

# SETTING CONDITIONS FOR SUCCESS

## Guidelines for Responsible Use of Technology for Schools

# SETTING CONDITIONS FOR SUCCESS:

## Guidelines for Responsible Use of Technology for Schools



### Purpose and Intended Audience

This resource provides guidance for educators, technology leaders, district leaders, and district communities on supporting responsible technology use and digital citizenship. It is intended to complement—not replace—district policies governing the use of technology and digital resources.

### Connectivity Is a Critical Foundation

Providing digital access to all learners is a critical foundation for their success in learning and life. This includes access not only to devices and broadband, but also to emerging technologies such as artificial intelligence (AI) tools that are increasingly embedded in learning platforms and productivity applications. 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 solve problems, balancing screen use with offline activities, as well as 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 and establishing appropriate behavior expectations for students. Responsible adoption of emerging technologies ensures students develop the digital and AI fluency, and the online safety skills needed for future academic and workforce success.

## Setting Technical Conditions for Success

This guide focuses on creating responsible digital norms for students. Schools should also be aware of technical and legal protections designed to help safeguard students online. In the U.S., the Children’s Internet Protection Act (CIPA) requires schools receiving federal E-rate funding for internet access to implement specific technical protections before allowing access to their networks. Additional federal laws, including FERPA and COPPA, along with a growing number of state student data privacy laws, also help support the safe and responsible use of educational technology in schools.

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 email, chat rooms and other forms of electronic communications.
- Unauthorized access, including 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.

## Responsible Use Agreements

The **Protecting Children in the 21st Century Act**, enacted following **CIPA** in 2001, requires schools to educate students about appropriate online behavior – including safe online interactions and responding to cyberbullying. Historically, schools have addressed these responsibilities through **Acceptable Use Policies (AUPs)** (*or other titles aligned with district terminology*), which are established by district or school leadership to promote healthy norms for responsible technology use. In many cases, AUPs are Board-approved policy documents, and students and/or their parents or guardians are asked to sign them to acknowledge their understanding of how to responsibly use school-provided accounts and devices. While AUPs serve an important purpose, they are often written in formal or legal language that can be difficult for students and families to understand and act on. This publication encourages school systems to adopt

**Responsible Use Agreements (RUAs)** – a more student- and family-friendly approach that prioritizes clarity, accessibility, and the development of a healthy digital culture both at school and at home. Where it is not possible to revise an existing Board-approved policy, schools are encouraged to create a companion RUA that translates that policy into practical, readable guidance. Unlike AUPs, RUAs are typically presented as guidance rather than formal Board policy – making them easier to update, personalize, and communicate to the communities they serve.

RUAs, when provided to students and families at the beginning of the school year, help establish the optimal conditions for effective digital activities. They can also be connected to classroom activities to teach about appropriate online behaviors, how to recognize misinformation or manipulated media (deepfakes), and the expectation to use technology to support curiosity and learning. By establishing expectations for meaningful and appropriate online behaviors, we not only allow students to be their best selves online, we prepare them to positively influence others. Addressing AI use when establishing norms further supports both ethical learning and student readiness for future academic and workforce success.

*Responsible Use Agreements may also be referred to, including but not limited to, Acceptable Use Policies (AUP), Technology Use Policies, or Technology Use Agreements, depending on district terminology.*

## **RUAs Gone Wrong**

Unfortunately, many RUAs have been developed in a way that does not help create effective conditions or help students prepare to be responsible members of a digital world. There are two common pitfalls that can be seen in ineffective RUAs: 1) using language that's too complicated or confusing for a student to understand, and 2) 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 RUAs, let's take a look at some examples of RUAs that are not effective. In this section, we'll share excerpts from actual RUAs that have missed the mark and explain why.

## Overly Negative

The example below shows the first portion of an RUA that lists 35 things not to do with technology, but doesn't include a single example of *what* to do with the technology. An effective RUA balances behaviors that are not permitted with competencies that should be practiced by students. After all, you can't practice not doing something, and being an effective digital citizen takes practice!

---

Users shall not use the network or technology, including access to the internet, intranet, collaboration 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:

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 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 network or technology;
  13. Obtains school technology or network access beyond those authorized;
  14. Engages in unauthorized or unlawful entry into a 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 personnel in a manner that violates state law, federal law, regulations, policy or guideline;
  18. any other school policy;
- 

### **Unnecessarily Complicated Language**

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

---

"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."

---

## Liability Prioritized Over Learning

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

---

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

## Creating Effective Responsible Use Agreements

Let’s now look at how to create an effective RUA. An RUA should guide students in being successful, effective digital citizens, and it should be written to meet students’ varying levels of understanding. For example, you may want to consider having separate RUAs for elementary students and secondary students. Keep these three tenets front and center when creating or updating a Responsible Use Agreement:

- **Keep it positive.** RUAs should not be a long list of don’t’s. Instead, make them mostly about the do’s of technology use.
- **Write in plain English.** This isn’t a real estate contract or a piece of legislation. Keep the language conversational, human-friendly, and accessible to students.
- **Engage the whole school community.** Involve students, families and caregivers—such as through PTA/PTO groups— to have input, make suggestions and ask questions, in reviewing and shaping the expectations so the entire school community understands and supports responsible technology use.

Finally, as we've all experienced, technology changes rapidly! Review your RUA annually to be sure any mention of outdated technology is removed, and your vision for how to use technology to support learning remains updated.

## What to Include

Remember, RUAs are learning tools. Everything that's included in the agreement should guide students in becoming confident, effective digital citizens. Classroom activities should help inform and deepen the understanding of the elements in your RUA.

The following elements should be included in an effective RUA:

### Purpose

Start with a clear purpose that helps students and parents understand why the agreement is so important. Such a statement might include a reminder that using school-provided technology is a privilege and technology is expected to be used to enhance curiosity and creativity in support of learning.

### Desired Digital Behaviors

The bulk of an effective RUA should focus on identifying desired digital citizenship skills. Remember, desired skills should be framed as "do's" instead of "don'ts" whenever possible. It might help to frame the agreement 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.

### **Authenticity and Digital Integrity**

Students should understand that technology can create or alter digital media in ways that appear realistic. Responsible use means creating and sharing content honestly, avoiding impersonation or manipulation of others, and reporting media that may mislead or harm individuals or communities.

Remember to focus on behaviors and responsible practices rather than naming specific technologies or websites (e.g., TikTok or Discord), since platforms change frequently and can quickly date the agreement. This helps keep expectations aligned with broader competencies—such as those outlined in profiles like an “AI-Ready Graduate”—that emphasize responsible, ethical, and thoughtful use of digital tools, and reflects the district’s mission, values, and existing guidance documents.

### **Resolving Problems**

One of the most important—yet often overlooked—parts of a strong RUA is guidance on what students should do when something goes wrong. Students will inevitably make mistakes or encounter challenging situations online. The agreement should clearly explain who students can go to for help and how to resolve concerns.

It is important that expectations encourage students to seek help from a trusted adult when problems arise. If consequences are written in a way that feel overly punitive, students may hesitate to report issues or ask for help.

Consequences for misuse should be clear, fair, and developmentally appropriate, with an emphasis on learning, accountability, and improving future behavior rather than punishment alone.

### **Partnering with Families**

Districts may also consider including a parent or caregiver acknowledgement that encourages families to support responsible technology use at home.

Create a place for students to physically or digitally sign that they agree to the code of conduct outlined in the agreement. You may also consider adding a parent/guardian signature. If there is a problem with digital behavior down the road, it may be helpful to show students their signed RUA and remind them of the behaviors they agreed to.

### **Responsible Use Agreement Template: Elementary School**

The following is a model RUA you can adapt for use with younger students. (Grades PreK-5; Typical ages: 4-11) You can adjust the language and elements of the template below to fit your unique school culture and goals. It is also recommended to use visuals with younger students.

---

## RESPONSIBLE USE AGREEMENT

At our school we use technology to make learning more engaging and help students be more curious and creative learners. It is essential that we develop good technology habits so they will be successful in their future learning and life. Using technology is a privilege, and any privilege comes with responsibility. Here are the expectations for using technology at our school.

### **How should I use educational technology?**

- I will use my device when a teacher asks me during class, 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 installing/using any new apps.
- I will take care of any school devices as if they were my own.

*Optional Primary Language: I will follow my teacher's guidance when using technology at school.*

### **What should I do with technology?**

- I will use my device to learn new things.
- I will check information to verify that it is true.
- I will give credit to the creators of content that is not mine.

I will remember that things I see online, like pictures or videos, might not always be real, and I will ask a teacher or trusted adult if I'm unsure if a picture or video I see online is true.

*Optional Primary Language: I will use school technology to learn and grow.*

### **How should I be a good citizen online and offline?**

- I will be a good cyber-friend, including being honest and kind online.
- I will let a teacher or parent know before contacting someone online I don't already know.
- I will not share personal information (like home address or birthdate) about myself or others online.
- I will give feedback and comments in ways that make others feel supported.

- I will use appropriate language and won't make others feel uncomfortable because of the things I say.
- I will always get permission from a trusted adult before sharing any pictures.
- I will not create, change or share pictures, videos, or messages that could embarrass or trick someone.
- I will practice digital wellness by being kind and thoughtful when using technology with myself and others.

**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 if anything happens on the computer or online that does not seem right or makes me feel uncomfortable.
- I will take responsibility for my actions, try to fix any hurt or problems I may have caused and use the experience as an opportunity to learn and grow.

*Optional Primary Language: I will tell my teacher when there is a problem with my classroom technology.*

I understand that using any school technology is a privilege I must earn. If I don't keep 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 Agreement Template: Secondary School

The following is a model RUA you can adapt for use with secondary students. (Grades 6-12; Typical ages: 11-18) You can adjust the language and elements of the template below to fit your unique school culture and goals.

---

### RESPONSIBLE USE AGREEMENT

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 modeling positive digital citizenship. I will treat people with dignity and kindness when using technology and online.

- I will be honest and ethical 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 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 understand that things I post may be seen by others at school and at home, and that things that are posted on the internet can be seen by anyone in the world.
- I will not share personal information (either my own or another student's), such as 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 provide comments in ways that help others feel supported.
- 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 something I wrote was done by someone else.
- I will always get explicit consent from others before using their image with any technology tools.
- I will not create, alter, or share images, video, audio, or messages that falsely represent another person or could harm someone's reputation. (i.e. deepfake)

### **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 learn new things.
- I will use technology to complete school activities or assignments.
- I will use my device to check information to verify that it is accurate.
- I will give credit to the creators of any content I use that is not my own.

### **Personal responsibility and safety**

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

- If I find content that is not appropriate on the internet, I will notify a teacher or a trusted adult, especially if I reached the inappropriate material in the course of completing an assignment.
- I will take care of the computer and all technology equipment from the school as if it belonged to me.
- I will respect the district network's security measures and only download apps or content I have permission to access.
- I will only log in to the computer or network with my own username and password.
- If I see digital content that appears manipulated or is meant to embarrass, deceive, or harm someone, I will report it to a trusted adult.

I understand that using any school technology, networks or personal devices at school 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 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 RUA 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 an agreement 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 equally; 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 support 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 RUA.

### Supporting Teachers

Teachers should be able to explain and model the responsible digital behaviors they expect from their students. The ISTE+ASCD 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, Guardians or Family Members

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.

For districts interested in deeper family engagement around technology use, screen time, and digital well-being, additional guidance is available in the **[ETLA Parent Technology & Screen Time Training resource](#)**, which provides a flexible model for partnering with families through conversations, student voice, and district transparency.

### **Supporting Resources:**

[Responsible Use Agreement Glossary of Key Terms](#)

[Example Agreements](#)

### **Acknowledgments**

A sincere thank you goes to the following people for their insights:

Richard Culatta, CEO, ISTE+ASCD

Keith Krueger, CEO, CoSN

Carmalita N Seitz, Ed.D., Managing Director, Online Learning & Digital Innovation, ISTE+ASCD

Layla Kwon, Head of Partner Relations, ISTE+ASCD

Marlo Gaddis, CEO Gaddis Education Consulting

Pete Just, formerly Metropolitan School District of Wayne Township, CoSN AI Project Director

Carla Wade, MS, Senior Director of External Relations, CoSN

Jill Brown Ph.D., Director of Professional Learning, CoSN

Stacy Hawthorne Ed.D., CETL, Board Chair/Executive Director, CoSN/EdTech Leaders Alliance (ETLA)

Ashley Cross, Ed.D., CAE, Senior Director of Education and Content, ATLIS

Peter Frank, CAE, Interim CEO, ATLIS

Cooper Sved, Elementary Teacher/ Policy Analyst, 2025 CoSN Blaschke Fellow

Dwight R. Levins Jr., Chief Technology and Information Officer, Oakland Schools

Dr. Emily Dillard, Chief Information Officer, Alexandria City Public Schools

Holly Doe, District Instructional Coach, MSAD 11

Sophia Mendoza, LA Unified School District

David Paszkiewicz, La Cañada Unified School District

**CC BY-NC**

Permission is granted under a Creative Commons Attribution + Non-commercial License to replicate, copy, distribute, and transmit this report for non-commercial purposes with attribution given to supporting organizations.

