

SETTING CONDITIONS FOR SUCCESS:

DRAFT

A Guide for Creating
Effective Responsible Use Policies





Equitable Connectivity Is a Critical Foundation

Providing equitable digital access to all learners is a critical foundation for their success in learning and life. However, providing this access comes with a great responsibility to help young people learn to be safe and responsible in their online activities. It also comes with a duty to build healthy habits, such as using technology to encourage curiosity and seeking help from a trusted adult when something goes wrong.

Creating the conditions for the safe and effective tech use in schools requires both technical policies to be implemented by IT staff and establishing appropriate behavior expectations for students.

Setting Technical Conditions for Success

While this guide focuses on the creation of effective Responsible Use Policies* (RUPs) - agreements students are asked to sign to indicate their understanding of how to responsibly use their school account and devices - it's important to note that there are also technical protections that schools should have in place to prevent student harm.

In the U.S., the Children's Internet Protection Act (CIPA) requires any school that accepts federal funding to help cover the cost of internet access to establish specific policies before allowing access to the school network.

According to guidance from the Federal Communications Commission (FCC), such protections should address:

- Restricting access by minors to content that could be inappropriate or harmful on the internet.
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.
- Unauthorized access, including so-called "hacking" and other unlawful activities by minors online.
- Unauthorized disclosure, use and dissemination of personal information regarding minors.
- The school's monitoring of minors' online activities.

**Note: Although many refer to these policies as Acceptable Use Policies, the preferred term is Responsible Use Policies.*

Responsible Use Policies

The Protecting Children in the 21st Century Act, enacted after CIPA, requires schools to educate students about appropriate online behavior, including interacting with other individuals online and cyberbullying awareness and response.

In addition to having a technical policy for keeping children safe, a good practice is to include an RUP that outlines student behaviors that lead to a healthy digital culture at school and home. RUPs, provided to students and families at the beginning of the school year, can be great tools to establish the optimal conditions for effective tech use in schools. Unfortunately, many current RUPs have been developed in a way that does not help create effective conditions or help students.

But when we establish expectations for meaningful and civil online behaviors, we not only allow our children to be their best selves online, we prepare them to bring out the best in others.

RUPs Gone Wrong

There are several common pitfalls to watch out for when it comes to creating RUPs. The two most common are using language that's too complicated or confusing for a student to understand, and focusing entirely on what *not to do*, without putting any emphasis on establishing what we want students *to do* with the technology.

Before looking at best practices for creating RUPs, let's take a look at some examples of RUPs that are not effective. In this section, we'll share excerpts from actual RUPs that have missed the mark and explain why.

Overly Negative

<p>Users shall not use the network or technology, including access to the internet, intranet, collaboration tools, bulk communication tools, social media, or email to use, record, share, upload, post, mail, display, store, or otherwise transmit in any manner, any content, communication or information that:</p> <ol style="list-style-type: none">1. Is hateful, harassing, threatening, libelous or defamatory;2. Is offensive or discriminatory to persons based on race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, place of residence or business, or status as a victim or family member of a victim of domestic violence, a sexual offense, or stalking;3. Constitutes or furthers any criminal offense, or gives rise to civil liability, under any applicable law, including, without limitation, U.S. export control laws or U.S. patent, trademark or copyright laws;4. Constitutes use for, or in support of, any obscene or pornographic purpose including, but not limited to, the transmitting, retrieving or viewing of any profane, obscene, or sexually explicit material;5. Constitutes use for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass, threaten or stalk another individual;6. Contains a virus, trojan horse, ransomware or other harmful component or malicious code;7. Constitutes junk mail, phishing, spam, or unauthorized broadcast email;8. Violates the security of any other computer or network or constitutes unauthorized access or attempts to circumvent any security measures;9. Obtains access to another user's DCPS network account, files or data, or modifies their files, data or passwords;10. Impersonates any person living or dead, organization, business, or other entity;11. Degrades the performance of, causes a security risk or otherwise threatens the integrity or efficient operation of, the network or technology;12. Deprives an authorized user of access to the DCPS network or technology;13. Obtains DCPS technology or DC network access beyond those authorized;14. Engages in unauthorized or unlawful entry into a DCPS Network system;15. Discloses confidential or proprietary information, including student record information, without authorization or without proper security measures;16. Discloses or transmits personally identifiable student information, videos and photographs without authorization or without proper security measures;17. Shares confidential information about students or DCPS personnel in a manner that violates DC law, federal law, regulations, policy or guideline;	<ol style="list-style-type: none">19. any other DCPS policy;20. Enables or constitutes wagering or gambling of any kind;21. Accesses, distributes, downloads or uses unauthorized games, programs, files, electronic media, and/or stand-alone applications from the internet that may cause a threat to the DCPS Network22. Promotes or participates in any way in unauthorized raffles or fundraisers;23. Promotes or participates in any way in partisan political activities;24. Promotes or participates in any way in internal political or election activities related to a union or other organization representing employees;25. Engages in private business, commercial or other activities for personal financial gain;26. Distributes unauthorized information regarding other user's passwords or security systems;27. Falsifies, tampers with or makes unauthorized changes, additions or deletions to data located on the DCPS network or any school systems;28. Accesses or uses data located on a DCPS Network for personal uses;29. Promotes or participates in any activity or relationship with a student that is not related to academics or school-sponsored extracurricular activities, unless authorized in advance in writing by the principal and the student's parent/guardian;30. Installs, downloads or uses unauthorized or unlicensed software or third-party system;31. Violates the terms of use specified for a particular technology, application or DCPS network system;32. Constitutes use that disrupts the proper and orderly operation of a school or office;33. Engages in hacking (intentionally gaining access by illegal means or without authorization) into the DCPS network to access unauthorized information, or to otherwise circumvent information security systems;34. Engages in inappropriate sexual conduct, including unwelcomed sexual contact, indecent exposure, transmitting sexually suggestive images, or other sexual activities; or35. Violates any prohibition noted in this policy or any other DCPS policy.36. Shares DCPS email addresses or distribution lists for uses that violate this policy or
---	---

In the example above, the RUP lists 35 things not to do with technology, but didn't include a single example of what to do with the technology. An effective RUP balances behaviors that are not permitted with competencies that should be practiced and developed by students. After all, you can't practice not doing something, and being an effective digital citizen takes practice!

Unnecessarily Complicated Language

“Transmission of any material in violation of any federal or state law or system policy is strictly prohibited. This includes, but is not limited to, threatening or obscene material, material protected by copyright or trade secret, material used for commercial activities by for-profit institutions, and material used for product advertisement or political lobbying. Students will be informed of issues regarding network etiquette, security and vandalism with the understanding that any violation of the regulations is unethical and may constitute a criminal offense or violation of acceptable student conduct and therefore require appropriate disciplinary action.”

“The use of proxy-type resources or other services with the express technical intention of circumventing the district’s cybersecurity measures are expressly and permanently prohibited.”

In the examples above, the schools missed the purpose of an RUP. Instead of establishing the conditions for effective technology use, it is providing complex legal language that most students would never understand.

Liability Prioritized Over Learning

“If a student violates any of the provisions outlined in this policy, his/her access will be terminated and may constitute a criminal offense resulting in legal action.”

“We make no warranties of any kind, expressed or implied, for the network service provided and are not responsible for any loss, damages, costs, or obligations arising from use of your account.”

In the examples above, the language used appears to be prioritizing shielding the school from legal action over helping set the right conditions for learning.

If your school’s RUP has any of the elements shown above, it’s time for an update!

Creating an Effective RUP

Having learned from some ineffective RUPs, let’s now look at how to create an effective RUP. An RUP should guide students in being successful, effective digital citizens, rather than being focused on legal protections. And it should be written to meet students’ levels of understanding. You may want to consider having separate RUPs for elementary students and secondary students.

Keep these three tenets front and center when creating or updating a Responsible Use Policy:

- 1. Keep it positive.** RUPs should not be a long list of don’ts. Instead, make it mostly about the do’s of technology use.
- 2. Write in plain English.** This isn’t a real estate contract or a piece of legislation. Keep the language conversational and human-friendly.
- 3. Involve students.** As you develop the expectations, allow students to have input, make suggestions and ask questions. Students should understand the policy and the reasons it was created and implemented.

Finally, as we’ve all experienced, technology changes rapidly! Review your RUP annually to be sure any outdated technology is removed and guidance on new tools or resources you plan to use are added.

What to Include

Remember, RUPs are learning tools. Everything that's included in the policy should guide students in becoming confident, effective digital citizens. The following elements should be included in an effective RUP.

Purpose

Start with a clear purpose that helps students understand why the agreement is so important. Such a statement might include a reminder that using school-provided technology is a privilege, or that technology can be a powerful tool for learning if used appropriately.

Desired Digital Behaviors

The bulk of an effective RUP should focus on identifying desired digital citizenship skills.

Remember, desired skills should be framed as "dos" instead of "don'ts" whenever possible. It might help to frame the policy using "I am" or "I will" statements. As you state the desired digital behaviors, consider using the digital citizenship skills developed by the Digital Citizenship Coalition as a guide. These skills include teaching students to be:

- Informed - Students should know how to use technology to support learning and curiosity.
- Inclusive - Students should make sure they are respectful of others and see the value of differing viewpoints.
- Balanced - Students should practice balancing tech use with other activities and recognize which digital activities have more value than others,
- Engaged - Students should use technology to make their school and local community better and help solve problems.
- Alert - Students should practice principles of online safety and create safe spaces for others.

Remember to stick to behaviors vs. listing specific technologies or websites (e.g. TikTok or Discord) as they change regularly, dating the agreement unnecessarily.

Resolving Problems

One of the most important, yet often overlooked, parts of a good RUP is guidance for what to do if something goes wrong. Nobody is perfect and all students will likely do something that is not in line with the RUP at some point. When that happens, how should they respond? Who should they tell? And what are the consequences for not following the agreement? One of the most important things for a young person to learn is the value of getting help from a trusted adult when something goes wrong online. As such, the consequences shouldn't be written in a way that seems so threatening that a student might be afraid to get help when needed.

Signature

Create a place for students to sign that they agree to the code of conduct outlined in the policy. You may also consider adding a parent signature as well. If there is a problem with digital behavior down the road, it may be helpful to pull out the signed RUP and remind students that these were the behaviors they agreed to.

Responsible Use Policy Template: Elementary School

The following is a model RUP you can adapt for use with younger students. You can adjust the language and elements of the template below to fit your unique school culture and goals.

RESPONSIBLE USE POLICY

Using your device is a privilege, and any privilege comes with responsibility. Here are the expectations for using personal devices at school or anytime you are using school-provided devices.

How should I use technology?

- I will use my device when a teacher asks me to, during my own study time or during breaks.
- I will put my devices away when a teacher says it's time for a device break.
- I will ask for permission before downloading any new apps or software.
- I will take care of any devices I am given access to.

What should I do with technology?

- I will use my device to bring new information to support class activities.
- I will use my device to check information to verify that it is accurate.
- I will use my device to learn new things.
- I will give credit to the creators of information or media that are not my own.
- I will respect the district network's security measures.

How should I interact with other people?

- I will be a good cyber-friend, including being honest and kind in my digital communications.
- I will let a teacher or parent know before contacting someone online I don't already know in person.
- I will only share appropriate content with others.
- I will not share personal information (e.g. home address, birthdate, etc.) about myself or others online.
- I will consider whom I am communicating with and think about how they might interpret my words.
- I will give constructive criticism and comments to help people in ways that do not make them feel bad.
- I will use respectful and appropriate language without swearing, name calling or causing others to feel uncomfortable due to their gender, race, appearance, behavior or beliefs.
- I will not impersonate others or try to trick people into thinking what I wrote was done by someone else.

What happens when something goes wrong?

- When I do something that is not in line with this agreement, I will talk to a teacher or trusted adult who will help me figure out how to make it right.
- I will immediately stop and tell a trusted adult at school if anything happens on the computer or on the internet that does not seem right or that makes me feel uncomfortable.

I understand that using any school technology or network is a privilege I must earn through responsible use. But we all make mistakes.

When I do something with my device that is not in line with this agreement, I will let a trusted adult know and ask them to help me make it right. If I can't consistently keep up my part of this agreement, I understand that privileges may be removed for a time and that I may face additional consequences.

Student signature: _____

Parent signature: _____

Date: _____



Responsible Use Policy Template: Secondary School

Here is a model RUP you can adapt for use with secondary students.

RESPONSIBLE USE POLICY

Using your device is a privilege, and any privilege comes with responsibility. Here are the expectations for using your personal devices at school or anytime you are using school-provided devices.

Digital citizenship

I am responsible for practicing positive digital citizenship. I will treat people with dignity and respect when using technology and accessing the internet.

- I will be honest in all digital communications.
- I will be kind and avoid making threats or insulting, gossiping or teasing others with cruelty while I am online or using a computer.
- I will respect other students' work on the computer. I will not copy, change or remove another student's work from the computer, the school network or the internet.
- I will give credit to authors or sources when using information or ideas that are not my own. I know that failure to properly cite my sources of information is called plagiarism and is a form of cheating.
- I will only download music software, apps and other works from reputable sources that credit the original creators.
- I understand that things I post may be seen by everyone at school and at home, and that things that are posted on the internet can be seen by everyone in the world.
- I will not share personal information (either my own or another student's), including references to where I live, details about family or friends (including names), my age, birthday, home address or telephone number on the internet.
- I will consider whom I am communicating with and think about how they might interpret my words.
- I will give constructive criticism and comments in order to help people and not to make them feel bad.
- I will use respectful and appropriate language without swearing, name calling or causing others to feel uncomfortable due to their gender, race, appearance, behavior or beliefs.
- I will fact-check information before I share it digitally.
- I will not impersonate others or try to trick people into thinking what I wrote was done by someone else.
- I will not use online forums or technology resources to cheat on tests or assignments.

Personal responsibility and safety

I know that school computers and internet communication tools must be used properly and with respect.

- I will be aware of privacy settings on websites that I visit.
- If I find something that is not appropriate on the internet, I will leave it right away and notify the teacher or a trusted adult, especially if I reached the inappropriate material in the course of completing an assignment.
- I will report any misuse of the computer or the network to a teacher.
- I will take care of the computer and all technology equipment as if it belonged to me.
- I will respect the district network's security measures.

Learning and curiosity

I understand that school technology and networks are primarily provided to help support my learning and curiosity.

- I will use technology to support classroom activities or assignments.
- I will only download software from the internet if directed to as part of a lesson.
- I will only log into the computer or network with my own username and password.

What happens when something goes wrong?

- When I do something that is not in line with this agreement, I will talk to a teacher or trusted adult who will help me figure out how to make it right.
- I will immediately stop and tell the teacher if anything happens on the computer or on the internet that does not seem right or makes me feel uncomfortable.

I understand that using any school technology or network is a privilege I must earn through responsible use. But we all make mistakes.

When I do something with my device that is not in line with this agreement, I will let a trusted adult know and ask them to help me make it right. If I can't consistently keep up my part of this agreement, I understand that privileges may be removed for a time and that I may face additional consequences.

Student signature: _____

Parent signature: _____

Date: _____

Next Steps

An effective RUP sets the conditions for effective tech use, but it is just one part of a broader strategy for educating young people on effective behaviors for technology use online. Creating a truly healthy digital culture in a school goes beyond a policy and must also include practice.

In addition, teachers should keep the conversation about device use going, discussing topics like the fact that all online activities are not created equal; how to know when it's time to take a device break; how to use technology for social good; and what positive and responsible digital citizenship looks like. Teachers can also be amazing role models for using technology to make the world a better place!

School leaders, teachers, parents and students need additional supports and examples to help them model the behaviors of a healthy digital culture. The following are some resources that can help support the implementation of an effective RUP.

Supporting Teachers

Teachers should be able to explain and model the responsible digital behaviors they expect from their students. The ISTE U course [Digital Citizenship in Action](#) unpacks dozens of ways educators can demonstrate leadership in online environments so students see real-life examples of how to use technology in healthy ways.

Supporting Parents

Healthy digital habits are important at home, too, but parents can easily feel overwhelmed when charged with being the primary teacher of digital citizenship and digital literacy. The book [Digital for Good: Raising Kids to Thrive in an Online World](#) provides tips and resources parents can use to help create a healthy digital culture at home to align and support the expectations of tech use at school.

Acknowledgments

A sincere thank you goes to the following people for their insights and contributions to this guide:

Christina Lewellen, Executive Director, Association of Technology Leaders in Independent Schools (ATLIS)

Jill Brown, Ph.D., Director of Professional Learning, Consortium for School Networking (CoSN)

CoSN board members Holly Doe, Marlo Gaddis and Pete Just





iste.org

800.336.5191 (Toll free)

503.342.2848 (International)

2111 Wilson Boulevard, Suite 300

Arlington, VA 22201

USA