

Keeping Our Kids Safe & Healthy in a Digital World

A Technology & Digital Citizenship
Field Guide for ACPS Families



About this Guide

As our students grow up in a digital society, it is inevitable that technology will play an important role in their lives. Indeed, our children will engage with technology throughout their entire school career. At ACPS, we believe that it is our responsibility to partner with families, providing both you and your child with strategies for healthy and responsible technology use. We also believe in transparency regarding various policies and procedures for technology use in our division. We hope that this guide will help to answer any questions you may have as a family, as well as provide you with resources for raising a healthy digital citizen.

1 Table of Contents

- 2 Understanding the Acceptable Use Policy (AUP)
- 3 Device Care: What Happens if it Breaks?
- 4 Device Care: Some Common FAQs
- 5 Device Personalization
- 6 Keeping Students Safe Online in ACPS
- 7 How are Digital Resources Approved for Use?
- 8 What is Digital Citizenship, and Why Does It Matter?
- 9 **Digital Footprint:** What follows my child online, even after logging off?
- 10 **Cyberbullying:** What is cyberbullying?
- 11 **Healthy Habits:** How much is too much?
- 13 **Evaluating Information:** What's real, and what's fake?
- 15 **Fair Use & Copyright:** What content is my child allowed to use?
- 16 **Netiquette:** How do I help my child use the internet appropriately?
- 17 **Online Safety:** How do I keep my child safe online?

Understanding the Acceptable Use Policy ...or the "AUP"



Image courtesy MaxPixel, used under Creative Commons Zero - CC0

What is the Acceptable Use Policy (AUP)?

The AUP is a school board policy that guides the use of technology in Albemarle County Public Schools. If you'd like to view this policy, please visit the ACPS website or request a paper version at your school's front office.

All use of the Division's technology must be:

- In support of education and/or research
- For legitimate school business.

ACPS School Board Policy IIBE

What is the purpose of the AUP?

The purpose of the AUP is to communicate division expectations for using school technology. It is important that students and families understand these expectations as technology plays a significant role in our schools.

What happens if my child violates the AUP?

We understand that mistakes happen. If a child violates the AUP, this behavior will be investigated and addressed by a school principal or division administrator.

Can I get a copy of the AUP in a different language?

Yes, of course--please work with your school to get a copy of a translated AUP.

Device Care: What Happens if it Breaks?

The Department of Technology has guidelines and procedures in place for device repair and even replacement when necessary.

I think my child's device is broken...what happens next?

Our schools have steps to follow when devices are broken or in non-working condition. Generally, the first step is to talk to the student's teacher or school administrator. From there, assistance will be given. The student can also check out a loaner device through the library or the student Help Desk (if the school has one).

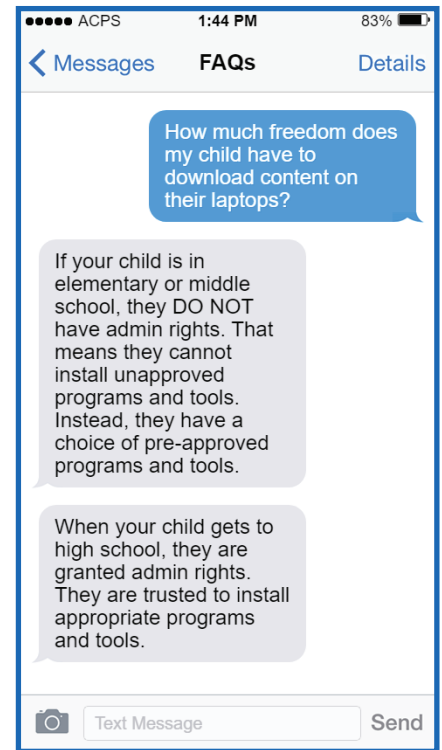
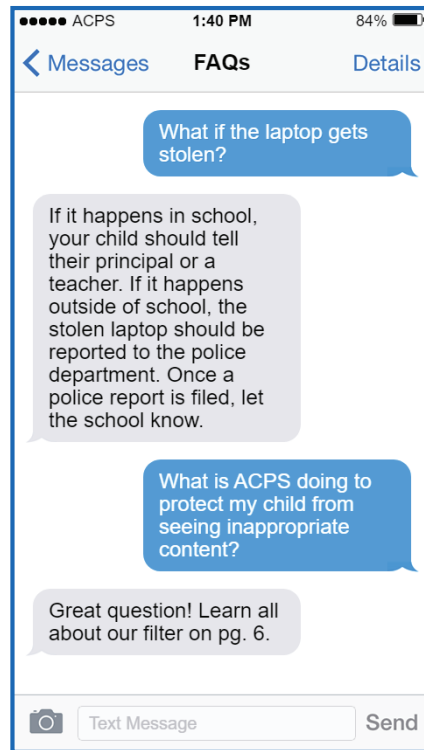
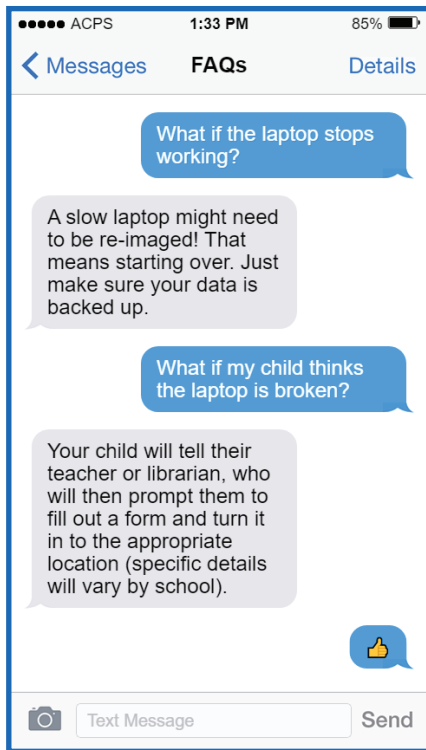
Who Fixes the Device?

ACPS Technology Support Specialists (TSS) who support their schools are certified to repair both Lenovo and Dell laptops. Student Help Desk members assist the TSS in conducting these repairs. Our ACPS Student Help Desk is a program that encourages students to serve as technology leaders and offer first level technology support to their school community. If you are interested in your 6th - 12th grade student participating in the ACPS Student Help Desk, please contact your school.

Do school computers come with device insurance?

All ACPS laptops come with a one-year warranty. We have additional accidental coverage on laptops that are brought to and from school on a daily basis.

Device Care: Some Common FAQs



Device Care: Some Dos and Donts

Your Child Should:	Your Child Should NOT:
• Keep the device protected • Carry it with two hands • Keep it away from food, drinks, and anywhere it can get really hot or cold • Keep the charger handy • Use the device in a safe and responsible way • Restart the device when things aren't working well	• Carry the device by the lid • Let someone borrow the laptop • Give someone the password • Change the operating system or hardware • Pick the keys off the keyboard

Device Personalization



Image taken by Alfred Toole, ACPS Learning Technology Integrator

What level of access do students have to personalize the laptop issued to them?

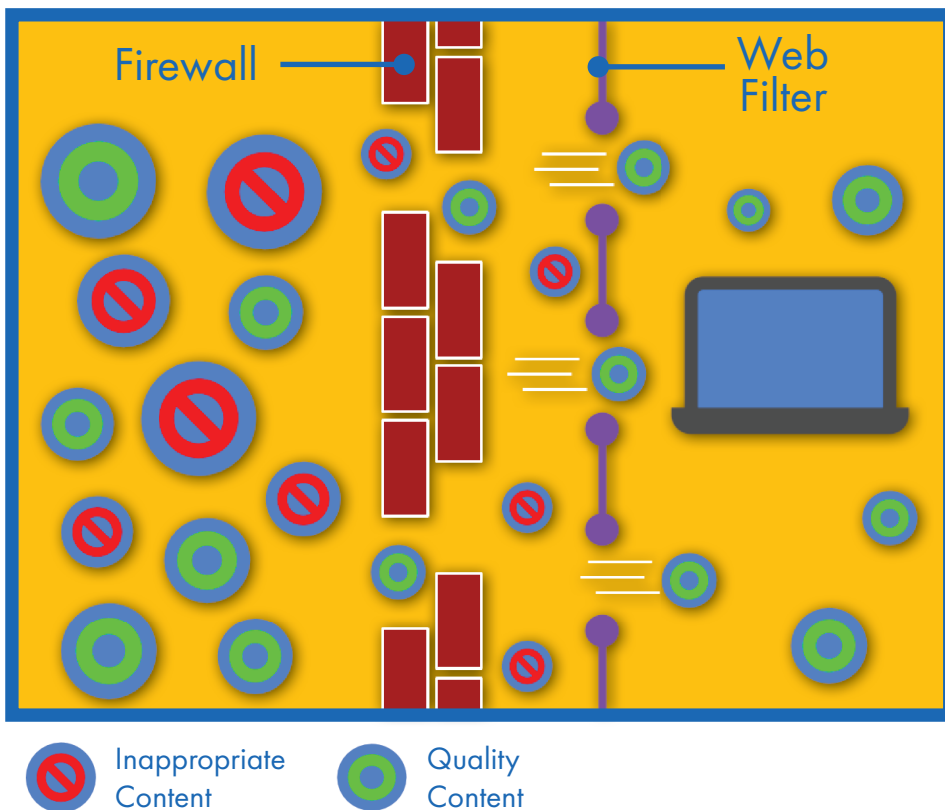
From the start, the district recognized that the most critical component of digital equity may be whether or not the students and teachers possess the literacy to take advantage of the available tools. Both students and teachers need the opportunity to develop the skills, knowledge, and attitudes to become confident, innovative, and creative learners who can harness the requisite technology to support themselves as expert learners. Therefore, the district designed their 1:1 program to allow for flexibility, choice, and customization.

In grades 3 through 8, all students can personalize their device. They are able to change the look and feel of the device. They also can install software that has been vetted and approved by their school principal.

ACPS provides students in grades 9 through 12 greater independence with their devices. They can install additional programs to meet a wide range of learning needs. This independence also gives our high school students more ways to practice managing their technology in a safe and responsible manner.

Keeping Students Safe Online

The internet is filled with content of all varieties: good and bad, appropriate and inappropriate. The Department of Technology believes that students should have open access to rich learning materials and opportunities through the web, but also understands the need to keep students safe and happy while using their device. As such, we have a filtering system in place to ensure that your child is as protected as possible from illicit content.



The web filter works in two stages: the firewall and the content filter. The firewall serves as a first line of defense against hacking, protecting the ACPs network from outside attacks. The content filter then steps in to weed out inappropriate content, blocking certain websites and search terms.

Our school division is required to filter internet content to be in compliance with the Children's Internet Protection Act (CIPA) enacted by Congress.

What happens if inappropriate content makes it through the filter?

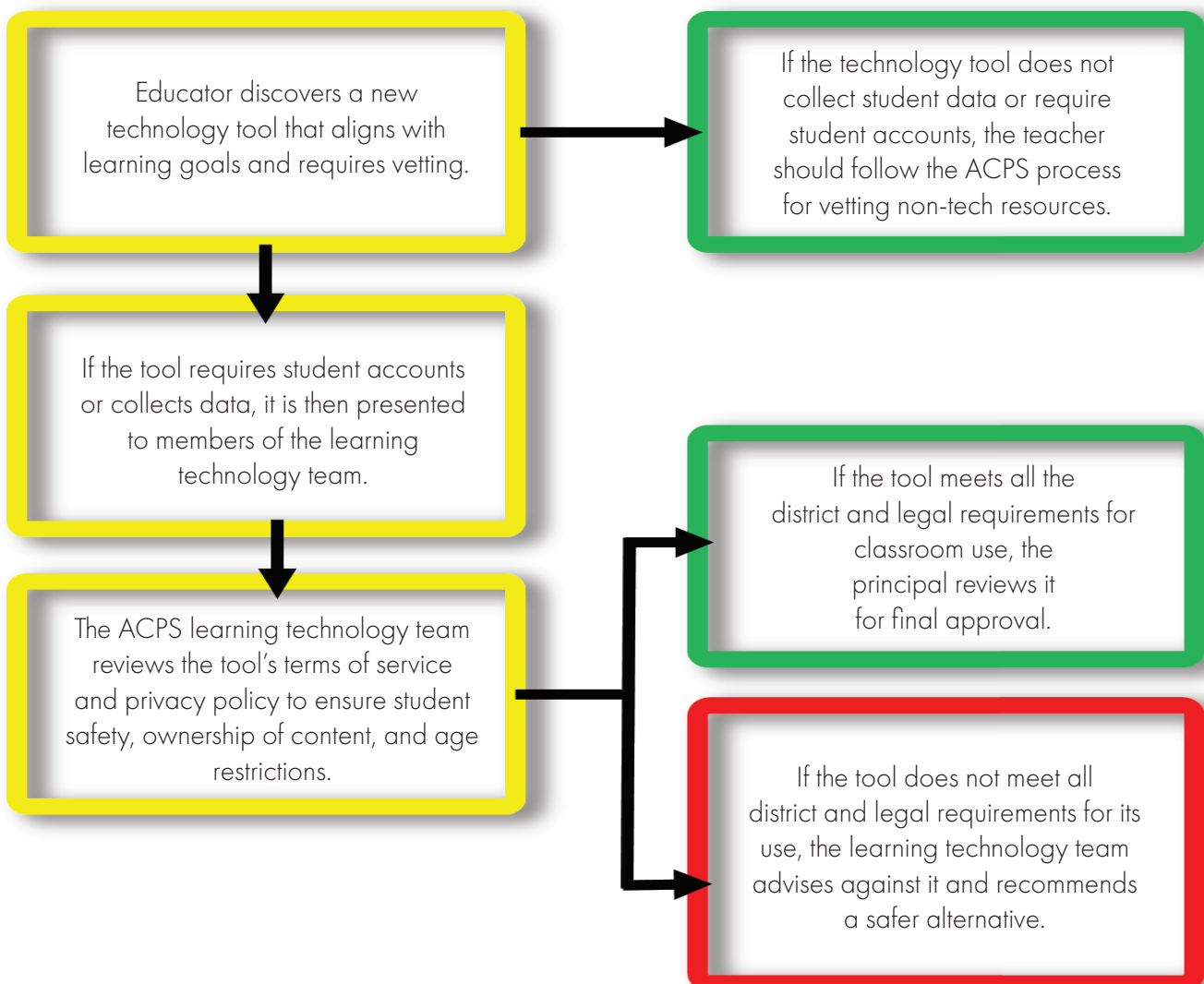
Filter systems are not perfect. Through our digital citizenship curriculum students are taught to close their laptop if they encounter upsetting or worrying content, and immediately inform a teacher. The teacher will then take appropriate steps to get the content blocked. The filter still works when your child uses an ACPs device at home, but if your child experiences this result at home, please contact your child's teacher. Do not include a link to the content in any email communications - just describe the incident.

How are Digital Resources Approved for Use?

The world of technology is full of countless programs and learning experiences that can offer students unique and meaningful opportunities. However, within these resources, there is often times a “fine print” that when overlooked can put your child’s safety and personal security at risk. The school division has a vetting system that continuously reads and reviews terms of service and privacy policies to ensure the programs used in the classroom serve an educational purpose that is safe.

Vetting a Digital Resource

A Step-by-Step Flow Chart



What is **DIGITAL CITIZENSHIP** ...and why does it matter?

ACPS students and families are all part of the same community. As a part of that community, we have a shared responsibility to promote safe, kind, and healthy behaviors. Good citizenship involves making choices to create a better community.

Citizenship in a digital world echoes the same behaviors of good citizenship in daily life. Just as we guide students to consider the effects of any choice, we must also teach them how to do this online. Technology changes at a fast pace. It is challenging to keep up with specific trends or the latest apps. Consequently, students must be able to adapt to a changing world. They must also apply their critical thinking skills and personal philosophies to ever changing digital experiences.

By putting devices in student hands, we become partners with families in empowering our children to make healthy, smart, and safe choices. We are united with our community in providing opportunities to discuss topics relevant to life in a digital world.

A strong digital citizenship curriculum gives students foundational knowledge and opportunities to discuss their perspectives surrounding topics such as privacy, screen time, and evaluating information online. This guide is an overview of the digital citizenship domains, as well as ways in which you can discuss them with your child at home.

Digital Citizenship Badging Initiative

ACPS teachers support digital citizenship and web-safety through a badging initiative and robust curriculum. Associated with each domain is a badge. Seeing one of these badges on your child's computer is an indication that they have completed a lesson in this domain. This badge provides a great opportunity to engage in conversation with children about what they have learned!



Digital Footprint

What follows my child online, even after logging off?



What's the deal?

A Digital Footprint is described as any online activity that has your name tied to it. Such activities include posts on social media (videos, photos, text, etc.) and "liking", "sharing", and "commenting". As stated by Google, "just as your footsteps leave prints on the ground while you walk, what you post online leaves a trail."

Your Digital Footprint

What follows you online?



Did you know?

No online activity is ever truly deleted. Even if it's deleted by you, it may be stored on a server in another location.

Colleges and employers sometimes investigate a candidate's digital footprint as part of the application process.

Conversation Starters

What kinds of information do you feel comfortable sharing online and why? Would you be comfortable with your grandmother seeing this activity?

What do you think happens when you delete something you've done or posted online?

Experts Recommend...

- Encourage your child to think before they post: is it true, helpful, inspiring, or kind?
- Be a role model: talk with your child about the privacy settings you use on your phone and share your process for deciding what you share with whom.
- Try Googling yourself. You may be surprised at the results, and what information you thought was private isn't.

Dive Deeper

- Oversharing - Think Before You Post: bit.ly/thinkb4posting
- Conversation Case: Young Children and Digital Footprints: bit.ly/youngdigitalfootprints
- Family Tip Sheet on Digital Footprint: bit.ly/digitalfootprintfamtips
- Digital Reputation: What Comes Up When You Google Yourself?: bit.ly/digitalreputationvideo

What's Happening in School?

Currently, students learn about the importance of a digital footprint through the ACPS digital citizenship curriculum. Please contact your school principal for details about where and when digital citizenship lessons occur.

Cyberbullying

What is cyberbullying?



What's the deal?

Cyberbullying is bullying that happens online. This includes sending, posting, or sharing content about someone else that causes embarrassment or humiliation. As with traditional bullying, in cyberbullying, the victim has less power than the bully (more popular, older, bigger, stronger, etc.), and the actions are repetitive.

Signs of Cyberbullying

VICTIM:

- Secretive with device
- Changes in mood after being online
- Appears uneasy about going to school
- Becomes withdrawn



BULLY:

- Closes app or hides screen around adults
- Uses device all night
 - Laughs excessively while online
 - Overly concerned with social status

Did you know?

Cyberbullies are often good students with positive reputations (Parents Guide to Online Safety, pg. 23)

Supporting victims can make a BIG difference, even if you don't know them well.

Most teens report experiencing cyberbullying.

Conversation Starters

Before posting, do you how it might impact others?

What would you do if you were a witness to cyberbullying? How about if you were the victim?

Experts Recommend...

- If you notice signs of your child being bullied, encourage them to ignore the bully, take screenshots and gather evidence, then contact your child's school counselor or administrator. If the content is threatening or explicit, you may also contact your local police department.
- Make sure your child feels comfortable and understands they won't get in trouble for reporting online issues.
- Teach your student the importance of being an upstander when they witness mean things online.
- If your student is struggling with digital drama, help them reflect on whether they need a break from tech.

Dive Deeper

- Conflict vs. Bullying: bit.ly/conflictvsbullying
- Plugged-In Families: Cyberbullying & Digital Drama: bit.ly/cyberbullyingparentguide
- Helping Kids Fight Cyberbullying: bit.ly/kidsfightcyberbullying

What's Happening in School?

The ACPS digital citizenship curriculum addresses cyberbullying for students in grades 3-8. Contact your child's principal for more information on delivery of this curriculum. Additionally, ACPS also has an anonymous student reporting app for cyberbullying and threatening content, which can be used by secondary students and families.

Healthy Habits

How much is too much?

What's the deal?

Healthy habits consists of balancing appropriate screen time for each age group, teaching students self-control when it comes to “screen addictions”, and identifying how perceptions of others on social media can influence behaviors and feelings. While there are recommended time limits, [Common Sense Media](#) identifies that some screen time is more beneficial than others, and the most important thing is to find the right balance. Balance includes getting adequate sleep, physical activity, and time away from the screen.



...set aside time to spend as a family.



...ensure you spend time outside.



...set aside time to interact online.



...create higher-quality screen time.

Use a Family Media Plan to...

Healthy Habits in the Real World

Check out these articles related to Healthy Habits:

- “To Grow Up Healthy, Children Need to Sit Less and Play More” from the World Health Organization: bit.ly/childrensitless
- “I Embraced Screen Time with My Daughter and I Loved It”: bit.ly/embracescreentime
- “Screen Time for Kids Under 2 More Than Doubles”: bit.ly/changesinscreentime
- “How Much Screen Time is Too Much for Kids?”: bit.ly/screentimebalance

What's Happening in School?

- Students learn about the importance of a healthy media diet through digital citizenship curriculum. Please contact your school administrator for details about where and when digital citizenship lessons occur.
- Physical education and health classes emphasize the importance of getting physical activity each day.
- Most schools offer opportunities for extracurricular activities. These can be a great way for students to balance their time spent online.
- Teachers learn about how to integrate technology purposefully. That way, the time students spend on laptops is aimed at expanding student thinking rather than replacing paper and pencil with a laptop.



Did You Know?

Social media can and often does have a strong influence on student behaviors and feelings.

You can set restrictions and time limits on video game consoles, cell phones, internet, and most other devices.

The average amount of time kids under 8 spend with mobile devices each day has tripled twice since 2011. Teenagers use an average of nine hours of media per day, and tweens use an average of six. (Common Sense Media)

Conversation Starters

What do you like to spend most of your time doing... (on your laptop, on your phone, on the tv, etc.)?

How do you know when to take a break from the screen? Are there signs that you look for?

Have you ever stayed up too late because of media?
How did it make you feel the next day?

Do you have friends or follow people that represent themselves differently on social media than in real life?

How do you think I (the family) would feel if you took away my facebook?

Experts Recommend...

- Try creating screen free zones and times in the house - family media plans can help outline this!
- Try creating a customized family media plan: bit.ly/aapfamilymediaplan
- The American Association of Pediatrics recommends that "all children and teens need adequate sleep (8-12 hours, depending on age), physical activity (1 hour), and time away from media."
- Going through and customizing a family media agreement: bit.ly/familymediaagreement
- Keep in mind, rather than just setting rules, it's important to talk it through with your child and acknowledge and understand that media may be a big part of his/her life. This is about finding balance with reasoning.
- Watch and explore together! Spend time with your student on high-quality and age-appropriate media. Common Sense has lots of family reviews for TV, movie, games, apps, and websites.

Dive Deeper

- Media Use Recommendations for Preschoolers: bit.ly/preschoolagemediause
- Can flip phones end our social media addiction?: bit.ly/cellphonetedtalk
- Social Media & Self Image: bit.ly/socialselfimage
- Social Media & Self Esteem: bit.ly/socialselfesteem

Evaluating Information

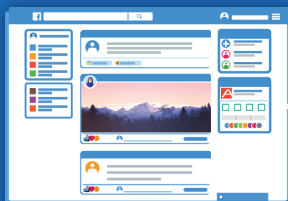
What's real, and what's fake?

What's the deal?

The internet allows access to an enormous amount of information which can be viewed at any time. As a result, students are able to conduct research for school projects and stay up to date on current events. To make sure that the information is correct, it is important for students to know that not everything online is true. There are several habits that can be adopted to ensure a safe and accurate web search:

- Cross referencing facts in order to uncover possible bias
- Not sharing sensationalized news articles
- Using fact checking websites for confirmation

In addition to credible searches, students should also be aware of email phishing, clickbait, and the risk of downloading corrupt files associated with these concerns.



Just because
something is popular or
trending online, does not
mean it is true!

It is best not to share
anything online until
you have fact-checked
it first!



Healthy Habits in the Real World

- The Very Real Consequences of Fake News and Why Your Brain Can't Ignore Them: bit.ly/fakenewsconsequences
- Scammers use phishing emails to steal \$100 million from Facebook and Google: bit.ly/facebookphishingscam
- Phishing Scam Targets Verizon Customers: bit.ly/verizonphishingscam

What's Happening in School?

- Many students learn about evaluating information through a research unit. However, more subject area teachers are starting to address information literacy because students need this skill to evaluate information across subject areas.
- Some schools have elective courses dedicated to computer literacy, including units on evaluating information.
- Students learn about the importance of evaluating information through the digital citizenship curriculum. Please contact your school administrator for details about where and when digital citizenship lessons occur.



Did You Know?

80% of middle school students in a [Stanford study](#) mistakenly identified a sponsored advertisement as a news story.

Less than 1 in 3 students are skeptical of biased news sources.

Research has shown that false stories are more likely to be spread by humans than by bots. ([Science Mag](#))

Phishing allows scammers to collect personal information by pretending to be a reputable company.

Clickbait is a link on a website or in a text message that can lead you to harmful or false information.

Conversation Starters

What kinds of news sources do you trust to report accurate and unbiased information?

Do you think it is important to verify sources before sharing news or links? Why or why not?

Where online do you find yourself learning most about what's going on in the world?

What kinds of stories or headlines do you think get the most clicks or likes? Why?

If your child shares information with you about a fact or current event they learned, it's a good opportunity to question their resources and what makes them believe it.

Experts Recommend...

- Teach your child to cross check news stories or facts, just like real-world fact checkers. Students should learn to check other available resources instead of just trusting a website, post, or picture.
- Verify information before sharing it!
- Learn that just because something is popular or trending, does not mean it is true. Searching for information about the source is helpful!

Dive Deeper

- Skills and Strategies/Fake News and Real News: bit.ly/realvsfakeskills
- Fake News - Keepin' it Real: bit.ly/stoppingfakenews
- Factitious Quiz: Can you tell real from fake news?: bit.ly/factitiousquiz
- How to Recognize and Avoid Phishing Scams: bit.ly/nomorephishing
- Check the accuracy of claims and news about politics using Politifact: [politifact.com](https://www.politifact.com)

Fair Use & Copyright

What content is my child allowed to use?



What's the deal?

The internet makes it easy to find and use other people's work: photos, videos, music, etc. It's important to talk to your child about copyright law and fair use so that they develop a sense of respect and fairness. Kids can avoid the serious consequences of plagiarism and piracy by learning that the internet is not a free-for-all. Training kids to ask "Do I need permission to use this?" and "Is the creator being given credit or paid?" are great first steps.

Did You Know?

Plagiarism was one of the most reported misbehaviors online for ACPS students in grades 6-12.

Pirated files are more likely to contain spyware which can steal your personal information.

Illegal streaming and downloading may result in fines and legal actions.

Your identity can be easily tracked when using torrents or peer-to-peer file sharing.

Conversation Starters

Do you ever download music, movies, TV shows, or games from the internet? What services do you use?

What are some ways we can listen to music or watch TV/movies without illegally downloading?

How would you feel if someone used your creative work without your permission?

Why is it important for a musician or artist to get credit and/or money for their work?

Experts Recommend...

- Encourage legal downloading and sharing: there are legal ways to stream music, movies, and more for free.
- Discuss the consequences of piracy - using peer to peer sharing sites can be illegal, can give your device viruses, and make you vulnerable to identity theft. They also prevent creators from getting paid. That's not fair!
- Encourage your child give credit to the work they use: students are taught to use citations for research papers in school, but this also applies to things like video mash ups or memes.
- Take ownership of your work: if you are creating original work like music, drawings, or videos, be sure to make sure you are clear about giving credit.

Dive Deeper

- Copyright Quiz - for you and your child to take together: bit.ly/quizcopyright
- Fair Use FAQ: bit.ly/fairusefaq
- Teaching Copyright Resources: bit.ly/resourcescopyright
- How Sketchy Streaming Sites Really Work: bit.ly/sitescams

Netiquette

How do I help my child use the internet appropriately?

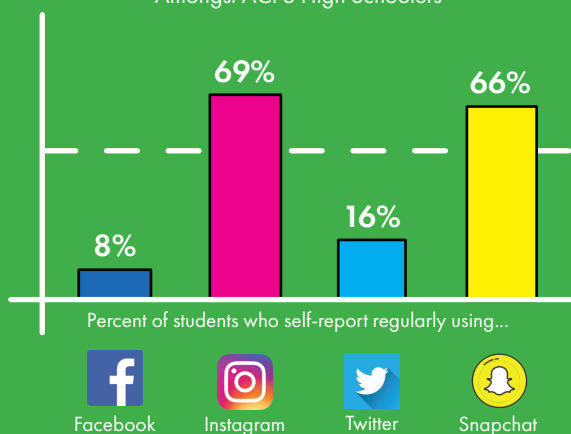


What's the deal?

In an online environment it isn't possible for others to read your body language, tone of voice, or facial expressions. Therefore, a suggested set of guidelines has emerged for online communications, called "netiquette". People sometimes use their devices as a mask to say things they wouldn't particularly say in person. Proper "netiquette" can teach students how to foster a positive online community and de-escalate any "digital drama."

Social Media Use

Amongst ACPS High Schoolers



* data reported from 2018-2019 SpeakUp survey

Experts Recommend...

- Don't spam others or share your contact lists.
- Know your jokes, sarcasm, and language can be misinterpreted.
- Avoid gossip and rumors online.
- Don't send or forward pictures you would not be willing to share with your families.

Dive Deeper

- Instagram's Family Guide: bit.ly/parentgram
- Instagram's pilot of new settings: bit.ly/grampilot
- How 4chan has become connected to threats of violence: bit.ly/4chanarticle
- Examples of Bad Netiquette: bit.ly/badnetiquette

Did You Know?

Instagram is piloting a new "nudge" feature that warns users when they're about to post something hurtful.

Some online forums are anonymous (examples: 4chan and 8chan) which can make them vulnerable to hate speech, inappropriate behaviors, and risky content.

91% of all social media users access social channels via mobile devices.

Conversation Starters

Do you communicate differently on a classroom message board or when emailing a teacher than you would on social media or texting with your friends?

Have you ever posted something that you wouldn't have said in person?

Have you ever posted something that got misinterpreted?

If someone said something that you found offensive, how would you react?

Online Safety

How do I keep my child safe online?

What's the deal?

It's necessary for kids to understand the importance of privacy online, and how to use privacy and location sharing settings to protect their information. Children must also consider how to interact with people they do not know online, and what to do if someone starts to make them feel uncomfortable. Safe searching and filtered searches help ensure that kids do not accidentally see inappropriate material online. Additionally, children should understand their responsibility in what they search for - if they type something inappropriate into a search engine, they are likely to end up with upsetting results.



Finding quality web content can be a challenge. Help your child navigate the internet by encouraging them to talk with you when they aren't sure if content is safe.

Online Safety in the Real World

- Amazon Flunks Children's Privacy, Advocates Say: bit.ly/echodotprivacy
- Don't Fall for It: A Parent's Guide to Protecting Your Kids from Online Hoaxes: bit.ly/hoaxguide
- Real World Reasons Families Should Care About Kids' Online Privacy: bit.ly/kidsonlineconcerns

What's Happening in School?

ACPS takes student's privacy, personal information, and safety very seriously. As part of the ACPS Digital Citizenship Curriculum, students learn about strong passwords, browsing the internet safely and securely, and determining what information is appropriate to post to the web. Of course, students make mistakes, so we have firewalls, web filters and other monitoring in place to help ensure that what makes it to a student's device is safe and appropriate. Read more about these filters on page 6.

Social Media Safety Tips



Most social media platforms have robust privacy settings that control who can see your posts. Consider setting them to "Friends Only", especially a child's account.

Snapchat has a feature called Snap Maps where all your Snapchat contacts can see your current location if you do not turn it off.



If you don't know them, don't accept their friend request!

Most smartphones "geo-tag" pictures with the location it was taken, making your location visible once the photo is posted. Turn this off in your camera settings.





Did You Know?

Children **under the age of 13** who are on social media have either claimed they were 13 years or older or have indicated they've received family permission. The Children's Online Privacy Protection Act (COPPA) **prohibits** children to use such sites otherwise.

Warning signs of a child being targeted by an online predator include: spending long hours online (especially at night), receiving phone calls from people they don't know, suddenly turning off the computer when you walk into the room, withdrawal from family life, reluctance to talk about online activities, and unsolicited gifts arriving in the mail. (KidsHealth, "Internet Safety")

According to the New England Journal of Public Policy, contact with online predators happens mostly in chat rooms, on social media, or in the **chat feature of a multiplayer game** (Roblox, etc).

Conversation Starters

What are some ways we can protect our privacy when we go online?

In what situations would you share your location? Why is it important to be thoughtful about location sharing?

What information would be okay to share with a friend you know from school versus a friend you met through online gaming?

Who is responsible for what you Google?

Have you or any of your friends ever seen something online that made you uncomfortable? What was it?

What makes a strong password? Why is it important to have a strong password? Why shouldn't you share a password with friends?

Experts Recommend...

- Teach your child what to do when they see something threatening, worrying, or upsetting online. Emphasize that they will not get in trouble for telling you, ensuring them that you are a safe person to talk to.
- Keep computer and device use in common family areas.
- Talk to your child about "red flags" when talking to someone online. Questions like "Are you a boy or a girl?", "Where do you live?" or "Do you want to talk privately?" are signals to stop talking and tell an adult.
- Teach your child how to turn off location sharing on their devices, and discuss under which circumstances you might want them turned off (increased privacy and safety) or turned on (using a map app for navigation).
- Spend time online together to teach your kids appropriate online behavior.

Dive Deeper

- Media Smarts Internet Safety Tips by Age Level: bit.ly/safetytipsbyage
- Privacy and Security Family Activity: bit.ly/famsecurityactivity
- Myths & Truths of Kids' Internet Safety: bit.ly/online myths and truths

Created by the
The ACPS Department of Technology

twitter: @acpslearntech

Questions or Comments? Email us at:
learningtech@k12albemarle.org

Resources based on Common Sense Media
and BeInternetAwesome by Google