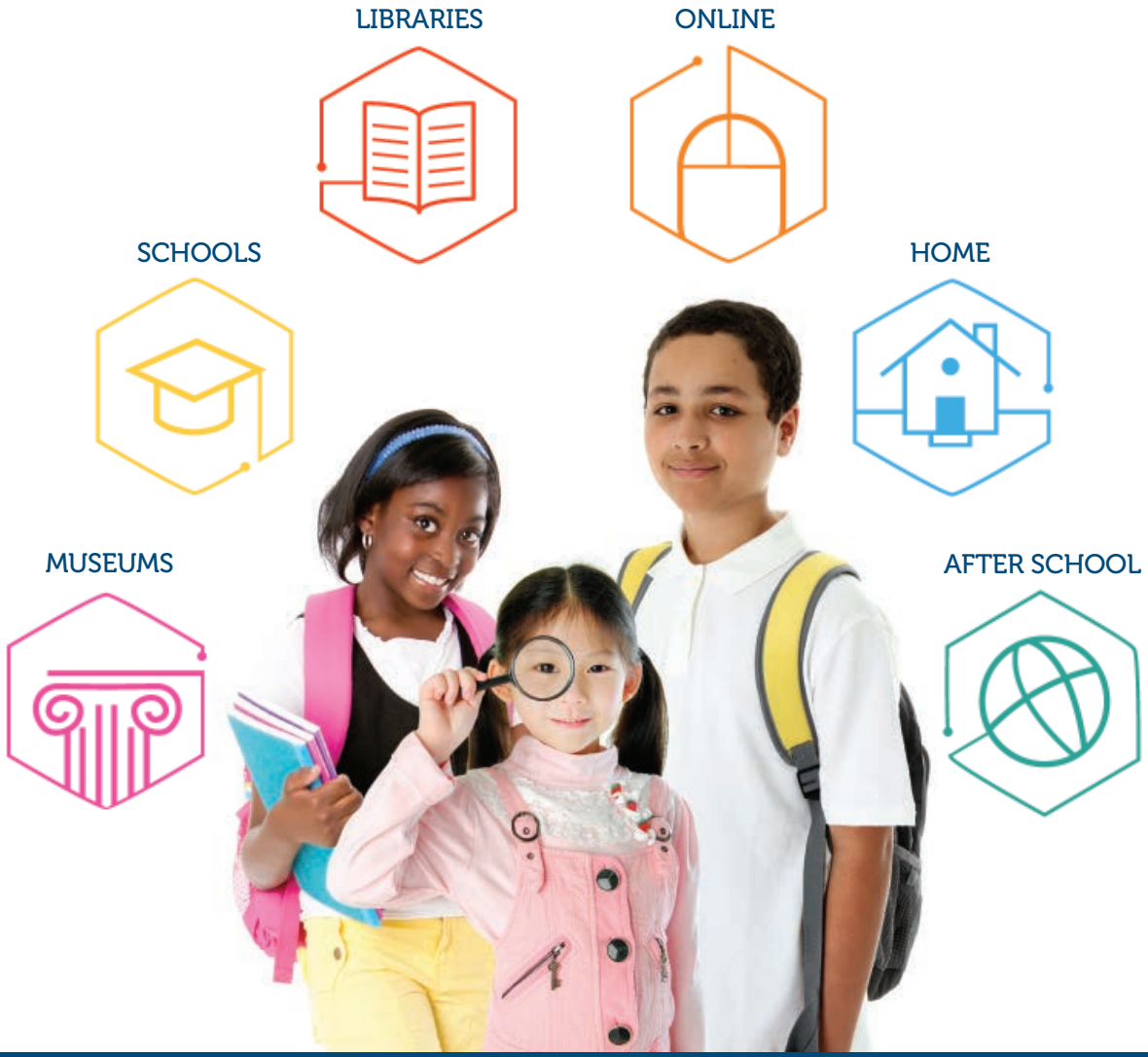
THE ASPEN INSTITUTE GUIDE FOR

CREATING TRUSTED LEARNING ENVIRONMENTS

Based on the report *Learner at the Center of a Networked World*



THE ASPEN INSTITUTE
Communications and Society Program

The Aspen Institute invites you to review the digital version of this report at **www.aspentaskforce.org**

Please note that this guide is a synthesis of various viewpoints and does not necessarily reflect the opinion of each participant or organization.

The Aspen Institute
One Dupont Circle, NW
Suite 700
Washington, DC 20036

Published in the United States of America in 2017 by The Aspen Institute
All rights reserved
Printed in the United States of America
ISBN: 0-89843-657-5
Pub 3: 17/004

Individuals are encouraged to cite this report and its contents. In doing so, please include the following attribution: The Aspen Institute Guide For Creating Trusted Learning Environments. The Aspen Institute Communications and Society Program, Washington, D.C.: The Aspen Institute, January 2017.

A project of the Aspen Institute Communications and Society Program and the John D. and Catherine T. MacArthur Foundation.

THE ASPEN INSTITUTE

MacArthur Foundation

CONTENTS

Introduction

The Aspen Institute, with support and guidance from the John D. and Catherine T. MacArthur Foundation, created a Task Force on Learning and the Internet. The Task Force of 20 innovative and respected minds in technology, public policy, education, business, privacy and safety sought to understand the ways in which young people learn today. As part of the discussions, participants explored how to optimize learning and innovation within a trusted environment. The Task Force highlighted both the new opportunities offered by this emergent learning environment and the issues that may arise such as trust, safety, privacy, literacy and equity of access. The following guide serves as a framework for dialogue and action among a learning community's many constituencies. The guide contains worksheets used for the following stakeholders:

Learners

Parents or Caregivers

In-school or Out-of-school Providers,

Developers

Task Force action items are marked A to Z in the publication, Learner at the Center of a Networked World at ***www.aspentaskforce.org****. This Guide is inspired by Action U.*

ACTION U:

Foster collaborative efforts at all levels to establish principles of a Trusted Environment for Learning.

The goal of such a trust framework is to protect young people while empowering them to explore, express themselves, pursue their interests and succeed in their education. The Task Force recognizes a trusted environment is not easy to define precisely and will not be simple to construct. It will require innovative approaches to policy and regulation, new technological solutions and the development of programs that educate teachers, parents and students about the risks and rewards of being online. It will constantly evolve as new technologies introduce new tensions and offer new solutions.

What's In it for You?

Everyone has an important role in creating and understanding trusted learning environments. This guidebook is a resource for you.

Learners

Learn about the principles and best practices for trusted learning environments so that you can get engaged and use your own voice and experiences to ensure your safety and security. (See page 18)

Parents and Caregivers

Gain access to information about best practices for creating trusted learning environments and learn about key questions to ask to determine if your child is part of a Trusted Learning Environment when participating in learning networks and online programs. (See page 19)

In-School and Out-of-School Providers

Help create trusted learning environments by leading community conversations, utilizing best practices and asking the right questions. (See page 20)

Developers

Learn from others in the field, get a better understanding of key principles and best practices so you can be part of the solution in creating trusted learning environments. (See page 22)

The best approach to establishing trusted environments is to have all stakeholders—including learning professionals, civic officials, local associations, parents, teachers, students and businesses—collaborate in setting local standards. This could also be done at state and national levels.

A NEW VISION FOR LEARNING

Learning today is no longer limited to the physical walls of a schoolroom.

Learning is active, engaged and personalized. It is made possible by a web of environments, or learning networks, that revolve around the learner. The learning networks are at once expansive—including libraries, museums, schools, afterschool programs, homes and more—but also highly individualized. In fact, much of the networks' power comes from their ability to customize the learning experience to individual users or small groups. Learners are able to choose the pathways that are most appropriate for their needs and learning styles.[1]

While learning in these networks occurs both on and off-line, it is clear that technology is an important catalyst. Technology supports innovation, broadens opportunities and gives learners more agency to connect their interests with educational experiences.[2]

This new vision contemplates connected learning systems that can be included such as: competency-based learning, micro-credentials or digital badges, personalized learning and adaptive learning.

Competency-based education. As noted in the Aspen Task Force report, competency-based education models often include five principles:

- **Students advance upon mastery;**
- **Competencies include explicit, measurable, transferable learning objectives that empower students;**
- **Assessment is meaningful and a positive learning experience for students;**
- **Students receive timely, differentiated support based on their individual learning needs;**
- **Learning outcomes emphasize competencies that include application and creation of knowledge, along with the development of important skills and dispositions.**

Micro-credentials. Also called digital badges, micro-credentials are an online representation of "skills, interest, and achievements earned by an individual through specific projects, programs, courses, or other activities."[3]

Personalized learning. Also called student-centered learning, personalized learning facilitates the academic success of each individual student by customizing learning experiences depending on his or her needs, interests and strengths.[4]

Adaptive learning. Adaptive learning is an education technology that changes the content, sequence or assessment that a student encounters in real-time, in response to the needs of the individual.[5]

THE NEED FOR **TRUST**

For technology to become a vehicle to support the learner and advance learning initiatives, learners need a trusted environment.

With trust, we can create incredible learning systems and opportunities that can catapult the learner forward. Trust, in this sense, ensures for a learner a safe experience online while securely protecting sensitive information. Realizing this will necessitate a commitment to establishing trust with teachers, parents, caregivers, children and communities. A trusted environment exists when the network of stakeholders around the learner trust each other and work to keep that trust in tact with transparency, communication and confidence in using technology to engage in learning.[6] It involves policies, tools and practices that effectively address the privacy, safety and security concerns related to learning online.[7] It involves parents being able to trust that their children's personally identifiable information is safe, secure and will not be used in ways other than to help their academic progress.

A trusted environment exists when the network of stakeholders around the learner trust each other and work to keep that trust in tact with transparency, communication and confidence in using technology to engage in learning.

Without trust, the ultimate success of networked learning could be in jeopardy. Unfortunately, much of the public discourse about children online emphasizes the dangers of the Internet and does not give enough attention to the positive potential of the technology as a tool for learning. Rather than relying on purely defensive measures for protection (like filtering and monitoring and other forms of restriction), parents, caregivers, educators, and other community stakeholders need to work together to create "trusted environments" that allow young people to pursue their interests safely.

What do parents worry about when it comes to student privacy and safety?

- Keeping student information safe from "hackers and would-be predators"
- Unnecessarily sharing information with "people or companies outside the education system," including for advertising purposes
- Tracking students and other "unintended consequences" of using data for educational decision-making
- The unknown

PRINCIPLES

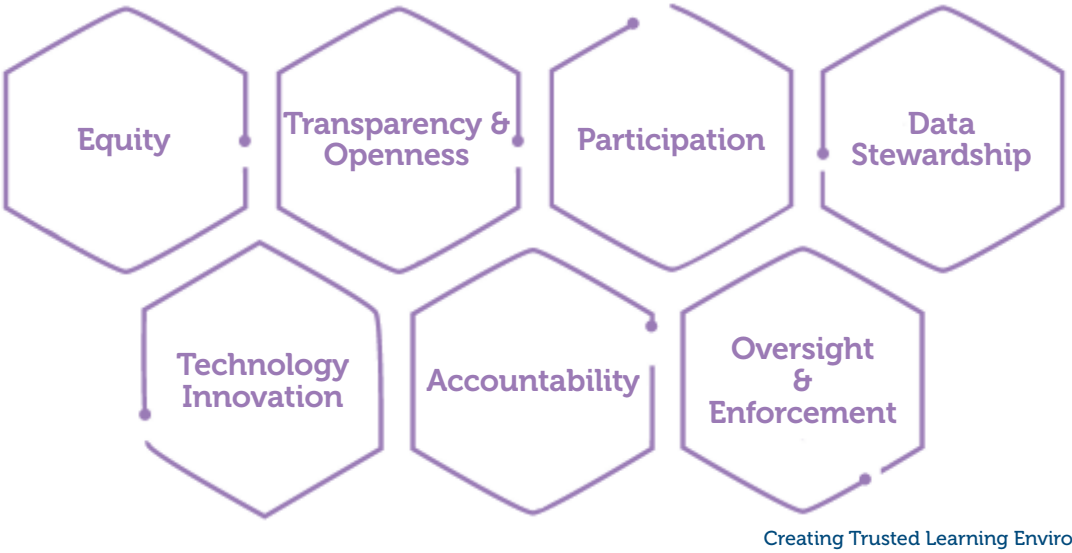
FOR TRUSTED LEARNING ENVIRONMENTS

Many districts, schools, communities and non-profits recognize their responsibilities to both learners and learning and are taking impressive steps to create trusted learning environments (see Best Practices in ACTION).

These stakeholders have taken action to keep the learner's data secure and to help the learner navigate safely online and across multiple platforms while emphasizing innovation and advancing learning.[8] They are focusing on communication and transparency, educating employees, learners, parents, caregivers and communities on the importance of learning online and how to be safe. They are also establishing practices for purchasing technology, products, and programs as well as implementing their own standards for trusted learning environments.[9] These efforts provide valuable guidance to others who seek to create trusted learning environments. For those stakeholders who invest the time and effort, the rewards could be tremendous.

In its report, the Aspen Task Force recognizes that the composition of a trusted learning environment may vary based on different contexts, platforms and stakeholders. It is a constantly evolving concept as new technologies introduce new tensions and offer new solutions. To help the process along, the Task Force identified a set of high-level principles intended to guide the process for developing a trusted learning environment. The key characteristics of a trusted environment: transparency and openness; participation; data stewardship; technology innovation; accountability; and oversight & enforcement.

The principles of a trusted environment: transparency and openness; participation; data stewardship; technology innovation; accountability; and oversight & enforcement.



The following principles demonstrate key characteristics to consider when developing a trusted learning environment:

Transparency and Openness:

Require easy-to-read disclosures to enable learners and other stakeholders to clearly understand who is participating, what the norms and protections are, what data is collected and how it is used.

Often, adoption and acceptance of new digital practices remains slow because of a lack of information regarding the use of data. This lack of information reduces trust in the platform, environment or media landscape. For example, the failure of the non-profit InBloom,[10] who centralized student information online to help educators personalize lesson plans and track student progress, failed to communicate with its stakeholders the trustworthiness of its information gathering.

The Aspen Task Force report states that stakeholders should have access to easy-to-read disclosures to enable learners and other stakeholders to understand clearly who has access to personal data, what the norms and protections are, what data is collected and how it is used. This is codified by the Federal government in its adaptation of the Fair Information Practice Principles (FIPPs) within the Privacy Act of 1974. As a key principle, organizations should be "transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII)."

Here are some examples of a variety of organizations that have taken steps to address transparency and openness:

Khan Academy—https://www.khanacademy.org/educator/parents-and-tutors/student-privacy-for-parent/a/khan-academy-privacy-principles

Schoolzilla—https://schoolzilla.com/why-schoolzilla/data-security/

The Wisconsin Department of Public Instruction (DPI)'s WISE data system—http://dpi.wi.gov/sites/default/files/imce/wisedash/pdf/StudentDataOverviewFAQs.pdf

Participation:

Provide opportunities for individual and interest-group participation in the decision-making and policy making of the development and deployment of connected learning solutions.

Another way to build trust with learners and key stakeholders is to involve and engage all end-users throughout the different stages of a project or product development. For example, the VIF International Education's Global Pathways project provides professional development to teachers across the globe in an inquiry-based model. VIF enables teachers to provide each other with peer feedback. In particular, VIF Global Pathways works on-the-ground with international teachers to help them acclimate to the variety of different teaching environments they encounter. VIF staff said that while initially the organization sought simply to update their online teacher peer review system, they quickly realized they needed instead to change the whole platform. Based on user feedback, teachers wanted more choices in how they interacted with the platform. They also said the best professional development they received was not just from expert assistance, but from other teachers. Having identified peer feedback as the driving need for users, VIF returned to the drawing board and is building a peer feedback tool that can be used across the platform, regardless of content.

Equity:

Provide access for all to digital media and the internet while keeping privacy and security in mind, supporting the teaching of digital, media and social-emotional literacies, and working to ensure access to high quality content. That is, be mindful not to exacerbate the tech divide.

As noted in the Aspen Task Force report, in order for students to pursue their interests online, they need to have access to the resources required for learning.[11] It is through broadband that students can access resources around the globe, or an instructor on the other side of the country, or expand their learning to times and places beyond the classroom. Broadband is also a vital mechanism for accelerating innovation and for fostering faster, more affordable distribution of services, content and tools for teachers and students.

However, connectivity should never be a trade-off for privacy and security. Though not federally mandated, or required by all states, stakeholders should ensure that learners', parents', caregivers' and communities' data is secure and will not be used for targeted advertising. In October 2016, the Federal Communications Commission proposed and adopted privacy regulations for broadband Internet Service Providers (ISPs). The FCC's privacy policies regulates how and when broadband providers can collect and use data for targeted advertising (known by regulators as "contextually relevant advertising" or "behaviorally targeted advertising").

In instances where learners currently lack access, it is important for schools and communities to think about how to embed principles and best practices for trusted learning environments. This includes digital literacy for learners and parents. The Aspen Task Force report calls on states and districts "to adopt policies to ensure that digital, media and social-emotional literacies are taught as basic skills, not as an 'extra' or an 'afterthought.' These literacies should be embedded into all appropriate core subjects rather than be taught as a separate course." These literacies ensure that learners can safely navigate digital media and the Internet.

In addition, all learners should have access to high quality content. While digital literacies help learners identify and understand high-quality content, it is often difficult to locate and utilize that content online. The Task Force report noted several emerging products to help learners in this area. These are included below along with a number of new offerings which have been launched since the report's release:

- **Graphite**, a website for preK–12 teachers developed by the nonprofit Common Sense Media to help preK–12 educators by providing ratings and reviews of apps, games, websites and digital curricula contributed by other teachers.
- **The Federal Registry for Educational Excellence (FREE)**, a site created by the U.S. Department of Education that includes a directory of over 400,000 learning resources organized by subject and by standard.
- **Gooru,** a search engine specifically designed to help teachers to find high quality interactive learning materials.
- **Amazon Inspire**, an online marketplace launched in August 2016, offers free lesson plans, worksheets and other open educational resource materials for teachers.
- **Summit Personalized Learning**, a Facebook-backed platform launched in August 2016, offers a free student-directed learning system developed jointly by Facebook and Summit Public Schools. The platform comes with curriculum developed and maintained by teachers and gives students the ability to set and track learning goals and work on content at their own pace.

Data Stewardship:

Find ways to protect data to include mechanisms to reduce the risk of harm. This may include: clearly delimiting the permissible uses of data, de-identifying sensitive data and/or deleting data once it no longer has value for learning. Data can also provide feedback about what works, thereby shortening the cycle to improve the ecosystem of learning networks, and improve learning itself.

Technology Innovation:

Create and deploy technologies that support a trusted environment, such as the use of metadata to convey and enforce data policy or privacy dashboards that indicate what information is shared with whom.

Accountability:

Adopt policies and procedures or a code of conduct that support responsible learning environments.

Oversight and Enforcement:

Establish governance structures to protect the integrity of learning networks with competent and appropriately resourced bodies in place to enforce these principles.

CREATING A TRUSTED ENVIRONMENT

BEST PRACTICES

The Aspen Institute created this guidebook to build on these principles and to provide best practices for stakeholders to use when creating trusted learning environments, engaging with them, and embedding them in communities.

Best practices for creating a trusted learning environment:

1. **Clearly define and communicate "trusted environment" and what "trust" means to your learner and his or her community.**
2. **Value the youth perspective and help them exercise their own voice.**
3. **Engage experts across disciplines to address need.**
4. **Be proactive and be ready to react when necessary.**
5. **Understand that language matters.**
6. **Pull from best practices and utilize lessons learned from previous organizations.**
7. **Define clear roles among the learning network.**

In addition, stakeholders need to communicate effectively in early discussions the iterative nature of creating a trusted learning environment. The development cycle of products, programs and platforms are rarely perfect from the beginning and require constant feedback for improvement. However, stakeholders should always have the information on what failings may have occurred and how their privacy and security was maintained and/or breached. While the number one goal is to avoid problems, the reality is that they can and do happen. Stakeholders need to know that all issues will be handled effectively and efficiently.

More information on these best practices, and how they are seen in action, appears later in this guide.

What's in it for you?

The following four activities highlight why you should care about trust if you are a learner, parent/caregiver, in-school or out-of-school provider, or a developer. The worksheets can be used:

- **For understanding what trust means to YOU**
- **As a guide for evaluating the current level of trust in your learning environment**
- **To uncover specific actions you might take to develop a trusted learning environment.**

We encourage you to work through these Activity sheets on your own, or with a group, and secure a trusted learning environment for you and your community. The guide is a form-enabled PDF. This means that you can enter your responses directly into the PDF document. Please remember to save your responses each time you use the fill.

In Conclusion

Learning and learning environments are evolving. The classroom is moving beyond a physical space to include learning networks enabled by technologies that aim to broaden opportunities and empower learners to personalize for their needs and learning style. These emergent trusted environments should advance learning initiatives and foster innovation without sacrificing the safety of the learner. To achieve this, a network of stakeholders at all levels (e.g. learners, parents, businesses, teachers and nonprofits) must work in collaboration to address potential issues of trust, safety, privacy, literacy and equity of access. It will involve creating policies, developing tools and fostering practices that align with the community's definition of trust.

The remainder of this guide features four worksheets aimed at learners, parents/caregivers, in-school and out-of-school providers, or developers interested in supporting a trusted environment. The worksheets are best used to explore what trust means to you, evaluate the current level of trust in your learning environment, and uncover specific next steps.

Lastly, the guide includes Best Practices in ACTION for additional reference. The challenges of creating a trusted environment can be addressed through a commitment by stakeholders to engage with a learner's community early and often. The goal of the remaining sections is to provide guidance for further discussions and to help identify priorities for each stakeholder.

ACTIVITIES

LEARNERS

PARENTS OR CAREGIVERS

IN-SCHOOL OR OUT-OF SCHOOL PROVIDERS

DEVELOPERS

ACTIVITY:

Questions for **LEARNERS**

Why You Should Care About Trust

Learning today is no longer limited to the physical walls of a schoolroom. Learning is active, engaged and personalized. You can create your own learning pathways and networks utilizing libraries, museums, schools, afterschool programs, homes and more.

As a learner, taking advantage of new learning opportunities is exciting and fun, especially when you can focus on your interests and passions. As you explore your learning opportunities you will want to know that you are safe and your privacy is protected. You should understand what you can do to navigate your learning network safely, and what to do if you have any questions or concerns about your learning network.

Conversations with your caregivers, instructors or a trusted adult can be a great way to understand what is being done to protect your safety and privacy, and to let them know what you think can be done to make things even better for you and your fellow learners.

The guide is a form-enabled PDF. This means that you can enter your responses directly into the PDF document. Please remember to save your responses each time you use the fill.

Questions You Can Think About Or Discuss

What does trust mean to you and your family?

What information about yourself would you feel comfortable sharing online?

What are some examples of information about yourself not safe to share online?

What information do the organizations in your learning network collect? Why?

Would you share a password with someone who is not a family member?

Who will you ask if you have any questions about your digital learning activity?

ACTIVITY:

Questions for **PARENTS or CAREGIVERS**

Why You Should Care About Trust

Learning today is no longer limited to the physical walls of a schoolroom. There are many opportunities for your child to participate in learning networks personalized to best meet her or his needs and learning styles.

As a parent or caregiver, you want your child to be able to take advantage of new opportunities to learn and engage with the best resources available. You also want to ensure that your child is safe and that his or her privacy is protected while he or she participates in these programs and activities. You might also wonder if you can trust the institutions or learning networks providing your child's digital learning experience.

Community meetings, one-to-one conversations with community leaders, or in-school and out-of-school providers can be a crucial way to understand what is currently being done to establish and foster trust in your child's learning network.

Questions You Can Think About Or Discuss

Whether you initiate a meeting or attend one, it is important to be ready with good information and questions. Here are some key questions that might help you better understand whether your child is part of a Trusted Learning Environment:

What does trust mean in my child's learning community?

What information is collected about my child?

How is my child's data protected?

How long is the data information stored? Where? Why?

How can I stay informed of changes in my child's learning network?

How can I be involved in decisions related to my child's participation?

Who should I speak with if I have any feedback or concerns about my child's participation?

ACTIVITY:

Questions for
IN-SCHOOL or OUT-OF SCHOOL PROVIDERS

Why You Should Care About Trust

Today, many districts, schools and afterschool programs are embracing innovation through technology to create and connect with learning networks that support learners and advance learning. There are a growing number of quality digital resources you can utilize to provide personalized learning experiences which best meet your learners' needs and learning styles.[12]

As an in-school or out-of-school provider, you might wonder how to take advantage of emerging learning networks. For example, you could tailor instruction based on your learners' performance data from their digital learning activities, and/or thoughtfully share and evaluate this data across partners in the network to best serve the learner. Sharing data requires trust with your learners, their caregivers, your team and the learning network. You will want to know that you can trust a learning network you are working with to protect your learners' data so that data is used only to improve learning, and not for any other purpose.

Community meetings or one-to-one conversations with caregivers, teammates and developers can be a crucial way to think through what is in place to establish and foster trust in your learners' learning network and discuss other possible ways to further build upon this trust.

Questions You Can Think About or Discuss

Whether you hold a community meeting, attend a one-to-one conversation with a caregiver or hold a discussion with developers, it is important to be ready with good information and questions. Here are some key questions to consider in your discussions. These questions may also be useful during planning sessions with teammates as you think through establishing and fostering a Trusted Learning Environment:

What does trust mean in this learning community?

How will we demonstrate this trust to learners? To caregivers?

Are there inherent tensions between developer and learner goals that need to be addressed?

What information is collected from learners? Why and how will it be used, stored and protected?

If we cease to work with the same developer, what will happen to learner data?

How will we gather feedback and engage with learners? Caregivers?

How can we involve learners and caregivers in decisions related to learner participation?

What will we do if something goes wrong – i.e., bullying, data breach?
What is the developer's plan if something goes wrong?

ACTIVITY:

Questions for **DEVELOPERS**

Why You Should Care About Trust

Learning today is no longer limited to the physical walls of a schoolroom. It is made possible by a web of people, places, organizations and programs or learning networks that revolve around the learner. Today, there are countless opportunities to innovate and develop quality digital resources, tools and platforms to create or enhance learning networks which support learning that is active, engaged and personalized.

As a developer, you might wonder how you can build an application that utilizes learner performance data to allow teachers to adapt their instruction in real-time to meet learner needs and improve learning outcomes. In building this application and working with in- or out-of-school providers, you will want to build an infrastructure that protects learners' data so that data is used only to improve learning, and not for any other purpose.[13] You might also wonder how to establish and foster trust with learners, their caregivers, in-school and out-of-school providers who utilize your platform.

Community meetings or one-to-one conversations with caregivers, teammates and in-school and out-of-school providers can be a crucial way to think through what is needed to establish and foster trust in your learners' learning network and discuss other possible ways to further build upon this trust.

Questions You Can Think About Or Discuss

Whether you hold a community meeting, attend a one-on-one conversation with a caregiver or hold a discussion with in-school and out-of-school providers, it is important to bring good information and be ready to listen. Here are some key questions to consider in your discussions. These questions may also be useful during product development and roll out as your team thinks through embedding elements to establish and foster a Trusted Learning Environment:

What does trust mean in our learning community?

How will we establish this trust with learners? Caregivers? Providers?

What do we gain from learners' participation in this learning experience?

Are there inherent tensions between our goals, the in- or out-of-school provider's goals and the learner's needs that need to be addressed?

Does information need to be collected to improve learners' learning experiences and outcomes?

If so, what specific information needs to be collected? Why?

Does learner information need to be stored? How long? Where? For what purpose?

How will we protect learners' data? What systems and infrastructure need to be in place?

How will we gather feedback and engage with learners? Caregivers? Providers?

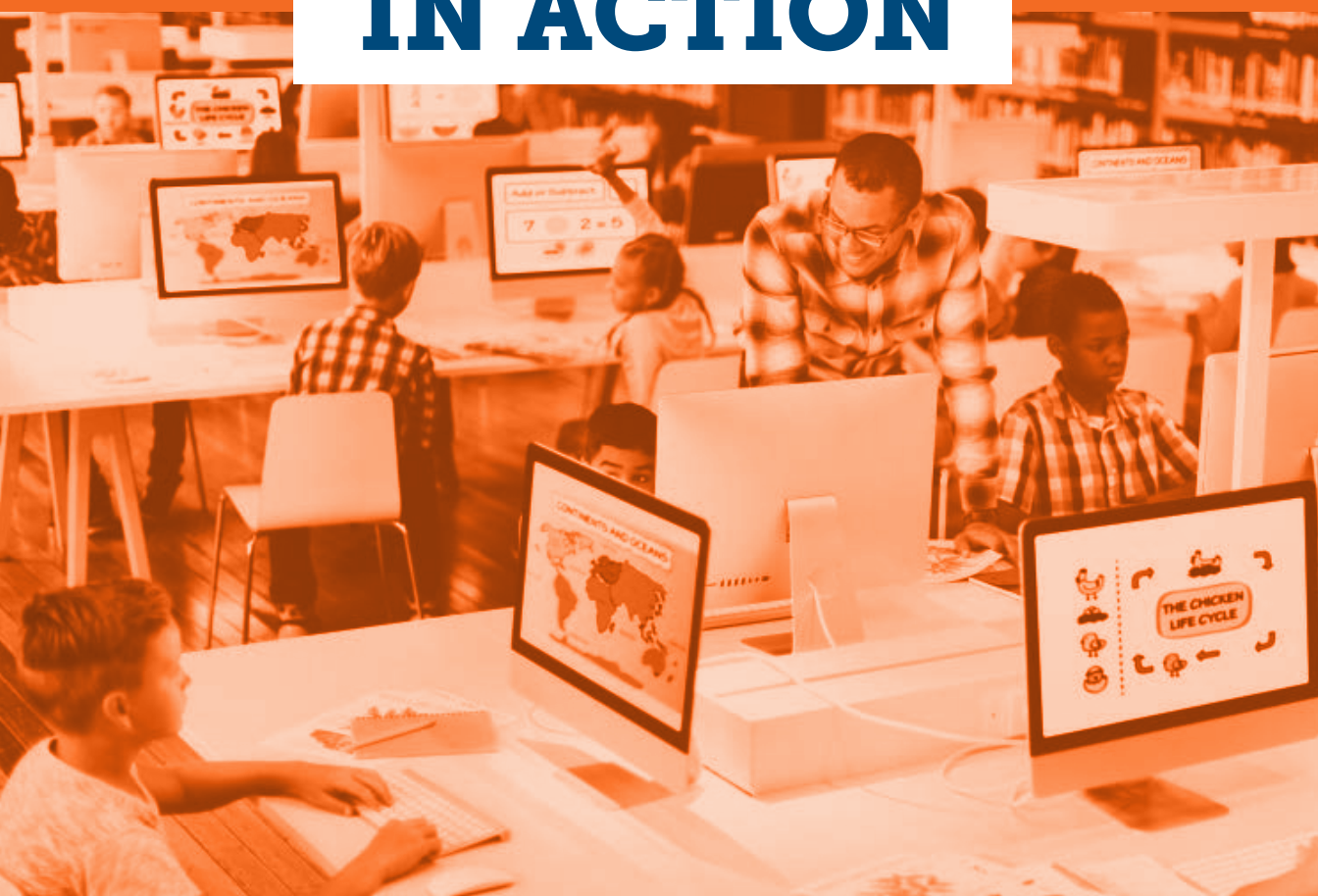
What will we do if something goes wrong – i.e., bullying, data breach?

What will happen to the data if we cease to work with the provider?

Are there best practices for our work? Can we learn from other developers in the education space or elsewhere who have prioritized trust?

More resources on how to run an effective convening can be found at www.libraryvision.org

BEST PRACTICES
IN ACTION



The following best practices were gathered through interviews in which pioneers of this area shared their experiences and lessons learned.

It is not a checklist or formulaic prescription, but rather a set of guideposts and a list of key elements to consider as stakeholders develop a plan to create trusted environments in their specific contexts. These elements are intended to inspire those who seek to advance this important work and provide direction to help interested actors get started.

1 Clearly define "trusted environment" and what "trust" means to your learner and their community.

As the Task Force report states, "A trusted environment is not easy to define precisely and will not be simple to construct." It is important to unpack buzzwords such as "trust," "privacy" and "safety" and define them in a way that supports the learner. For example, the learner may be seeking trusted content, a secure online platform, or trusted organizations with which to connect. Recommended examples and resources include:

- **MediaBreaker/Studios** is an online video editing and remixing platform that provides youth opportunities to re-democratize copyrighted content while learning about fair use and focuses on trusted media sources and trusted content. In this context, they define "fair use" in terms of critical remix, so that students are able to create critical comments about media, while transforming that media into something new and distinguishable from the original source material. At last count, the tool is in use by nearly 200 educators in 42 states. Their project contributes to the larger discussion about trust by providing a safe space to experiment with fair use and the deconstruction of media messages so that students become responsible and informed digital citizens who have "healthy digital relationships."

- **The Mozilla Foundation** is dedicated to protecting and building a healthy Internet as a global public resource, open and accessible to all. The foundation stewards Hive NYC, a peer learning network of groups like DreamYard Project, Mouse, Parsons, Educational Video Center, City-as-School, Reelworks and Urban Arts Partnership. With a grant from the Digital Media Learning (DML) Trust Challenge, the group developed the Building Connected Credentials project. The project studied existing and emerging credentialing practices (from portfolios to digital badging), shared promising practices, common tactics and viable models. The group concluded that using participatory design practices is key to developing valued and trusted credentials that can then be used to address systemic inequalities in access to learning.

- **The Center for Solutions to Online Violence (CSOV)** is a distributed network of activists, advocates, content creators and educators who want to enable women and feminists to take preemptive steps to ensure control of their online identities and to educate everyone about the many forms of online violence.[14] In creating CSOV, the network discovered that "trust" is complicated, and you must involve and understand the end user when building a trusted learning environment. The project kicked off with a multi-day meeting to hear what communities prioritized and to understand where existing mistrust resides. CSOV found that traditional safety mechanisms and tools might be dangerous to certain at-risk populations. For example, domestic abuse or violent crime survivors found two-step authentication systems threatening because many had created pseudonyms or used other identity obscuring strategies for self-protection.

2 Value the youth perspective and help them exercise their own voice.

In order to create trusted environments for learners, youth must engage in the process. Their feedback is critical not only in the creation of the product, program or platform, but also in getting their "buy in." However, not all young learners will immediately understand what questions to ask to ensure their safety and security. Therefore, it is also important to empower them with knowledge and help learners ask the questions that will allow them to navigate safely through a learning environment.

- Researchers from the **Youth and Media team at the Berkman Klein Center for Internet & Society** have curated and produced a Digital Literacy Resources Platform, which is an evolving collection of resources that teachers, administrators, parents, and youth can use to learn more about online safety, privacy, information quality, creativity, and copyright. One such resource is the "Safety, Privacy, and Digital Citizenship: Introductory Materials." This curriculum aligns with national standards and includes a variety of workshop modules that inform youth about key concepts related to privacy, safety and reputation.[15] In the workshop materials, there is a set of evaluation questions students can answer to reflect on what they have learned. It includes questions such as "How do you define privacy online?" and "Does privacy matter to you? Why?"[16]

- **DigitalMe** is a non-profit organization in the United Kingdom which helps young people gain skills and confidence through new technology by co-designing new ways to develop, assess and reward the competencies learners need to thrive. DigitalMe's Safe project is a program of activities that develops young people's digital skills, self-confidence and safety awareness when using social networking sites. For example, youth involved in the project expressed an interest in learning more about "digital footprints." They had heard of the term, but did not really understand the concept or how to develop positive digital footprints. This feedback was incorporated into the Safe program, which now includes the "Safe Digital Footprint," that provides an easy to understand definition and offers tips for creating positive digital footprints.

3 Engage experts across disciplines to address need.

The creation of trusted learning environments often requires multiple levels of expertise and diverse viewpoints. Combining education pedagogy with technical knowledge, legal and policy acumen will create a stronger program, product or platform. Recommended resources include:

- **VIF International Education** builds global education programs that prepare students for success in an interconnected world. The interdisciplinary team advancing VIF's Global Pathways project includes experts who specialize in education research and others from computer game decision and user interface design backgrounds. By approaching the work from multiple perspectives and allocating a lengthy amount of time to the ideation phase, they have been able to tackle their project in a way that creates the most open-ended tool possible while addressing users' needs.

- **Center for Solutions to Online Violence (CSOV)** emphasizes the need to think about how communities experience digital environments differently. In order to develop its content, CSOV created a team composed of 50% academics and 50% non-academics to have a richer conversation around online violence. CSOV initially envisioned building its own digital hub of living resources. However, it shifted its focus from production of specific content to content produced through broader community collaboration. CSOV now supports stakeholders in creating their own content or engaging in acts of activism in their communities. While handing over the creation of content to non-academics embedded within the communities was outside of its grant's initial vision, CSOV's end product is much more valuable and important for leveraging the diverse expertise of its larger community.

- **Safe** is a free curriculum of activities that develops student skills, self-confidence and safety awareness when using social networking sites. In 2014, computing curriculum became a mandatory part of every child's education in the United Kingdom. For many teachers, the resulting approach to digital education presented a chance to build on ICT lessons in an exciting new way. However, there was a "rising tide of panic" among others who were concerned that they did not have the knowledge, skills and resources required to respond to the new requirements. In response, DigitalMe teamed up to collaborate with O2, an organization that has worked with schools across the UK to support youth development of digital and enterprise skills. Together they created Safe which garners positive response from teachers.

4 Be proactive and be ready to react when necessary.

It is best to work with key advisors to gain knowledge of the current landscape – laws, regulations and technical capacity. Laws and regulations are often lagging with respect to the pace of technology. But your planning need not be constrained. Find the nexus of what is feasible and best for your organization and stakeholders. Remember: smart choices and a focus on higher standards will lead to success even when there are capacity challenges.

- **RyeCatcher** is a program whose mission is to ensure that all students, including kids with disabilities, are connected with high-quality service providers that support their diverse and unique needs. When RyeCatcher built its 2.0 tool, it sought to build within the product what encryption was legally required. When this process began, Secure Sockets Layer (SSL)[17] was a requirement for banking and credit card transactions, but not a requirement in education. RyeCatcher consulted its legal and technical partners and determined that using SSL was not so overwhelming that it would alter the fundamental architecture of its system. By incorporating SSL and working one-step beyond the level that was required, RyeCatcher was able to anticipate and be ready for the next development in data security. In turn, users experience a feeling of increased security regarding their data.

5 Understand that language matters.

Given language barriers and the complexity of policies that can be difficult for non-lawyers to comprehend, clear, concise and understandable language is critical.

- **MediaBreaker/Studios** conveys the purpose of its program to parents and non-digital media educators by talking in terms of "critical thinking skills" and "interest-driven learning" rather than "media literacy." This allows MediaBreaker/Studios to communicate its tool's purpose successfully.

- Members of the **Youth and Media team at the Berkman Klein Center for Internet & Society** define privacy as "the ability to control what other people know about you." The curriculum, co-developed with New York Public Library and WGBH, empowers educators to convey what privacy is and why it is important using straightforward language school-age students can easily comprehend. For example, "What privacy means to you and your family might be very different than what privacy means to the other kids in this class and their families. If we're more aware of what we value as private, and how our behaviors online can shape our privacy, we'll be able to make better choices about what kind of privacy we want."[18]

- **RyeCatcher** found that they are better able to engage parents, caregivers and families in conversations using familiar terms. For example, the term "permission" speaks to parents in a way that "consent" does not. Parents, caregivers and families understand the process of providing permission slips, emergency contact and transportation information to schools. The right language makes all the difference, and intimidating terminology should be avoided. RyeCatcher worked with content specialists and sociolinguists to develop simple text for emails or newsletters for each of their constituencies that describe their product, the work they are advancing and their end goals.

6 Pull from best practices and utilize lessons learned from previous organizations.

Many have tried, some have succeeded and some have failed, but all provide valuable lessons.

- **Mozilla Foundation** staff caution against not acknowledging the importance of past efforts that may have taken place under a different unifying label. Mozilla Foundation's Building Connected Credentials project examined the current New York City connected credentials ecosystem. In the context of New York City-based connected credentials work, many organizations conducted related work for decades. Their legacy and community provide a valuable resource from which innovations may draw inspiration, lessons learned and find new collaborators.

- To develop the **RyeCatcher** platform, legal and technical teams learned from the prior work related to electronic health information exchanges. While the content focus of RyeCatcher's work was different, the set of federal and in-school work laws RyeCatcher considered as it built its platform was a valuable model in the complicated interagency federal coordination that Data Use and Reciprocal Support Agreement (DURSA) was built to address.

7 Define clear roles among the learning network. Remember you are part of a learning network and the learner is best served when efforts are coordinated.

It is important to have partners in this work to build capacity and help lend expertise to further stakeholder efforts. However, it is also crucial to ensure alignment with partner beliefs. Partners must have clearly defined roles and understand where they fit in the trusted learning environment as there can be many actors with different skill sets advancing various facets of trusted environment work.

- Members of the **Youth and Media team at the Berkman Klein Center** emphasize that in order to enable a strong network for the learner, all partners involved should possess a good understanding as to where they fit in the trusted learning environment, what the goals are, and how different pieces work together to achieve these objectives.

- During the year of **Center for Solutions to Online Violence's (CSOV) Digital Media Literacy Trust Challenge** project, CSOV discovered that much of the content initially planned for development had already been created by other organizations. For example, they found resources related to online harassment and rapid response through the Speech Project started by the Women's Media Center and the Crash Override Network. As a result, CSOV decided to further the field and redirect their resources into augmenting the collective work and to partner rather than duplicate efforts. One area of particular focus is advancing the insights and experiences of women of color in particular. Various individuals and groups step forward and step back as needed to work on CSOV as a community driven and sustained project.[19]

RESOURCES LIST

Advocates & Experts

CoSN Protecting Privacy Toolkit
http://www.cosn.org/focus-areas/leadership-vision/protecting-privacy

CoSN Security Questions to Ask of an Online Provider
http://www.cosn.org/sites/default/files/03_SecurityQuestions.pdf

CoSN 10 Steps Every District Should Take Today
http://www.cosn.org/sites/default/files/Privacy_10_Steps.pdf

CoSN Trusted Learning Environment Program
http://trustedlearning.org

Data Quality Campaign and CoSN Student Data Principles
http://studentdataprinciples.org

Education Technology Industry Network of SIIA
http://www.siia.net/Divisions/ETIN-Education-Technology-Industry-Network/Resources/Student-Privacy-Data-Security-Toolkit-for-School-Service-Providers

EPIC Student Privacy Project
https://epic.org/privacy/student

Future of Privacy Forum: K-12 Education
https://fpf.org/issues/k-12-education

K-12 Blueprint: Toolkit
https://www.k12blueprint.com/toolkits/privacy

The LAMP
http://thelamp.org

RyeCatcher Family Trust Network
https://www.ryecatcher.com/family_trust_network

Student Privacy Pledge (Led by FPF and SIIA)
https://studentprivacypledge.org

Youth and Media, Berkman Klein Center
http://youthandmedia.org/publications/papers/all/%22

K-12 Tech Apps

ClassDojo
https://www.classdojo.com/learnmore

Globaloria
http://globaloria.com

MathCrunch
https://www.mathcrunch.com

Privacy Evaluation Platform developed by Common Sense Media
https://privacy.commonsense.org

Remind
https://www.remind.com

Government Sources

Children's Online Privacy Protection Act FAQs
https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

FCC's Children's Internet Protection Act (CIPA)
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Protection of Pupil Rights Amendment (PPRA)
http://familypolicy.ed.gov/ppra

US Department of Education Family Policy Compliance Office
http://www2.ed.gov/policy/gen/guid/fpco/index.html

US Department of Education Privacy Technical Assistance Center
http://ptac.ed.gov

ACKNOWLEDGMENTS

The Aspen Institute Communications and Society Program acknowledges and expresses deep gratitude to the MacArthur Foundation for their guiding advice and generous grant in support of this project. We also acknowledge the Penn Hill Group for their expertise and relentless effort in the creation and development of this guide from concept to its final release.

We also thank the educators, academics, policymakers and community partners who participated in interviews and critique sessions for the purpose of gathering a variety of perspectives. The guide is a synthesis of these various viewpoints and does not necessarily reflect the opinion of each participant or organization. We thank them for their generous contribution of time and expertise. The individuals and organizations involved in shaping the guide are (listed in alphabetical order by participant last name):

Linnette Attai
Founder
PlayWell, LLC.

Alan Berry
Author
The LAMP

Iris Bond Gill
Mozilla Foundation

Catherine M. Casserly, Ph.D.
Fellow
Aspen Institute

Sandra Cortesi
Director
Youth and Media - Berkman Klein Center for Internet & Society at Harvard University

M. Briggs DeLoach
Researcher
Youth and Media - Berkman Klein Center for Internet & Society at Harvard University

Sheryl Grant
Director of Alternative Credentials and Badge Research, HASTAC
Director of Social Networking, DML Competition, HASTAC
Duke University

Paulina Haduong
Fellow
Berkman Klein Center for Internet & Society at Harvard

Grainne Hamilton
Programme Director
DigitalME

Julie Keane
Head of Research
Global Gateway: VIF Process Lab

L. Arthi Krishnaswami
CEO
RyeCatcher Education PBC

Emily Long
Director of Communications & Development
The LAMP

Meghan McDermott
Mozilla Foundation

Lisa Mills
Speech Language Pathologist
Anne Arundel County Public Schools

Sandra Moscoso-Mills
The World Bank

Matt Rogers
Product Manager
DigitalMe

Felton Thomas, Jr.
President, Public Library Association
CEO, Cleveland Public Library

Joe Weedon
Ward 6 Representative
DC State Board of Education

Jacqueline Wernimont, Ph.D.
Interim Director, Nexus Lab
Director, Computational and Digital Humanities Certificate Program
Co-Director, HS Collab
Arizona State University

Peter Zamora
Director of Federal Relations
Membership and Outreach
Council of Chief State School Officers

Elana Zeide
Associate Research Scholar
Princeton Center for Information Technology Policy

Sarah Zeller-Berkman, Ph.D.
CUNY School of Professional Studies
Consultant to Mozilla

ENDNOTES

1 Elana Zeide, Future of Privacy Forum. (March 2016). "19 Times Data Analysis Empowered Students and Schools Which Students Succeed and Why?" https://fpf.org/wp-content/uploads/2016/03/Final_19Times-Data_Mar2016-1.pdf

2 Leah Plunkett, Urs Gasser. Berkman Klein Center. (September 2016). "Student Privacy and Ed Tech (K-12) Research Briefing." https://cyber.harvard.edu/publications/2016/StudentPrivacyBriefing

3 Alliance for Excellent Education. (August 2014). "Expanding Education and Workforce Opportunities through Digital Badges." http://all4ed.org/reports-factsheets/expanding-education-and-workforce-opportunities-through-digital-badges/

4 S. Abbot (Ed.). The glossary of education reform. (July 2015). "Hidden curriculum." http://edglossary.org/hidden-curriculum/

5 Edtech Wikis on EdSurge. (n.d.). "Adaptive Learning." https://www.edsurge.com/research/edtech-wiki/adaptive-learning

6 RyeCatcher. (2015). "Family Trust Network." https://www.ryecatcher.com/family_trust_network

7 Brenda Leong. Future of Privacy Forum. (May 2016). "Student data privacy: Moving from fear to responsible use." https://fpf.org/2016/05/23/student-data-privacy-moving-fear-responsible-use/; "5 Back to School Privacy Tips for Parents of K-12 Students." https://www.privacyrights.org/blog/5-back-school-privacy-tips-parents-k-12-students

8 Reg Leichty and Brenda Leong. Foresight Law + Policy and Future of Privacy Forum. (2015). "De-Identification & Student Data." https://fpf.org/wp-content/uploads/FPF-DeID-FINAL-7242015jp.pdf; Haduong, et. al. Harvard Berkman Klein. (2015) "Student Privacy: The Next Frontier Emerging & Future Privacy Issues in K-12 Learning Environments." https://cyber.harvard.edu/node/99063

9 Data Quality Campaign (DQC) / National PTA. (August 2013). "What Every Parent Should Be Asking about Education Data." http://dpi.wi.gov/sites/default/files/imce/wise/pdf/DQC-PTA-Data-Guide-for-Parents.pdf

10 Stephen Balkam. The Huffington Post. (April 2014). "Learning the Lessons from the InBloom Failure." http://www.huffingtonpost.com/stephen-balkam/learning-the-lessons-of-t_b_5208724.html

11 The Aspen Institute recognizes inequities in connectivity and while tackling this issue is not a focus of this guide, there are many organizations who do invaluable work in equitable access to connectivity, including the following: Consortium for School Networking (CoSN). (2016). "Digital Equity Action and Digital Equity Action Agenda." http://www.cosn.org/focus-areas/leadership-vision/digital-equity-action-agenda

12 Emily Long. The Learning About Multimedia Project (LAMP). (August 2016). "3 Things to Do Before You sign Up For Another ED Tech App." http://thelamp.org/3-things-sign-another-ed-tech-app/

13 Kim Wright. Harvard Berkman Center. (February 2014). "Student Privacy and Cloud Computing in the K-12 Edtech Space: A new report from the Berkman Center." http://today.law.harvard.edu/student-privacy-and-cloud-computing-in-the-k-12-edtech-space-a-new-report-from-the-berkman-center/

14 Center for Solutions to Online Violence (CSOV). (n.d.). "CSOV Community & Speaker's Bureau." http://femtechnet.org/csov-who-are-we/

15 Berkman Klein Center. Digital Literacy Resource Platform. (March 2016). "Safety, Privacy, and Digital Citizenship: Introductory Materials." http://dlrp.berkman.harvard.edu/node/85

16 Sandra Cortesi, David Cruz, Urs Gasser, Paulina Haduong, Andres Lombana-Bermudez, Jeremiah Milabauer, Leah Plunkett, Dalia Topelson Ritvo, and Zoe Wood. The Berkman Center for Internet & Society at Harvard University. IKeepSafe / The Berkman Center for Internet & Society. "Safety, Privacy, and Digital Citizenship - High School Curriculum." (March 2016). http://blogs.harvard.edu/youthandmediaalpha/files/2016/03/DLT-Curriculum-Introductory-Materials.pdf

17 As of 2016, online credit card transactions are protected via vendors compliant with the Payment Card Industry Data Security Standard (PCI DSS).

18 Youth and Media, Berkman Klein Center for Internet & Society, in collaboration with the New York Public Library and WGBH (featuring Ruff Ruffman: Humble Media Genius from PBS). (August 2016). "The Internet and You [Full Curriculum]. Digital Literacy Resource Platform." http://dlrp.berkman.harvard.edu/node/94

19 Jacque Wernimont. (July 2016). "Feminist Infrastructure as Metamorphic Infrastructure." https://jwernimont.com/2016/07/13/feminist-infrastructure-as-metamorphic-infrastructure

THE ASPEN INSTITUTE

Publications Office
P.O. Box 222
2014 Carmichael Road
Queenstown, Maryland 21658

MacArthur Foundation

Pub 3: 17/004
ISBN: 0-89843-657-5

A Project of the Aspen Institute Communications and Society Program and the
John D. and Catherine T. MacArthur Foundation