spyware** (terms referring to harmful software) - Students may unknowingly infect their devices with dangerous software by visiting infected websites, clicking on ads or pop up messages, downloading infected games, etc. It is important to stress that students at the K-2 level should be visiting websites that are approved by a trusted adult or teacher. Also, teachers need to guide students into recognizing advertisements and popups so that they understand what is not safe to click on. Free games, etc. are usually infected with malware. This is how the makers of the games or the owners of the hosting websites are able to publish the games for free. It may not be apparent that the harmful software is working in the background, but it could be sending back personal information stored on the device or even recording every keystroke to capture usernames and passwords.

**Cyberbullying** - According to the website Stopbullying.gov, the definition of cyberbullying is: “Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior” (Tips for Teachers). Schools and school systems should already have in place procedures and programs to prevent and address cyberbullying. Students need to be able to recognize when cyberbullying occurs and know how to report it to an adult who can help.
is occurring and to know how to react appropriately. In a cyberbullying situation there are various roles that students may play: the bully or person perpetrating the abuse, the victim or target of that abuse, and others that may have knowledge of the situation and either stand by and do nothing or may try to help the situation. A few essential rules to emphasize to students are: never respond to a bully as that typically escalates the issue, always talk to a trusted adult whether they are the victim or just have knowledge of bullying, and try to capture proof of the bullying with screenshots, photos, print outs, etc. Also, according to Common Sense Education, lessons “focusing on empathy and compassion, [and] conversations about cyberbullying can give young kids a foundation for future positive online experiences.”

**In-app purchasing** - Although not a common occurrence at school, children have created financial hardships for their families through unsupervised in-app purchases. Teachers can lead discussions that encourage students to stop and think when using apps and always receive parent/guardian permission before playing games that offer in-game items for purchase.

**Other inappropriate use of technology** - As with addressing any negative behaviors in the classroom, it is beneficial to occasionally use these as teachable moments. Other harmful behaviors that might arise could include: negative online interactions (some interactions may not be considered cyberbullying, but need to be addressed), the spread of false information, or other actions that violate the school or school system’s AUP (appropriate use policy).
Malware, Viruses, and Spyware Resource Links

Brainpopjr.com - Internet Safety (free video)
https://jr.brainpop.com/artsandtechnology/technology/internetsafety/
Educator resources

Good Computer Kids - Computer Viruses (school-created video)
https://www.youtube.com/watch?v=pNwrqi9ZhJ4

How Can Teachers Teach Students To Stay Safe From Malware Attacks? (informational article)
https://k12teacherstaffdevelopment.com/tlb/how-can-teachers-teach-students-to-stay-safe-from-malware-attacks/

Meet the Malwares (video from the UK- preview before using with students)
Cyberbullying Resource Links

Brainpopjr - Bullying (free video)
https://jr.brainpop.com/health/feelings/bullying/

BullyingNoWay from the government of Australia
also, free iOS and android apps
https://bullyingnoway.gov.au/Resources/BullyingNoWayApps

Code.org - Screen Out the Mean lesson (K-2)
https://curriculum.code.org/csf-19/coursec/1/

Code.org - The Power of Words lesson (3-5)
https://curriculum.code.org/csf-19/coursef/17/

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons. Below are former and current lessons that focus on Cyberbullying.

   Common Sense Media - Digital Citizenship Curriculum
   https://www.commonsense.org/education/digital-citizenship/curriculum
   Look for this lesson that deals with digital footprint and identity at the K-2 level.
   2nd Grade Putting a Stop to Online Meanness

   (Previous cyberbullying lesson from Common Sense Media)
   K-2 Screen Out the Mean

Stopbullying.gov Resource Tips
https://www.stopbullying.gov/cyberbullying/tips-for-teachers/index.html
CSS.DC.K-2.3.5

Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

5. Follow safety rules and exhibit responsibility when using a device.


This element is about using the safety rules outlined in each of the other elements of this Digital Citizen domain on a consistent basis. While working on projects in other domains, this element creates the expectation that students are using technology responsibly. It is important to reinforce positive uses of technology and address negative issues as they arise. Physically or electronically posting clear and positive expectations of student use of technology can also be helpful in reinforcing this element. Most school systems have acceptable use policies and should be referred to when communicating safe and responsible expectations for students.

Resource Links

5 Internet Safety Tips for Kids:
- [https://www.youtube.com/watch?time_continue=17&v=X9Htg8V3eik](https://www.youtube.com/watch?time_continue=17&v=X9Htg8V3eik) (lessons and activities with the video)

B4UClick: (information, videos, and interactive quizzes)
- [https://b4uclick.org/](https://b4uclick.org/)

NetSmartz: (New “Into the Cloud” content 2019: videos, activities, and a free android/iOS game)
- [http://www.missingkids.org/netsmartz/videos#elementary](http://www.missingkids.org/netsmartz/videos#elementary)
- [https://www.netsmartzkids.org/](https://www.netsmartzkids.org/)
CSS.DC.K-2.3.6

*Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.*

6. Create an artifact that shows the use of positive safe behavior when using technology.


This element is about providing the opportunity for students to create an artifact that illustrates the good choices they make while using technology.

Positive safe behaviors might include:

- Keeping personal information private
- Using safe/secure usernames and passwords
- Using safe websites (adult approved when age appropriate)
- Not clicking on ads or popups
- Not downloading games, etc. without permission
- Respecting others’ privacy
- Citing others’ work appropriately and using graphics with appropriate usage rights
- Being kind to others while using technology
Artifact Ideas

**Illustration** - Google Drawing, ABCya Paint, AutoDraw - Students create an illustration showing themselves or others making good digital choices. (See illustration created using Google Drawing.)

**Document** - Google Docs, any word processing software - Students collaborate on a story where characters must make choices in their digital lives.

**Animation** - ABCya Animate [https://www.abcya.com/games/animate](https://www.abcya.com/games/animate), Scratch [https://scratch.mit.edu/ideas](https://scratch.mit.edu/ideas) - Students animate characters making good digital choices. (See animation created using ABCya.)

**Video** - Students create a mock interview with a “famous” great digital citizen and ask questions about how they stay safe.

**Flipgrid** - [https://info.flipgrid.com](https://info.flipgrid.com) - Free site where teachers can create a prompt that students can respond in 15 sec. - 5 min. video recordings.

**Robotics** - Students pilot a robot through a student-created maze of positive choices. (See photo of Sphero robots controlled by a Chromebook.)
Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

7. Recognize work that is created by others.


This element is about helping students recognize items that are created by others. These items, or assets, could be images, information, animations, videos, etc. found on websites or through searches. When creating projects in other domains, students need to recognize where the assets come from that they use. This can lead to simple discussions on copyright and plagiarism.

Example Activity

Students could create an artifact that includes a photo or drawing created by themselves and one from a website. Discuss with students the difference between their work and someone else’s.

(drawing created with Google Drawing)

The same idea would apply for information written in their own words and compared to information from a website.
Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

8. Recognize that credit is given for the work of others found online.


This element is about helping students realize they should give credit when using items, graphics, or ideas created by someone else. This addresses the awareness of plagiarism with students. Teachers should model this by citing sources of the items they use in teaching materials they create. Depending on the level, students can begin to provide simple source citations for the items they use that were created by others. It is not necessary for K-2 students to use sophisticated citation format such as MLA. The source information could even be added to the project by the teacher. The emphasis should be to simply add the source name or URL (website link) to projects to create the awareness that work done by others should receive credit.
Resource Links

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons.

  Common Sense Media - Digital Citizenship Curriculum
  https://www.commonsense.org/education/digital-citizenship/curriculum
  Look for this lesson that deals with giving credit at the K-2 level.
  2nd Grade - Let’s Give Credit

  Common Sense Media Copyright and Fair Use Animation (Overview of the topic)
  https://www.youtube.com/watch?v=suMza6Q8J08

Copyright Facts for Kids
https://kids.kiddle.co/Copyright

Educator’s guide to Copyright and Fair Use
https://www.educationworld.com/a_curr/curr280.shtml

Photos For Class (cites the source automatically)
https://www.photosforclass.com

Pixabay - free (no login required), no attribution requirement photos
https://pixabay.com/

Unsplash - 350+ free pictures, no attribution required but easy citation with one click
https://unsplash.com/s/photos/free

Pexels - Free stock photos, no attribution required but easy citation with one click
https://www.pexels.com/

NASA images and videos
https://images.nasa.gov/
Example Activity

When students create an artifact, they can include a short citation with the websites from which they got information and photos. In this illustration, a student created a Google drawing and searched for photos in the Explore pane for the parts of a plant. (S1L1- GA Standards) After adding the photo to their page, they (or the teacher) can easily click the copy button on the photo and paste the location of the picture on the page. (see image below)  Note: Photos used in a student project as shown below would be considered “Fair Use” of those photos.

For more information on Google Image searching - [https://support.google.com/websearch/answer/29508?hl=en](https://support.google.com/websearch/answer/29508?hl=en)
Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

9. Create an artifact that demonstrates a positive personal digital identity.


This element is about the opportunity for students to create an artifact that illustrates keeping a positive digital footprint.

Positive digital identity behaviors might include:

- Having positive, friendly, and respectful interactions with others
- Knowing that anything done online can be permanent and public
- Keeping searches and web history clean and appropriate
- Showing students’ personal potential and personal achievements
- Being supportive of victims of cyberbullying
Artifact Ideas

**Illustration** - Google Drawing, ABCya Paint, AutoDraw: to illustrate the above behaviors

**Documents** - Google Docs, any word processing software: to write a narrative on the above behaviors

**Animation** - ABCya Animate
https://www.abcyaa.com/games/animate,
(See animation created in ABCya.)

**Scratch** - https://scratch.mit.edu/ideas Students could create a simple interactive game where the users must make positive choices.

**Robotics** - Students pilot a robot through a maze of positive digital footprint choices

**Video** - Students could act out a scenario where they make positive choices using cameras or mobile device (iPad, other tablet, Chromebook).

**Flipgrid** - https://info.flipgrid.com/ Free site where teachers can create a prompt that students can respond in 15sec. - 5 min. video recordings. Students could act out a scene exhibiting positive behaviors.
Should I go to that weird website someone told me about?

No, I better not. It didn't sound safe!

It could damage my device and my digital footprint!
CSS.DC.3-5.3.1

Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

1. Discuss real-world cybersecurity problems (e.g. viruses, phishing attacks, click bait, etc) and how personal information can be protected.


This element is about creating awareness and conducting discussions of various cybersecurity problems and the importance of protecting our personal information in the digital world.

**Viruses, Malware, Spyware** (terms referring to harmful software) - Students may unknowingly infect their devices with dangerous software by visiting infected websites, clicking on ads or pop up messages, downloading infected games, etc. It is important to stress that students at the 3-5 level are transitioning from visiting websites that are approved by a trusted adult or teacher to making thoughtful searches and choices for themselves. Also, teachers need to guide students into recognizing advertisements and popups so they understand what is not safe to click on. Free games, etc. are usually infected with some form of malware. This is how the makers of the games or the owners of the hosting websites are able to publish the games for free. It may not be apparent that the harmful software is working in the background, but it could be sending back personal information stored on the device or even recording every keystroke to capture usernames and passwords.

**Phishing attacks** - A phishing attack is when a user is tricked into clicking on a message, email, or website which then infects that person’s computer or device with malware. Some phishing attacks can result in the computer or device being “held for ransom” in that the attacker locks the device and will not release it until a ransom has been paid (and there’s no guarantee that it will be released even if the ransom is paid.) Attackers use carefully social engineered techniques to trick users. Sometimes, it is virtually impossible to discern whether a message or email is safe. Posts on social media are also frequently linked to phishing scams. Teachers should discuss strategies with students to help them stop, think, and analyze when clicking on messages or other communications.
emails. Things to consider would be: finding the actual email address of the sender (many times the actual email address that sent the email is not who it seems), watching for misspellings and grammar mistakes (although this is becoming less common with improvements in artificial intelligence), never clicking links unless you are certain of the sender (try going to the site manually instead of clicking a link).

**Clickbait** - “A form of false advertisement which uses hyperlink text or a thumbnail link that is designed to attract attention and entice users to follow that link and read, view, or listen to the linked piece of online content, with a defining characteristic of being deceptive, typically sensationalized or misleading.” (Wikipedia) It is important for students to realize that they can be manipulated into viewing material or advertisements.

**Protecting Personal Information** - Students need to learn how to keep personal information private by identifying what personal information is, being aware when that information is being asked for, and the dangers of providing that information. Personal Information is any data that specifically identifies a person which includes: student names, family names, home address, phone numbers, school, birthday, age, current or future locations, photos of themselves, etc. These items are not safe for students to share without adult supervision.

Websites, apps, and messages from others in games or chat functions may ask for various forms of personal information. Some websites or apps ask for this information as part of the account creation process, and even these requests could be fraudulent. These sites may or may not be safe environments for students at this level. It is important that students know that any time their personal information is requested they should immediately alert a trusted adult. Even when playing games, some students are confronted with requests for information which is unsafe to share and it is important for them to know how to handle those situations. Regardless of the context, students need to be able to recognize that they are being asked to provide information that should be kept private.

Providing personal information can be dangerous. In May 2019 the GBI reported that through a recent operation, 31 people were arrested in Georgia for internet crimes against children. Several
of these arrests were directly related to online predators obtaining children’s personal information for the purpose of harming them (Georgia Bureau of Investigation 2019). It is important that children know that even though they believe they are communicating with someone that shares their interests, it could be someone that means them harm. Not only can providing personal information be used to harm them physically, it can also cause digital identity or financial harm to themselves or their families.

Teachers can provide activities in which students are asked for various pieces of information in different situations. Discussions about what to do in those situations and proper responses such as asking an adult help students work through the thought process so that when a real problem arises, they know how to react.

Resource Links

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common sense media updated their lessons. Below are former and current lessons that focus on personal information, clickbait, and phishing.

Common Sense Media - Digital Citizenship Curriculum
https://www.commonsense.org/education/digital-citizenship/curriculum

Look for these lessons that focus on privacy and security at the 3-5 level.
3rd Grade - Password Protect
4th Grade - Private and Personal Information
5th Grade - You Won’t Believe This!
6th Grade - Don’t Feed the Phish

(Previous lessons from Common Sense Media)
3-5 You’ve Won a Prize!
https://www.commonsense.org/education/lesson/youve-won-a-prize-3-5
6-8 Scams and Schemes
https://www.commonsense.org/education/lesson/scams-and-schemes-6-8

Good Computer Kids - Computer Viruses (school-created video)
https://www.youtube.com/watch?v=pNwrqi9ZhJ4
How Can Teachers Teach Students To Stay Safe From Malware Attacks? (informational article)
https://k12teacherstaffdevelopment.com/tlb/how-can-teachers-teach-students-to-stay-safe-from-malware-attacks/

Meet the Malwares (video from the UK- preview before using with students)
CSS.DC.3-5.3.2

Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.

2. Understand, demonstrate, and encourage respect for intellectual property of print and digital media.


This element is about helping students realize they should respect and give credit when using items, assets, or ideas created by someone else. This addresses the awareness of plagiarism with students. Teachers should model this by citing the sources of the items they use in teaching materials they create. Depending on the level, students can begin to provide simple source citations for the items they use that were created by others. It may not be necessary for 3-5 students to use sophisticated citation format such as MLA. The emphasis should be to add the source name or URL (website link) to projects to emphasize that work done by others should receive credit.

Resource Links

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons.

Common Sense Media - Digital Citizenship Curriculum
[https://www.commonsense.org/education/digital-citizenship/curriculum](https://www.commonsense.org/education/digital-citizenship/curriculum)

Look for this lesson that deals with giving credit at the 3-5 level.
4th Grade - A Creator’s Rights and Responsibilities

(Previous lessons from Common Sense Media)
3-5 Whose is it, Anyway

1762 Twin Towers East • 205 Jesse Hill Jr. Drive • Atlanta, GA 30334 • www.gadoe.org
https://www.commonsense.org/education/lesson/whose-is-it-anyway-3-5
3-5 How to Cite a Site
https://www.commonsense.org/education/lesson/how-to-cite-a-site-3-5

Common Sense Media Copyright and Fair Use Animation (Overview of the topic)
https://www.youtube.com/watch?v=suMza6Q8J08

Copyright Facts for Kids
https://kids.kiddle.co/Copyright

Educator’s guide to Copyright and Fair Use
https://www.educationworld.com/a_curr/curr280.shtml

Photos For Class (cites the source automatically)
https://www.photosforclass.com

Pixabay - free (no login required), no attribution requirement photos
https://pixabay.com/

Unsplash - 350+ free pictures, no attribution required but easy citation with one click
https://unsplash.com/s/photos/free

Pexels - Free stock photos, no attribution required but easy citation with one click
https://www.pexels.com/

NASA images and videos
https://images.nasa.gov/
CSS.DC.3-5.3.3

*Identify the rights, responsibilities, and opportunities of living, learning, and working in an interconnected society and model behaviors that are safe, legal, and ethical.*

3. Create and manage digital identity through positive, safe, and ethical online interactions.


This element is about creating and maintaining a positive digital identity, also called a digital footprint. A digital footprint is made up of messages and pictures that have been shared via email, texting, social media, etc. as well as a record of websites visited and searching history. At the K-2nd grade levels, students learn about protecting their personal and private information. At the 3rd-5th grade levels, students should recognize that everything they do and share online is contributing to their digital footprint which can then affect their current and future opportunities for education, jobs, and relationships. They must protect their private information as well as think about how other behaviors form their digital identity. Students should be guided to stop and think about messages, photos, etc. that they intend to share and then consider longer term consequences of their actions. Also, encouraging students to keep their online interactions positive is another way to help students create and manage their digital identities.

As a part of creating a positive online identity, it is important to address the issue of cyberbullying. According to the website Stopbullying.gov, the definition of cyberbullying is: “Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior” (Tips for Teachers). Schools and school systems should already have in place procedures and programs.
to prevent and address cyberbullying. Students need to be able to recognize when cyberbullying is occurring and to know how to react appropriately. In a cyberbullying situation there are various roles that students may play: the bully or person perpetrating the abuse, the victim or target of that abuse, and others that may have knowledge of the situation and either stand by and do nothing or may try to help the situation. A few essential rules to emphasize to students are: never respond to a bully as that typically escalates the issue, always talk to a trusted adult whether they are the victim or just have knowledge of bullying, and try to capture proof of the bullying with screenshots, photos, print outs, etc. Also, according to Common Sense Education, lessons “focusing on empathy and compassion, [and] conversations about cyberbullying can give young kids a foundation for future positive online experiences.”

Digital Footprint Resource Links

Brainpop- Digital Etiquette  
https://www.brainpop.com/technology/freemovies/digitaletiquette/

Code.org - Unplugged Lesson - Your Digital Footprint  
https://code.org/curriculum/course2/18/Teacher

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons.

Common Sense Media - Digital Citizenship Curriculum  
https://www.commonsense.org/education/digital-citizenship/curriculum
Look for this lesson that deals with giving credit at the 3-5 level.  
3rd Grade - This is Me  
3rd Grade - Our Digital Citizenship Pledge  
4th Grade - Our Online Tracks  
4th Grade - Keeping Games Fun and Friendly  
5th Grade - Beyond Gender Stereotypes  
5th Grade - Digital Friendships

(Previous lesson from Common Sense Media)  
3-5 Picture Perfect  
https://www.commonsense.org/education/lesson/picture-perfect-3-5
3-5 Privacy Rules
https://www.commonsense.org/education/lesson/privacy-rules-3-5

Health Powered Kids - Lesson - Online Safety for Kids: Your digital footprint and digital imprint

How to Teach Students About their Digital Footprint
https://www.eschoolnews.com/2014/01/20/kids-digital-footprint-937/

Teaching Children about Digital Footprints and Online Reputations

Young Children & Digital Footprints

Cyberbullying Resource Links

BullyingNoWay from the government of Australia
also, free iOS and android apps
https://bullyingnoway.gov.au/Resources/BullyingNoWayApps

Code.org - The Power of Words lesson (3-5)
https://curriculum.code.org/csf-19/coursef/17/

Common Sense Media - This site contains an entire digital citizenship curriculum K-12. Teachers must create a free account to access the lessons. In 2018 and 2019, Common Sense Media updated their lessons. Below are former and current lessons that focus on Cyberbullying.

Common Sense Media - Digital Citizenship Curriculum
https://www.commonsense.org/education/digital-citizenship/curriculum
Look for this lesson that deals with digital footprint and identity at the 3-5 level.
3rd Grade The Power of Words
4th Grade Be a Super Digital Citizen
5th Grade Is it Cyberbullying

(Previous cyberbullying lesson from Common Sense Media)
What’s Cyberbullying?
https://www.commonsense.org/education/lesson/whats-cyberbullying-3-5

Stopbullying.gov Resource Tips
https://www.stopbullying.gov/cyberbullying/tips-for-teachers/index.html
Related Vocabulary:

**K-2**

**Ads** - advertisements. These can be posted on websites in order for the website makers to earn money if they are clicked. They may be videos or graphics or even pop-ups that are tempting for students to click on.

**Copyright and Fair Use** - Copyright is a law that protects creators and allows them to decide what is done with their work. Fair Use is an exception to copyright law that allows people to use a small amount of someone’s work for educational purposes.

**Cyberbullying** - is “bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior” (Tips for Teachers)

**Digital Citizen** - a person’s digital identity as they participate in an online environment.

**Digital Footprint** - a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services. (The Tech Terms Computer Dictionary)

**Downloading** - the process of receiving data over the Internet. (The Tech Terms Computer Dictionary)

**Malware** - comes from the combination of the words malicious and software This would include things like computer viruses and spyware.

**Personal Information** - information about yourself that identifies you specifically. Your name, address, phone numbers, school, location, etc.

**Password** - a string of characters used for authenticating a user on a computer system. For example, you may have an account on your computer that requires you to log in. In order to successfully access your account, you must provide a valid username and password. This combination is often referred to as a login. While usernames are generally public information, passwords are private to each user. (The Tech Terms Computer Dictionary)

**Plagiarism** - taking someone else's work or ideas and passing it off as one's own.
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acceptable Use Policy (AUP)</strong></td>
<td>A list of rules created by your school or school system that guide teachers and students in the appropriate use of technology resources. This could also be a part of a “code of conduct.”</td>
</tr>
<tr>
<td><strong>Ads</strong></td>
<td>Advertisements. These can be posted on websites in order for the website makers to earn money if they are clicked. They may be videos or graphics or even pop-ups that are tempting for students to click on.</td>
</tr>
<tr>
<td><strong>Chat</strong></td>
<td>A method for communicating with other people through a website or game. Usually, this is done by text.</td>
</tr>
<tr>
<td><strong>Copyright and Fair Use</strong></td>
<td>Copyright is a law that protects creators and allows them to decide what is done with their work. Fair use is an exception to copyright law that allows people to use a small amount of someone’s work for educational purposes.</td>
</tr>
<tr>
<td><strong>Cyberbullying</strong></td>
<td>Is “bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior” (Tips for Teachers)</td>
</tr>
<tr>
<td><strong>Digital Citizen</strong></td>
<td>A person’s digital identity as they participate in an online environment.</td>
</tr>
<tr>
<td><strong>Digital Footprint</strong></td>
<td>A trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services. (The Tech Terms Computer Dictionary)</td>
</tr>
<tr>
<td><strong>Downloading</strong></td>
<td>The process of receiving data over the Internet.</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>Comes from the combination of the words malicious and software. This would include things like computer viruses and spyware.</td>
</tr>
<tr>
<td><strong>Personal Information</strong></td>
<td>Information about yourself that identifies you specifically. Your name, address, phone numbers, school, location, etc.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>A string of characters used for authenticating a user on a computer system. For example, you may have an account on your computer that requires you to log in. In order to successfully access your account, you must provide a valid username and password. This combination is often referred to as a login. While usernames are generally public information, passwords are private to each user. (The Tech Terms Computer Dictionary)</td>
</tr>
<tr>
<td><strong>Plagiarism</strong></td>
<td>Taking someone else's work or ideas and passing it off as one's own.</td>
</tr>
</tbody>
</table>
Citations


U.S. Constitution. Art.I, Sec. 8


Grade by grade progression

Kindergarten

Description of Digital Citizen for kindergarten: In kindergarten, students should be part of discussions and lessons focused on being a “good” digital citizen and following safety rules for using technology in the classroom and at home. Teachers can emphasize keeping personal information and passwords private as well as recognizing “strangers” online. Verbally acknowledging when the teacher or student uses digital items that were created by someone else is sufficient for creating awareness of proper use of copyrighted items at the kindergarten level.

Some artifacts that kindergarteners can create include drawings or other expressions that illustrate themselves showing positive safe behaviors and drawings or other expressions that show a positive personal identity.

Sample activity:

1 - Students can draw or write (on paper or digitally) how you can stay safe online. These drawings were completed by first graders on Nearpod.com in a “Draw It” activity.

<table>
<thead>
<tr>
<th>Student wrote that he/she would not talk to people you do not know.</th>
</tr>
</thead>
<tbody>
<tr>
<td>only go on green websites.</td>
</tr>
<tr>
<td>Student wrote that they only go on green (good) sites.</td>
</tr>
<tr>
<td>Student drawings showing working on computer with parent at home.</td>
</tr>
</tbody>
</table>
First grade

Description of Digital Citizen for first grade: In first grade, students should be part of discussions and lessons focused on being a “good” digital citizen and following safety rules for using technology in the classroom and at home, as well as learning about some of the dangers that exist when online. Teachers should emphasize keeping personal information and passwords private as well as recognizing various dangers online. Simple teacher or student labelling of sources when using digital items that were created by someone else is sufficient for creating awareness of proper use of copyrighted items at the first grade level.

Some artifacts that first graders can create include drawings or other expressions that illustrate themselves showing positive safe behaviors or dangers online and drawings or other expressions that show a positive personal identity.

Sample activity:
1 - Students can draw pictures illustrating how cyberbullying makes people feel? These drawings were completed by first graders on Nearpod.com in a “Draw It” activity.

2 - Students can draw pictures illustrating people that they can get help from if they feel angry, sad, or scared when they are online. This drawing was completed by a first grader on Nearpod.com in a “Draw It” activity.
Second grade

Description of Digital Citizen for second grade: In second grade, students should be part of discussions and lessons focused on being a “good” digital citizen, following safety rules for using technology in the classroom and at home, dangers that exist when online, as well as creating a positive digital footprint. Teachers should emphasize keeping personal information and passwords private as well as developing the understanding that what we do online leaves a permanent digital footprint. Simple student labelling of sources when using digital items that were created by someone else is sufficient for creating awareness of proper use of copyrighted items at the second grade level.

Some artifacts that second graders can create include drawings or other expressions that illustrate themselves showing positive safe behaviors and drawings or other expressions that show a positive personal identity.

Sample activity:
1 - Students can create a drawing that includes all of the things that make up our digital footprint. They could even include a photo of their own feet.

2 - https://youtu.be/IuQ4BKofvtE Students could use Flipgrid.com to record messages about how they will use technology safely. This is a sample of a 2nd grader recording herself talking about how she will take care of her school Chromebook. Note: All faces were pixelated for this Georgia CS Standards project.
Third grade

Description of Digital Citizen for third grade: In third grade, students should begin to demonstrate good digital citizen habits and understanding in the three elements under this standard: cybersecurity, intellectual property, and digital identity. Lessons that emphasize keeping personal information private is a vital part of circumventing cybersecurity problems. Discussions that create awareness of malware dangers as well as other cybersecurity issues is also important. At the third grade level, students should recognize and give credit for work they use that was created by others. Third graders should cite sources of print or digital media in a simple format. Through discussions and practice, third graders should become aware of their digital identity and recognize what behaviors can affect it.

Some artifacts and samples that third graders can create include:

**Cybersecurity:**
Students can create a safe username that doesn’t include personal information and then build a password that is strong and yet memorable. Students can start with a word or the first letters of the words in a phrase, then add numbers and symbols which can build a very strong password or username.

(Photo example of 3rd grade commonsense.org activity from the “Password Power-Up” lesson.)

**Intellectual Property:**
Students should list the websites where they obtain pictures, etc. for use in their academic work. This could be done on the page of its use or in a list at the end of a presentation or essay.
What conditions do Blizzards Have to have to make Blizzard?

By Eshan

A blizzard has to be three hours long to be an official blizzard.

A blizzard is only possible to form when the temperature is 20 degrees or lower. That could give you hypothermia.

Facts from:

A blizzard has winds as fast as thirty-five miles per hour!!! That could make roof cave-ins and trees breaking!!!

(Example of 3rd grade inquiry activity with a citation at the bottom)

Digital Identity:
Students can create a selfie of themselves (hand drawn or digital). Students can also discuss comments that might be made if that picture was posted, personal information or assumptions that might be gleaned from it, and what they might need to change or think about when creating selfies in the future.
(Example of a 3rd grade Commonsense.org activity from the “This is Me” lesson.)
Fourth grade

Description of Digital Citizen for fourth grade: In fourth grade, students should demonstrate good digital citizen habits and understanding in the three elements under this standard: cybersecurity, intellectual property, and digital identity. Lessons that emphasize keeping personal information private is a vital part of circumventing cybersecurity problems. Discussions that create awareness of malware dangers as well as other cybersecurity issues is also important. At the fourth grade level, students should recognize their responsibility to give credit for work they use that was created by others. Fourth graders should cite sources of print or digital media in a simple format. Through discussions and practice, fourth graders should be aware of their digital identity and recognize what behaviors can affect it and the identities of others.

Some artifacts and samples that fourth graders can create include:

**Cybersecurity:**
Students could create a clickbait styled header or ad for an academic report. (ex. Everyone’s asking - Who wrote the Declaration of Independence? Number 3 will surprise you!) The emphasis should be that the ad grabs attention, but is misleading in the content provided. (ie. There might not be anything surprising about the authors of the Declaration of Independence.)

Or, students could create a flipgrid video about Clickbait consequences like these students.
https://youtu.be/7vQe33SQt3A

**Intellectual Property:**
Students should list websites where information or graphics came from and when possible, include the author or organization where they obtain pictures, etc. for use in their academic work. This could be done on the page of its use or in a list at the end of a presentation or essay. Note in the above graphic, the photo has an attribution that was simply copied from Wikipedia where the photo was found.
Digital Identity:
Students could create a Scratch (https://scratch.mit.edu/) interactive story or quiz that illustrates how a person’s digital identity can affect themselves and others (friendships, education, or employment opportunities).

(Example - 4th grade Digital Footprint quiz - https://scratch.mit.edu/projects/345622776/)
Fifth grade

Description of Digital Citizen for fifth grade: In fifth grade, students should demonstrate good digital citizen habits and understanding in the three elements under this standard: cybersecurity, intellectual property, and digital identity. Lessons that emphasize keeping personal information private is a vital part of circumventing cybersecurity problems. Discussions that create awareness of malware, clickbait, and phishing dangers as well as other cybersecurity issues is also important. At the fifth grade level, students should give credit for work they use that was created by others. Fifth graders should cite sources of print or digital media in a simple or standard format. Through discussions and practice, fifth graders should be aware of their digital identity and recognize what behaviors can affect it and the identities of others.

Some artifacts and samples that fifth graders can create include:

Cybersecurity:
Students could create a map that illustrates how fast a phishing scam can travel. Start with 1 person that has 5 email contacts. If that person clicks the infected email and it sends to all contacts and if 2 of each of those contacts clicks the email and then sends to their contacts, it is easy to see how fast the number grows keeping in mind that people usually have 100+ contacts and the click rate might be higher.

Intellectual Property:
Students should list the websites and when possible, include the author or organization where they obtain pictures, etc. for use in their academic work. Fifth graders can begin to use a bibliography or citation list in a simple format.

Sources:
- Shedd Wildlife - Humane Wildlife Control
  https://www.sheddwildlifecare.com/5-raccoon-habits-you-should-know
- National Geographic
  https://www.nationalgeographic.com/animals/mammals//raccoon
5th Grade ESL Flipgrid assignment to create an explainer video on Copyright and plagiarism.
https://youtu.be/8TeS_Tz9kMQ

**Digital Identity:**
Students could record a video using Flipgrid or other software to explain how their digital identity can follow them for the rest of their lives. Students could do an “explainer” video (YouTube style) or they could work in partners or groups to film a simple scenario of a conversation between friends in a digital identity situation.
https://youtu.be/rJTFES2ZnZU