LEARNER AT THE CENTER OF A NETWORKED WORLD
Students should have safe and trusted environments for learning.
About the Aspen Task Force on Learning and the Internet

The Aspen Task Force on Learning and the Internet, with support and guidance from the John D. and Catherine T. MacArthur Foundation, is a group of 20 innovative and respected minds in technology, public policy, education, business, privacy and safety. The Task Force’s goal was to understand the ways in which young people learn today and to optimize learning and innovation within a trusted environment. From there, the Task Force defined how parents, teachers, young learners, businesses and nonprofits can expand new learning opportunities, online and off-line, and inside and outside the classroom.

After a year of study, outreach to stakeholders, public input and internal deliberations, the Task Force believes that a new vision of learning is emerging. But to ensure that young learners are able to take full advantage of the opportunity, we must resolve serious issues of trust, safety, privacy, literacy and equity of access. To help resolve some of these challenges, the Task Force has highlighted five essential principles and twenty-six action steps with the intention they be used as a guide for action – a tool to help those who wrestle with these issues at the local, state and federal levels to tackle them with new insights, clarity, and efficiency.

Members of the Task Force on Learning and the Internet

Jeb Bush (Honorary Co-Chair), State of Florida
Rosario Dawson (Honorary Co-Chair), Voto Latino
John Bailey (Co-Chair), Digital Learning Now!
Maria Teresa Kumar (Co-Chair), Voto Latino
Meredith Baker, CTIA Wireless Association
John Seely Brown, Deloitte Center for the Edge
Catherine Casserly, Creative Commons (through February 2014)
Anne Collier, Net Family News, Inc.
Dr. Wanda Cook-Robinson, Oakland Intermediate School District
Anil Dash, Activate and ThinkUP

Julius Genachowski, The Carlyle Group
Marne Levine, Facebook
Brendon Lynch, Microsoft
Alice Marwick, Communication and Media Studies, Fordham University
Bruce Mehlman, Mehlman Vogel Castagnetti, Inc.
Betsy Masiello, Google
Delia Pompa, National Council of La Raza
Mark Surman, Mozilla
Deborah Taylor Tate, United Nations ITU Special Envoy for Child Online Protection
Felton Thomas, Jr., Cleveland Public Library
Many online behaviors that have raised concerns among parents, such as bullying or stereotyping, are not new or unique to the online world but have their roots and analogs in off-line behaviors. Their remedies should be integrated into those already in place for dealing with real-world problems.

Parents, educators and others responsible for the welfare of young people have real concerns about the safety and privacy of children online.

To confidently pursue their learning goals, students need an environment where their safety and privacy are protected.

Ensuring student privacy is especially critical in networked environments that involve multiple entities providing services to students.

Data collection and use are crucial to fulfilling the vision of personalized learning, yet for some there is a lack of trust around the security and privacy of student data.

Approaches to providing safety online that are defensive and fear-based are often ineffective and can have the unintended consequence of significantly restricting learning opportunities for young people.

There is a need to explore alternative approaches that create trusted environments that protect learners’ safety, privacy and security without compromising their ability to pursue their interests.

Although technology is partly responsible for creating fear, it can be part of the solution by helping create trusted environments. But equally important is equipping learners, parents and educators with the skills to function online safely and effectively.

THE TASK FORCE FINDS:
Realizing the benefits of learning networks will necessitate a commitment to establishing trust with teachers, parents and students that children will have safe experiences online and that sensitive personal information is securely protected. Trust is a prerequisite for learning that is based on students exploring online resources, taking online courses and engaging with different educational partners. Without trust, the ultimate success of networked learning could be in jeopardy.

Unfortunately, too 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 and educators need to help create “trusted environments” that allow young people to pursue their interests safely.

A trusted environment exists when all stakeholders have confidence in using technology to engage in learning. It involves policies, tools and practices that effectively address the privacy, safety and security concerns related to learning online. It involves parents being able to trust that their children’s personally identifiable information is safe, secure and won’t be used in ways other than to help their academic progress. A framework for trust will emerge from conversations among local stakeholders that grapple with key questions related to students:

- **Safety** Am I physically and emotionally safe?
- **Privacy** Is my data being used appropriately? Do I have access to my data and records? Do I have the ability to determine how my data is used, by whom and under what circumstances?
- **Security** Am I confident that my data is secure? Are there adequate protections against unauthorized access?

Promising approaches such as “privacy by design,” “kid-readable disclosures,” “identity management tools,” and “trust framework architectures” need to be developed and tested. In addition to pursuing technology-based approaches, it is also important to give learners and parents the skills to navigate through the online world safely and successfully.
Create Trusted Environments for Learning.

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.

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.

To help this process along, the Task Force has identified an initial set of high-level principles intended to guide the process for developing a trusted environment. Key characteristics of such an environment might include:

- **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.

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

- **Data Stewardship.** Find ways to protect data that may include mechanisms to reduce the risk of harm, such as 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 be used to provide feedback about what works, thereby shortening the cycle to improve the ecosystem of learning networks.

- **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 regulatory arrangements to protect the integrity of learning networks with competent and appropriately-resourced bodies in place to enforce these principles.

THE TASK FORCE RECOMMENDS:

RECOMMENDATION 6

Create Trusted Environments for Learning.

The Task Force recommends:

- 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.

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

- Data Stewardship. Find ways to protect data that may include mechanisms to reduce the risk of harm, such as 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 be used to provide feedback about what works, thereby shortening the cycle to improve the ecosystem of learning networks.

- 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 regulatory arrangements to protect the integrity of learning networks with competent and appropriately-resourced bodies in place to enforce these principles.
These principles can guide governmental, nonprofit and corporate institutions as they create their plans for digitizing learning. The Task Force recommends that these principles focus on capabilities needed to be successful in college and careers, such as collaboration, communications, assessment and creation of content, rather than on the device or the tool, since those are constantly changing.

**Action V Invest in deeper research and studies on the efficacy of existing federal privacy laws, such as COPPA, CIPA and FERPA, as well as various state laws, and seek recommendations on how to improve and modernize them or develop more effective alternatives to support learning networks.**

Policy makers have responded to the concerns of parents and child safety advocates by creating a patchwork of legal and regulatory mechanisms intended to protect young people online (see Sidebar). Typically, these initiatives place restrictions on operators of websites or applications that are used by children. The most prominent federal law, the Children’s Online Privacy Protection Act (COPPA), requires websites used by young people to obtain explicit parental permission before they can collect any ‘personal information’ from children under age 13, along with other provisions governing marketing aimed at children.

Critics of COPPA point out that it was developed before the emergence of many cloud-based services, online resources and social media and fails to address the new media environment. For example, while children under age 13 can legally provide personal information with their parents’ permission, many websites simply bar underage children from using their services due to the additional work involved in complying with the provisions of COPPA. This has had the unintended consequence of encouraging children to make use of sites that do not attempt to enforce COPPA’s restrictions and that may be less conscientious about protecting young users. And by identifying a specific age to trigger its provisions, the law gives no protection to children over that age. In short, critics suggest, the law is overly restrictive and, arguably, relatively ineffective.

The Task Force sees a mismatch between current legal and regulatory approaches and the real needs of young people. It recognizes that Congress, the Federal Trade Commission, Federal Communications Commission, the U.S. Department of Education, other agencies, and individual states are all actively working on these important but sometimes emotional issues. The Task Force urges these policy makers to base their deliberations on evidence-based research. Accordingly, it calls on philanthropy and policymakers to support rigorous studies by skilled researchers of the strengths and limitations of these approaches, as we do not want to so overprotect our young learners that they do not have access to high-quality content. The Task Force also calls on funders to support researchers, legal scholars, or panels of experts to develop new approaches, tools and practices that could overcome these limitations.
Federal Children’s Protection Laws

COPPA
The Children’s Online Privacy and Protection Act (COPPA) is a federal law that went into effect in 2000 that governs the participation of young children in online activities. It requires a website operator to obtain “verifiable consent” from a parent or guardian for the participation of any child under age 13, mandates what must be included in a website’s privacy policy for young people and describes the responsibilities an operator has to protect children’s privacy and safety online, including restrictions on the marketing to those under 13.
⇒ coppa.org/coppa.htm

CIPA
The Children’s Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children’s access to obscene or harmful content over the Internet. CIPA applies to schools or libraries that receive discounts for Internet access through the Federal Communications Commission’s E-Rate program. To receive the E-Rate discounts, schools and libraries must have an Internet safety policy that includes technology protection measures that block or filter Internet access to content that could be harmful to minors. Before adopting an Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal. Schools are also required to monitor the online activities of minors and provide for educating minors about appropriate online behavior.
⇒ fcc.gov/guides/childrens-internet-protection-act

FERPA
The Family Educational Rights and Privacy Act (FERPA) is a federal law intended to protect the privacy of student educational records. The law applies to all schools that receive funds from the U.S. Department of Education. FERPA gives parents or students over age 18 certain rights with respect to educational records. Parents or eligible students have the right to inspect and review records maintained by the school and to request that a school correct records that they believe to be inaccurate or misleading. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student’s educational record.
⇒ ed.gov/policy/gen/guid/fpco/ferpa/index.html
**Action W:** Re-examine federal and state regulations governing collection and access to student educational data to provide appropriate safeguards that protect against specific harms relating to learners’ privacy and security and, at the same time, accommodate the future of learning tools and services.

Data on student learning, when collected properly and used appropriately, can be a vital tool for personalizing instruction and providing feedback on their progress. For example, with the Teach to One model, each student receives a unique daily schedule (called a ‘playlist’) based on his or her unique strengths and needs. The underlying data also allows for adjustments to the student’s schedule in order to better accommodate their ability and preferred learning method (e.g., within small groups or one on one with a teacher). Teachers can view real-time data on each student’s achievement and adjust their instruction accordingly. Data empowers not just personalized learning using online resources from a variety of providers, but also more informed teaching to ensure students are receiving the right resources, at the right time, in the right method.

Parents and others continue to be concerned about adequate protection of data in the learning process. Responses to this concern that completely close learning networks may offer some protections but also will hamper rich personalized learning and limit exposure to educational opportunities, resources and courses offered online. Important lessons can be drawn from the privacy work done in other sectors, such as health care, where regulations have struck a balance between protecting personal information in electronic medical records and enabling the sharing of data among doctors, nurses and other providers.

The Task Force recognizes the importance of protecting personal data and privacy. Indeed it becomes even more important in a networked learning environment, and systems will likely fail where such protections are not sufficiently taken into account. But given the enormous potential for supporting individualized learning through the collection and interpretation of student performance data, it is critical that rules and regulations be balanced between protecting sensitive data and ensuring students have access to a high quality education. The White House Big Data and Privacy Working Group Review, issued May 1, 2014, takes a similar twin goal approach: protect privacy and encourage innovation in education.

**Action X:** Design, implement and evaluate technology-based approaches to providing a trust framework that addresses privacy and safety issues while permitting learners to pursue online learning.

The Task Force recognizes that not every concern about privacy or safety online is amenable to a technological solution. But there are some areas where the sophisticated use of privacy-enhancing technology can help create a more trusted environment for young people. Rather than relying entirely on young people to take all of the steps...
necessary to protect their own privacy, website operators and app developers could build in safeguards through a process of “privacy by design.”

For example, credit card companies have established a Trust Framework architecture, in which each individual is given a unique digital identifier to protect against fraud. Developers of educational devices and platforms should explore Trust Framework architecture to provide a technical solution to the privacy and safety issues and more effectively enable children to explore their interests online for learning purposes. They should utilize data to focus on learner needs and capacity, creating safe tools and environments for learning. One example might be a tool that allows students access to their own data to encourage agency and allow the students to help define their learning pathway. This tool could be similar to the electronic medical records used in the health care arena where records are portable and transferable. Data from schools and from other avenues of a child’s life can create a fuller picture of his or her progress, goals and interests.

One approach provides tools that enable users to keep tabs on their own data collection and control their sharing with their peers in an open and safe space. The system, known as Open Mustard Seed, employs “trusted computer cells” (the basic units of individual control over data) that enable users to manage privacy settings and data collection and manage their digital personas (who has access to what information about me)? Service providers and app developers should also provide in-service user education on how to manage one’s privacy and safety.

**Action Y: Fund public awareness campaigns about the importance of and methods for acting safely and responsibly on and off-line.**

These campaigns could include public service announcements that empower individuals (young and old) to “manage their digital reputations.” watch out for one another and otherwise act responsibly online as well as understand that risks exist both on and off-line and there are ways to keep risk from turning into harm. Ideally, such campaigns would highlight the benefits of being online as well as the potential dangers that can be mitigated through digital literacy and other user education. Businesses could devote corporate resources to this effort just as they have done effectively with “Don’t TXT and drive” or “Stop. Think.Connect.”

**Action Z: Arm learners with the capability to protect themselves online through appropriate risk prevention education and teaching digital, media and social-emotional literacies.**

Media, digital and social-emotional literacies are “internal” tools to help keep one safe—the “filtering software” in their heads that’s with them wherever they go throughout their lives, typically improving with use. The Internet is a global medium beyond the control of authorities in the United States or any one country. A single country cannot legislate to keep all dangerous content off the web, and even if it did, bad actors will be out there. The best, first defense for protecting young people, online or off-line, is to arm them, starting at an early age, with the capabilities
to understand their environment and how to optimize their safety and privacy within it (see Action T).

For instance, the International Telecommunications Union has launched a global partnership for online protection which includes entities as varied as UNICEF, Disney, First Ladies and a small nonprofit in Nigeria. They have proposed Guidelines for Child Online Protection (COP) for ministers, parents, educators and the industry worldwide that include digital age literacies.61

A NOTE ON IMPLEMENTATION
There are a number of ways these action steps can be implemented. Many start with funding, of course, and we recommend that federal, state and local governments all take steps to fund pilots, experimentation and eventually full implementation of the steps called for in this report. Many of these recommendations can be embedded in existing funding streams that already support schools, libraries and nonprofits. We also call on philanthropies and businesses to mobilize support, funding and action around these action steps. With regard to the latter, businesses can not only fund through their corporate giving and employee assistance but also engage innovatively, such as by making their Wi-Fi hotspots available to students in their communities, building new privacy tools into their services and making their products interoperable with others. School districts can also collaborate in new partnerships that will take advantage of the experience and knowledge of other school districts, public agencies or private businesses.

The Task Force has also called for innovative ways of bringing its recommendations to fruition. One approach it finds particularly useful is the prize competition that is spelled out in Action L. We urge funders to sponsor such prizes in response to other Action recommendations as well.

Policy makers will need to take bold steps to bring to fruition the vision of the United States as a country of learners. It is our tradition, as is innovation in new technologies. Now the confluence of the two is posing a challenge to America’s education system. There may be risks involved in moving forward in a bold way, and there will no doubt be strong differences of opinion. But the opportunity is too significant for our country’s legislators, regulators or officials not to move with a sense of urgency in this area for the benefit of all learners, now and for future generations.

Most importantly, it will be on the shoulders of each parent, each teacher and each student to undertake the hard work of moving forward with a leap into the future.