

Closing the Homework Gap While Protecting Student Privacy

A Quick Guide to Building Students' and Families' Literacy to Stay Safe Online

As schools work to [close the homework gap](#), it is important to give students and families the tools they need to keep safe in the digital space. To improve students' and families' literacy to stay safe online, school administrators should focus on two important steps:

- Engage students and families on school policies and digital literacy needs
- Provide training and support tailored to the community's needs



Engage Students and Families on School Policies and Digital Literacy Needs

[Community engagement](#) refers to the involvement of stakeholders outside a school in decision-making processes that impact their lives. It is especially important to engage the people who are impacted by school policies regarding devices and broadband — which means students and their families. This engagement should include efforts to increase digital literacy and to create and enact school policies on the uses of devices and broadband.

Engage Community Members in Creating and Enacting Policies

Engaging communities when setting policies helps ensure any concerns about those policies are raised and addressed before they are put into place, especially regarding devices and broadband connections issued by schools in their efforts to close the homework gap. For example, although schools have long maintained [“acceptable use” or “internet safety” policies](#) governing their devices and networks, these policies often have not kept pace with the use of school-issued devices in students' homes. Emerging issues that need to be addressed, and would benefit from community input, are family members' use of school-issued devices, schools' use of [student activity monitoring software](#), and how policies intended to protect students and families — such as restricting the software installed on school-issued devices — might hamper them. In these engagement efforts, it is important to connect with underrepresented communities and provide sufficient information for communities to provide input.

Engage Community Members in Assessing Digital Literacy Needs

In addition to community engagement around policies, schools can ensure their efforts to increase digital literacy meet community members' most pressing needs regarding the homework gap, devices, and broadband access. Communities have existing knowledge and insight from which schools can learn and make better decisions as they develop digital literacy programs. Therefore, the development of digital literacy programs should not be a one-way dissemination of information but rather a dialogue that allows for deeper understanding of the community's needs for training on digital literacy, privacy, and security. In engaging the community, schools should consider utilizing

centers of community life to make it more accessible for communities to have voice and agency and partnering with local organizations that have credibility and trust within the community.

Clearly and Proactively Communicate Policies, Including Regarding Data Destruction

Any new technology program should make clear what the appropriate uses of devices and connections are and share that information with students and families in easily understood ways. This information is most impactful when it is grounded in why it matters, and the related guidance and expectations are explained in easy-to-understand language to students and families. An issue of particular concern is data destruction, particularly when devices are returned to schools. Students and families should understand what happens to their information when the school resumes possession of a device.



Provide Training and Support Tailored to the Community's Needs

In addition to engaging students and families, it is important to give students and families the tools they need to keep themselves safe in the digital space. As part of schools' efforts to enable safe and secure environments, they should explicitly focus on the following steps.

Provide Training and Resources

Connecting students and families to online resources may expose them to harm due to unsafe privacy and security practices. Consequently, students and families should be provided with training about safely using devices to interact with services online, especially when those systems may be unfamiliar. As described above, schools should engage community members to understand their training needs, which ensures that the training will meet community needs, build trust, and encourage its use. Training also should include security practices like [secure passwords](#), [phishing](#), [updating software](#), and the basic functionality of devices and their software. Training and resources will be more widely used if they are available in a number of different formats, including in-person and recorded online options, and are short, free of jargon, and available in multiple languages.

Provide Technical Support

Offering technical support to students and families is a key way to strengthen security and protect student privacy. As with training, technical support should be available in multiple formats and be available in multiple languages. CDT's two-page guide, "[A Quick Guide to Maintaining and Protecting School-Issued Devices](#)" includes more details on how to provide efficient, seamless technical support without compromising students' and families' security and privacy.

This two-pager is one of a series designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. Find out more at cdt.org/student-privacy.