Sharing the Health

Guidance for Schools When Procuring Mental Health Technologies

June 2023

CENTER FOR
DEMOCRACY
& TECHNOLOGY

Supported by

Youth and Media

CENTER FOR
DEMOCRACY
& TECHNOLOGY

The **Center for Democracy & Technology** (CDT) is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet. The organization is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

As governments expand their use of technology and data, it is critical that they do so in ways that affirm individual privacy, respect civil rights, foster inclusive participatory systems, promote transparent and accountable oversight, and advance just social structures within the broader community. CDT's **Equity in Civic Technology Project** furthers these goals by providing balanced advocacy that promotes the responsible use of data and technology while protecting the privacy and civil rights of individuals. We engage with these issues from both technical and policy-minded perspectives, creating solutions-oriented policy resources and actionable technical guidance.

Youth and Media

Youth and Media (YaM) encompasses an array of research, advocacy, and development initiatives around youth (age 12-18) and digital technology. Interacting closely with other teams at the Berkman Klein Center, YaM draws on the knowledge and experiences of individuals with various backgrounds, including psychology, ethnography, sociology, education, media theory, and the law. Building upon this interdisciplinary approach, YaM invites and amplifies the voices of youth throughout the research process, aiming to develop contributions that reflect and address young people's needs, perspectives, experiences, and interests. The team's work builds upon an evidence-base that offers unique insights into the creative, educational, and revolutionary possibilities of youth activity in the digital space while addressing the genuine concerns that come with living life online.

Sharing the Health:

Guidance for Schools When Procuring Mental Health Technologies

Author

Hannah Quay-de la Vallee

Acknowledgements

CDT thanks **Youth and Media** team members Sandra Cortesi, Madeline McGee, Leah Plunkett, and Elizabeth Sylvan for their advisory role in this project.

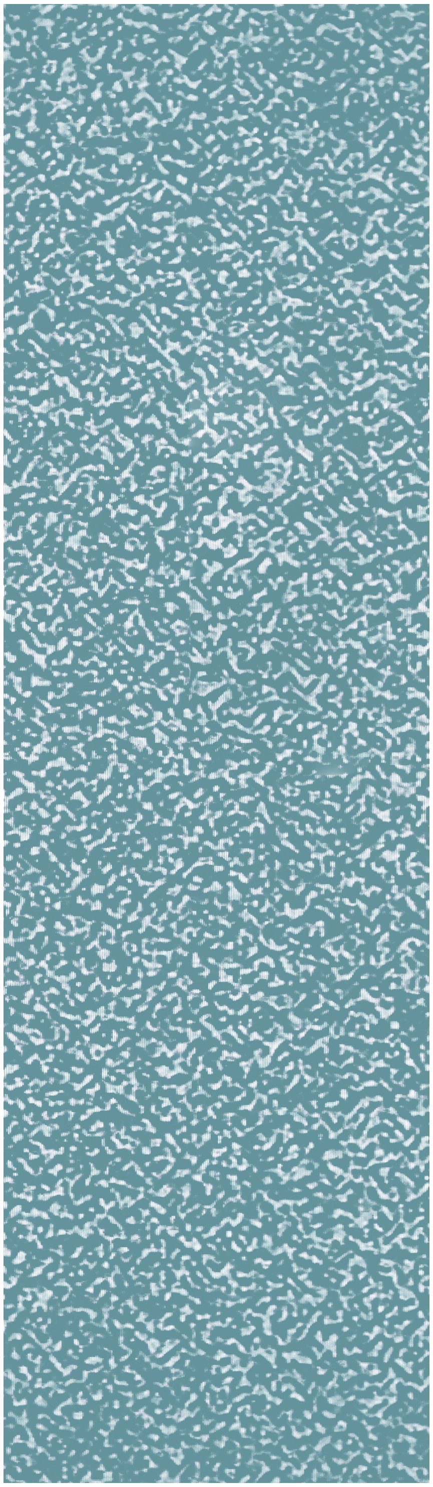
Links in this report include links archived and shortened by the Perma.cc service. The Perma.cc links also contain information on the original link, date of retrieval, and archive.

June 2023

This report is licensed under a Creative Commons Attribution-Sharealike 4.0 International License.

Table of Contents

Executive Summary



Although student mental health has long been a priority for schools, factors such as the pandemic and its aftermath and a rise in the prevalence of school shootings have pushed the issue of youth mental health to the forefront. Various factors, including staffing challenges, limited financial resources, weighty expectations placed on schools, as well as tech innovation, are pushing schools to find new, tech-based approaches to helping students manage their mental health. Most schools do not have the expertise in-house to develop the type of technology they want, so many are turning to vendor-provided products. While these products have the potential to help schools address this critical issue, the landscape of mental health products demands careful consideration on the part of schools that wish to procure these tools. **Technology that is not designed for the education context, ineffective at its stated goals, or insufficiently protective of student privacy could do much more harm than good for students.**

Consequently, it is important that schools procuring mental health technologies address these pitfalls. This report offers guidance to help schools and districts procure technology that will help them meet students' needs, rather than inadvertently placing students at risk of further harm. This report includes a discussion of the potential benefits and the risks presented by mental health technologies and provides procurement principles to help school staff determine if mental health technologies will serve their needs and, if so, select the most effective technologies for their contexts and communities.

These principles include considerations such as:

- **Data governance** to ensure that sensitive student data is protected;
- **Efficacy assessment**, to ensure that schools select a tool that has been proven to be effective at its stated purpose;
- **Regular evaluation** to ensure that the tool remains effective over the course of its use by the school; and
- **Bias auditing** to ensure the tool performs equitably across the school community.

Technology that is not designed for the education context, ineffective at its stated goals, or insufficiently protective of student privacy could do much more harm than good for students.

Introduction

Although student mental health has long been a priority for schools, recent discussions of a youth mental health crisis have pushed the issue to the forefront. In particular, concerns about students struggling with their mental health or harming themselves as reflected in a recent CDC report, especially as students grapple with the aftermath of COVID-19 and school shootings rise in prevalence, are urgent issues for schools.

Various factors, including staffing challenges (e.g., shortage of school counselors and teachers often thinly stretched across many responsibilities), limited financial resources, weighty expectations placed on schools (such as identifying students at risk of harming themselves or others), as well as tech innovation, are pushing schools to find new, tech-based approaches to helping students manage their mental health. Most schools do not have the expertise in-house to develop the type of technology they want, so many are turning to vendor-provided products.

These vendor offerings are focused on understanding, addressing, and/or treating students' mental health. While these products have the potential to help schools address this critical issue, the landscape of mental health products demands careful consideration on the part of schools that wish to procure these tools. Though it is typically adopted with the goal of helping and supporting students, using technology that is not designed for the education context, ineffective at its stated goals, or insufficiently protective of student privacy, could do much more harm than good for students. Consequently, it is important that schools procuring mental health technologies address these pitfalls. This report offers guidance to help schools and districts procure technology that will help them meet students' needs, rather than inadvertently placing students at risk of further harm.

Understanding Student Mental Health

As mental health is a complex topic, and the term mental health can be understood in different ways, this paper will use – based on definitions by the American Psychological Association, the Centers for Disease Control and Prevention, and work currently conducted at Youth and Media – the following framework for what constitutes “mental health:”

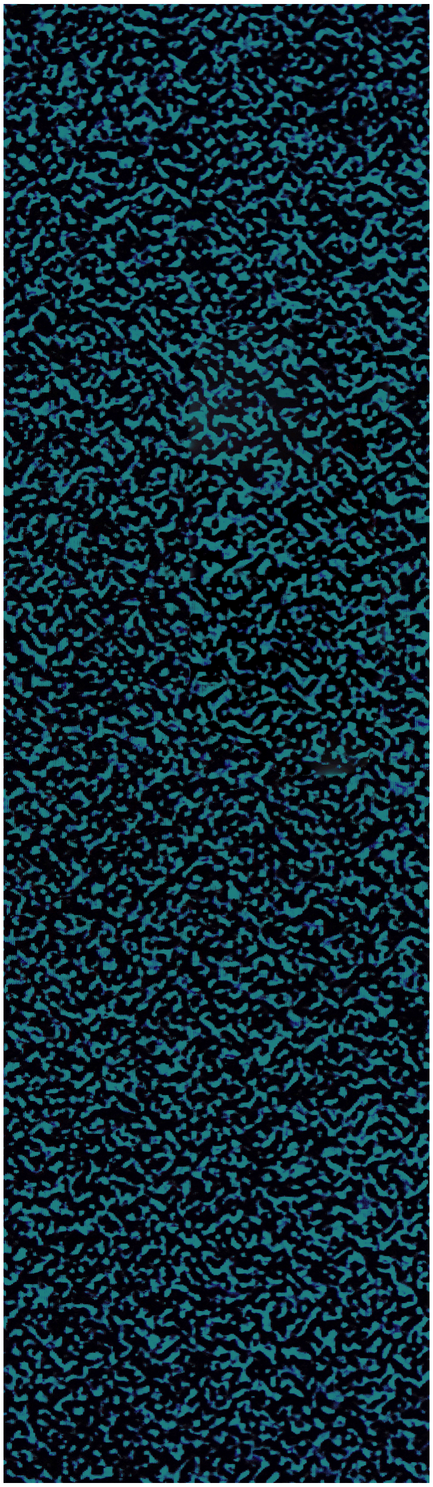
- **Mental health is one component of overall health**; it is different from physical health.
- **Mental health is composed of three elements:** emotional, psychological, and social.
- **Mental health challenges range from symptoms to diagnosable diseases.**
- **Mental health is not only managing challenges;** it is also supporting robust emotional, psychological, and social health.

Mental health technologies, then, are those that are intended to help address the mental health needs of students.

Goals of Mental Health Technologies

Technologies aimed at addressing mental health have a number of intended purposes: Some technologies are focused on understanding the landscape of mental health among their students and community, such as platforms that help schools conduct student surveys. Others are designed to alert schools to students who they believe to be at risk of harming themselves or others due to a mental health crisis. Still others aim to strengthen the mental health of students, whether that be at the student body level or at the individual student level. Despite their diversity, all of these technologies are meant to help schools understand, improve, or support their students' mental health.

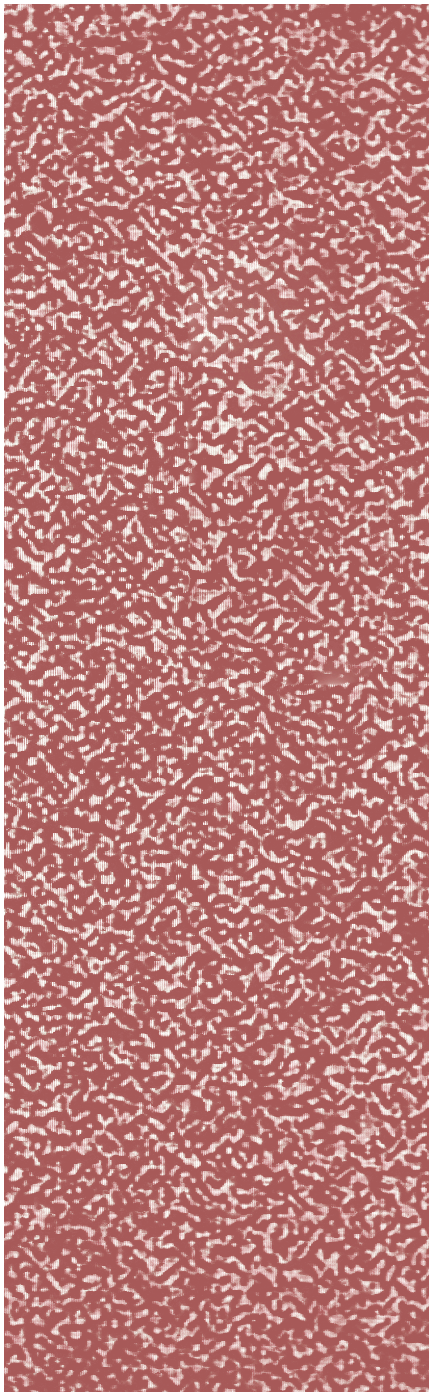
Defining *Procurement*



While some schools may choose to build mental health technologies themselves, most will likely procure the technology from a third party, since developing effective and safe mental health technology requires expertise and resources beyond what most schools and districts will maintain in-house. Procurement is the process of defining requirements, seeking bids, and ultimately acquiring an appropriate product.

This guidance focuses on how to build a procurement process to select safe and effective mental health technologies and hold product vendors accountable for protecting students, as acquiring such technologies is a critical foundation for a mental health program that supports students. It will not provide guidance on how to use and govern mental health technologies once they have been procured, though schools should ensure that they have a robust data governance program and a strong understanding of general best practices for student data privacy.

Potential Benefits, Risks, and Harms of Mental Health Technologies



Using technology to address student mental health has a number of potential benefits. However, in order to reap those benefits, mental health programs must be approached thoughtfully and managed carefully, and educators should be appropriately trained to avoid potentially harming students.

Potential Benefits

Technology-based mental health programs may range from collecting data to understand the mental health needs of the community to supporting students in managing their mental health to improve learning outcomes and overall well-being. These programs can confer a number of benefits for schools and their students and communities:

- **Wide reach.** Most importantly, technology-based programs may allow schools to serve more students in a more systematic way than relying on approaches like counseling staff. This benefit can be a result of cost savings over traditional staffing or because shortages of qualified workers do not allow for the level of staffing a school would prefer.

- **Ease of use.** Technology solutions may allow for more functional and usable improvements to existing programs. For example, online surveys may be easier for students and families to respond to, as well as enable much more robust data analysis. Similarly, technologies can add additional modes of communication and interactions, allowing students another channel of access to trusted adults.

- **Integration into school systems.** Technology-based programs may allow schools to more easily integrate their mental health programs into the rest of their technology systems, allowing teachers and other practitioners to incorporate a more holistic view of their students.

Risks and Potential Harms

The sensitivity around mental health means that using technology in this space carries risks to the privacy and safety of students and the broader school community. This section will focus on those risks that are most likely to arise when using third-party technology and which can be managed or mitigated through the procurement process:

- **Privacy and misuse.** The sensitivity of mental health information means that allowing a third party to collect or access such information creates significant privacy risks. If information is leaked or breached, it could cause increased harm to students in the form of social stigma, in addition to the standard harms of a data breach (such as placing families at risk of financial damage and losing community trust). Similarly, if vendors use or disclose mental health data in a way that the school community does not expect or does not approve of, it could cause harm to students and damage the trust that the community places in the school. Additionally, these scenarios may also cause a chilling effect, where the community is less willing to share information with the school going forward. This loss of trust could hamper the school in its primary mandate of educating students if students and parents do not fully engage with the school going forward.

- **Safety.** Mental health information often contains data that, if it is revealed to the wrong people, can put students in an unsafe situation. For instance, if a student reveals that they identify as trans in order to discuss identity-based bullying that is harming their mental health, outing the student to their family may result in the student losing their housing or being subject to abuse. Students who report challenges that they are experiencing in their home environment may face repercussions in that environment if their family learns they are disclosing the information. If schools do not ensure that any products they use take protection and governance of this sensitive data seriously, they may place their students at risk.

- **Inequitable effects.** Technologies that have different efficacy depending on the population of students can create inequities, or exacerbate historical inequities, in mental health. Schools that do not select technologies that perform equitably may further these biases, harming marginalized, underserved, or disadvantaged student populations.

- **Wasted resources.** If the technologies do not fulfill their intended purpose and effectively support the school community, the resources spent on the technology (both financial and human) will be wasted, when they could have been used to support more effective approaches to the critical issue of promoting students' mental health.

These risks, if not effectively managed, can derail a school's mental health program. Many of these risks can be managed, and potential benefits encouraged, through the procurement process.

If schools do not ensure that any products they use take protection and governance of this sensitive data seriously, they may place their students at risk.

Legal Compliance

Tools to provide mental health support may gather sensitive information that is traceable back to individual students, meaning that schools have legal obligations regarding that student data, including requirements under the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Health Insurance Portability and Accountability Act (HIPAA), and state laws.

Family Educational Rights and Privacy Act (FERPA)

FERPA is the primary federal law governing public K-12 institutions' maintenance and sharing of student data, including disclosing student data to school contractors and when data may be considered "deidentified:"

- **School contractors.** FERPA permits schools to share student data with contractors such as the vendors of online apps if they meet certain requirements. The contractor must perform an "institutional service or function" for which the school would otherwise use employees, remain under "direct control" of the school in its use of student data, have a "legitimate educational interest" in the data, and use the data only for purposes authorized by the school.

- **Deidentified data.** FERPA does not apply to student data that has been truly "deidentified," meaning that the data is no longer "linked or linkable" to an individual student. Deidentification, however, requires more than simply removing students' names or identification numbers. To determine if data is truly deidentified, a school must compare it to data in the same set, in previous data sets, and in publicly available information. Thus, descriptions of a student's unique or well-known personal characteristics or highly publicized events may not be deidentified, even if the student's name has been removed.

Protection of Pupil Rights Amendment (PPRA)

The PPRA is the primary federal law governing public K-12 institutions' collection of certain sensitive information. The PPRA prohibits schools from asking students to take surveys related to "mental or psychological problems of the student or the student's family" unless:

- For required mental health surveys funded as part of a U.S. Department of Education program, the schools obtain parental consent prior to requiring students to take the survey; or,

- For optional surveys or surveys not funded by a U.S. Department of Education program, the schools provide parents with notice and an opportunity to opt-out of the survey.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Privacy Rule applies to a limited set of healthcare professionals and expressly exempts student data covered by FERPA from its requirements; thus, most public K-12 institutions are not usually covered by HIPAA's Privacy Rule. However, some institutions, such as private clinics on campus or private K-12 schools that provide healthcare services may be covered by HIPAA, and must adhere to its restrictions on sharing students' personal health information and ensure that their vendors do so as well.

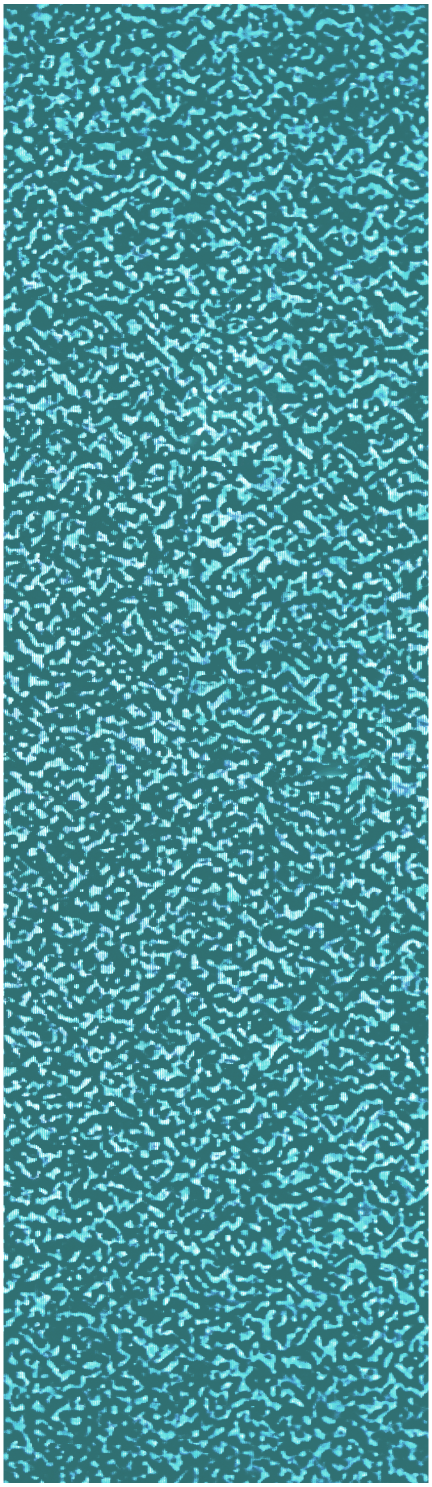
State law

More than 140 state laws governing student privacy have been passed, and schools should consider their impact both to comply with their privacy requirements and to mitigate their impact on marginalized groups of students:

- Privacy protections. Many states have passed laws similar to the PPRA, but with slightly varying requirements by imposing additional notice requirements or expanding the list of protected topics to include gun ownership, family life generally, and medical history beyond "mental or psychological problems."

- Mitigating impact on marginalized groups of students. Other states have passed laws or implemented executive orders that may require schools to notify parents or other governmental entities about a student's LGBTQ+ status or research into controversial topics; schools should consider whether those state laws could apply to data gathered from mental health tools and if they may lead to unintended consequences for marginalized groups of students.

Procurement Principles



To select products that maximize the benefits of using mental health technologies while minimizing the risks to students, administrators should consider incorporating certain principles into the procurement process. The principles are divided into categories based on how the school intends to use the technology, as certain uses will raise specific concerns. Addressing the specific risks of specific uses is another reason for administrators to have a clear understanding of what their goals are when procuring mental health technologies.

Overarching Principles

While certain uses of mental health technology warrant more specific procurement considerations, some principles will apply to the procurement of any mental health-related technology, regardless of its intended purpose:

- **Community engagement.** Go through a robust community engagement process to gather feedback from a broad range of community members and experts, such as students, parents, teachers, mental health practitioners, and technical staff. Administrators responsible for the procurement should aim to understand what limitations or guardrails the community would like to have on any technology put in place. These discussions should then feed into the procurement process to select technology that is capable of implementing those guardrails. The community should be engaged in a discussion of any specific technologies, even if there has been a community engagement process about student mental health in general. Any specific tool may raise new considerations that should be incorporated into the procurement process. To that end, schools should ensure that stakeholder views are present throughout the lifecycle of the technology, such as by creating an advisory group, similar in makeup to those consulted in the earlier engagement process, that is incorporated into the procurement and management of the technology.

- **Purpose-first approach.** Determine the goals of any technology before beginning the procurement process. These goals should provide the foundation for the procurement process, informing RFPs and analyses. Because technologies aimed at addressing mental health have a number of intended purposes, schools should ensure that the functionality of the tool they procure is aligned with their specific needs. Consider, for example, a school that feels it could improve its students' mental health by providing better avenues of communication between students and trusted adults to allow students space to discuss mental health issues. A technology that provides training in meditative techniques might be beneficial in the abstract but would not serve that school's specific needs. If the school cannot find a suitable product, or they are not sufficiently satisfied that the developer has shown that their product is effective, they should reconsider adopting a technical approach, as the resources that would have gone to that product may be more valuable spent on a non-technical intervention.

- **Data governance.** Because mental health data is sensitive, any mental health technology adopted needs to allow those who will administer it to perform robust data governance functions. Given that, the procurement process should select vendors that are able to meet the following requirements, which could be included in a request for proposals and subsequent contract:
  - *Data minimization.* Administrators must be able to decide what sort of data they wish to collect and store;
  - *Data retention.* Administrators must be able to delete (or require the vendor to delete) data as necessary, determine the technical strategies and business rules by which data is destroyed, apply additional use limitations to deidentified data, and receive assurances that information has been destroyed;
  - *Access limitations.* Administrators must be able to determine who sees what data and establish limitations on when and how data is accessed. Administrators should consider the physical and psychological safety of students as part of determining who has access to mental health data, and ensure that the tool enables them to tailor guardrails based on the sensitivity of information around things like therapy notes;
  - *Data use restrictions.* The vendor must allow administrators to determine how the data collected will be used. If a tool does not allow administrators to, for example, disallow any secondary use of the data, the tool may not be suitably protective of student data;

  - *Secondary uses and disclosures.* Administrators must ensure that information collected will not be used for purposes beyond the scope of the contract and that it cannot be redisclosed without written permission;
  - *Data breach notification.* Administrators must be notified in a timely manner if there is a suspicion of information being accessed by unauthorized users.

- **Strong privacy and security controls.** Maintain control of student information through negotiated individual contracts and related data sharing agreements, not click wrap or other "contracts of adhesion" provided by the vendor, which may serve to protect the vendor, and may not address the specific needs or requirements of the school. The education institution must maintain control of student data, including through legal, administrative, or technical means or by physical possession of the data, to ensure that it is not repurposed or used in unexpected or harmful ways. Privacy and security controls that schools should require of vendors include:
  - *Privacy and security requirements.* Vendors must provide appropriate levels of security and privacy protections for the data created or handled by their product. These requirements may include but are not limited to:
    - » Standards for transmission and storage of data.
    - » Permitting individuals to exercise control over their data.
    - » Identifying primary points of contact for privacy and security responsibilities.
    - » Privacy and security training for staff with access to sensitive data.
  - *Legal agreements.* Assurances provided by bidders must be memorialized in a formal contract and/or related data-sharing agreement with the selected vendor; state education agencies should consider providing or mandating standardized contractual provisions with minimum privacy and security standards.

- **Sub-vendor compliance.** If a vendor uses sub-vendors for any component of their product or system, the primary vendor must certify that the sub-vendor will also comply with any relevant requirements set out for the primary vendor. For instance, if a vendor uses a sub-vendor for data storage, the primary vendor must ensure that the sub-vendor adheres to any secure storage requirements.

Data Collection and Analysis Principles

Data collection and analysis approaches are those that do not aim to facilitate any sort of intervention or mental health goal but rather serve to help educational institutions understand the state of their student body's mental health and the challenges they face. Examples of this approach would include **school climate surveys, mental health surveys,** or any other way of collecting quantitative or qualitative data about students' mental health. While this may appear to be a lower-risk approach it can carry significant risk, as evidenced by the challenges to protect student data faced by King County, WA following the adoption of such a tool.

To address privacy and ethical challenges related to this use of mental health technology, procurement policies and practices should include:

- **Parental or student opt-out.** Programs designed to collect this sensitive information must allow for parents and students to opt out of the data collection; indeed, depending on the content of the survey the school may be legally required to do so. Vendors that provide survey distribution platforms must ensure that their tool provides a clear way for parents and students to opt out of participating.

- **Data use restrictions.** These restrictions, though important for all mental health technologies, are particularly critical for information-gathering technologies. Gathering sensitive data from the community requires trust that the data will be used only to inform administrators and not repurposed or misused, so it is critical that schools select vendors that are able to implement strict controls on data use, ensuring that the data is used only for educational purposes as defined under FERPA.

- **Privacy-first design.** Schools should require the vendor to provide information on how they design privacy into their system (for instance, by using strong encryption when collecting and storing sensitive data like student survey responses).

- **Use of commercial tools.** Commercial tools not designed for an educational context may not be designed to comply with education-specific laws and regulations. If considering such tools, schools should require information about how the tool complies with those requirements. This means vendors must be able to provide information like how their tool will comply with legal requirements governing student data, how their staff will be trained regarding student and educational data, and how their data governance procedures will serve the school's needs.

Support and Intervention Principles

Support and intervention efforts are those designed to improve the overall mental health climate of the student population, facilitate interactions that would support student mental health, and/or offer therapeutic interventions for diagnoses made by licensed providers. This category may include things like community-building or communicationfacilitation apps and platforms that provide trainings on topics such as self-care or healthy relationships.

To address privacy and ethical challenges related to this use of mental health technology, procurement policies and practices should include:

- **Efficacy assessment.** Schools should take steps to ensure that they select a tool that has been proven to be effective at its stated purpose. To assess this, schools should require independently-verified research about the tool's efficacy, and if unavailable, request information from vendors during and throughout the procurement process on how they have evaluated their technology for efficacy. Vendors that cannot provide such information may not have done enough evaluation to ensure their product is effective. This research should be evaluated on the school's behalf by someone with expertise in child and youth mental health, such as a licensed mental health practitioner.

- **Regular evaluation.** In addition to an initial evaluation, schools may also wish to analyze efficacy within their own community. To do this, they will need to select a vendor that is able to provide them with sufficient information about the tool's operation and set expectations through the RFP and contractual processes that this information is expected to be delivered on a predetermined basis. Although schools may do some of this assessment outside of the tool itself (such as through surveys about the tool's effectiveness) where possible, schools should select a vendor that is able to provide information about how the tool is being used within the school.

- **Bias auditing.** Tools must not create or exacerbate any biases amongst the school community (such as a meditation app that only works on late releases of an operating system that are incompatible with older phones). Administrators should include accessibility requirements in their RFP process that address issues like accommodating individual disabilities (e.g. speech to text for hearing-impaired students), offering different language(s), and ensuring diverse device or operating system compatibility. For AI-based tools, the AI system should be included in the bias audit. If schools are unable to find suitable tools that provide this information, they may consider provisional contracts that include a requirement that the vendor will start doing assessments, share the findings with the school, and commit to remediating any bias issues discovered by these assessments.

Sharing Mental Health Data with Law Enforcement

Sharing data with law enforcement should always be cause for caution, and mental health data is certainly no exception to that rule. In fact, prior CDT research has shown that for student activity monitoring systems (which often have detecting student mental health challenges as part of their stated goals), sharing data with law enforcement raises significant concerns for parents, particularly parents of Black, Hispanic, and LGBTQ+ students. These reports are particularly concerning in a legal environment where many state legislatures are introducing bills that further marginalize LGBTQ+ students in school environments. Additionally, teachers who work with students with disabilities are more concerned by sharing with law enforcement than general education teachers. This is particularly troubling given that these monitoring systems often result in law enforcement involvement: CDT research has found that 37 percent of teachers at schools that use student activity monitoring outside of school hours report that a third party focused on public safety, such as law enforcement, receives alerts from the monitoring system after hours, and 44 percent of teachers report that one or more students have been contacted by law enforcement because of behaviors flagged by the student activity monitoring system.

While sharing data with law enforcement is typically done with the goal of preventing harm to students, these concerns highlight that it can provide another avenue for disciplining students and can widen the school-to-prison pipeline. Worse, these negative impacts are not felt uniformly, but rather fall disproportionately on already-marginalized student populations.

Due to the risks of this sharing, vendors should not share data with law enforcement without school permission unless it is required by law.

Harm Prevention Principles

Harm prevention approaches to student mental health typically aim to prevent events that may harm students' mental health or prevent harm as a result of student mental health, such as self-harm or other violence by students. Technologies used in these approaches may include student activity monitoring systems or social media monitoring systems. Although these technologies are intended to prevent harm, they can also *cause* harm, such as outing students or chilling student exploration.

To address privacy and ethical challenges related to this use of mental health technology, procurement policies and practices should include:

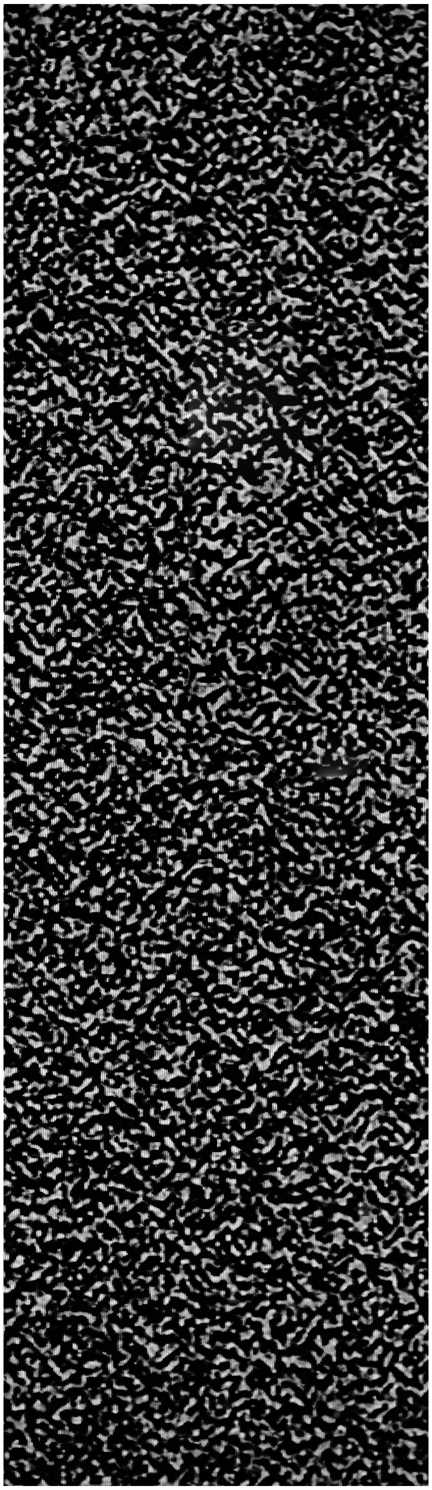
- **Impact assessment.** Understanding the impact of a harm prevention technology is critical to ensuring that it does not negatively impact students. An impact assessment is a structured process for determining how well a tool addresses its stated goal and what other impacts it may produce. Several harm prevention technologies have exhibited disproportionate negative impacts on certain marginalized student populations, such as Black and Hispanic students, students of lower socioeconomic status, students with disabilities, and LGBTQ+ students. Administrators should require the vendor to provide the results of any impact assessments or other equity evaluations the vendor has done or commissioned. Vendors who cannot provide such assessments may not have taken care to ensure that their tool performs equitably across populations.

- **Regular evaluation.** In addition to an initial impact or equity assessment, schools should take steps to ensure that they select a vendor with an ongoing commitment to equity. Schools should require regular assessments from their vendor, incorporating this requirement into their contracts and RFPs. Schools may also wish to analyze the impact within their own community. To do this, they will need to select a vendor that is able to provide them with sufficient information about the tool's operation. For instance, a threat assessment system would need to provide information such as the demographics of students who are flagged so the school can compare disproportionate impacts. As with vendor-run assessments, schools should ensure that the data sharing needed to do their own assessments is embedded in their final contracts.

- **Data handling customization.** Limiting the potential negative impacts of harm prevention technologies requires implementing secure and legally-binding guardrails around the technology. This requires selecting a tool that, either off the shelf or via customization, allows the school to enforce those guardrails. This may mean things like allowing the school to determine what information is collected, when the tool is in operation (allowing a school to choose not to monitor their students outside of school hours or outside of school grounds), or how reports or flags from the tool are handled. An important consideration within data handling more generally is how data is shared with law enforcement, either proactively or in response to requests. Schools should specify that data should not be shared with law enforcement without their consent unless it is legally required (e.g., a court order).

Although these technologies are intended to prevent harm, they can also cause harm, such as outing students or chilling student exploration.

Conclusion



Procurement is one component of responsible use of technology to support mental health, and the above principles can help schools ensure that they are selecting technology that can best support their students.

However, procurement is only one step in an ongoing process to limit harm and ensure that these technologies are used to support students. These procurement principles can help schools set themselves up for an effective and equitable mental health technology program.

Appendix

Excerpt of Model RFP Language for Procuring Mental Health Technologies

This appendix provides sample RFP language to capture the principles outlined in the guidance above. This is not an exhaustive list of requirements for vendor-provided technologies, as schools will also want to ensure that the technologies they procure are interoperable with the rest of their system, that it clearly outlines the intended technology purpose, that it is appropriately priced, and any other requirements they need.

Purpose-first approach. Supporting the mental health of students is an important component of supporting the overall health of students, which is critical to success in school. Having a strong technical program to support mental health while also preserving students' privacy can help build a framework where student mental health is supported. *[insert institution name]*, ("the school") invites qualified vendors of a technology product capable of *[insert technology purpose]* ("the product") to submit proposals for the contract outlined below.

The product shall only be used for these purposes and never used for non-educational purposes, including but not limited to commercial purposes, data resale, data profiling, or other non-educational uses.

Data governance. The product provided by the vendor must adhere to the following specifications:

- The product must allow administrators to customize data that is collected, including the ability to minimize sensitive data fields from collection if that data is not required for the functioning of the product.

- The product must allow administrators to customize pre-set retention timelines of *[insert desired timeline]*, or similar, for all elements of student data, after which time student data will be deleted from the school's system and from the vendor's data storage system unless an authorized administrator requests that the data be retained.
- The product must allow administrators to delete student information upon request. The vendor must be able to certify that the data has been deleted using industry best-practice deletion methods. The vendor must provide a certificate of deletion signed by the technical leader for data management.
- The product must include a role-based access management system controlling access to student data. Those roles must include *[insert required roles]*.
- The vendor may not use the data collected by and stored in the product for any purposes other than providing the contracted services.
- The vendor shall notify the school of any data breach, security breach, or suspicion of such a breach within *[insert time frame]*.

Strong privacy and security controls

- The school shall retain control of all data created or used by the product. The data shall not be reused or repurposed for any use other than the delivery of the product services unless explicitly allowed by the school.
- The vendor shall use industry-standard best practices for the transmission and storage of all student data.
- The vendor shall provide the school with primary points of contact for those responsible for the privacy and security of the school's data.
- The vendor will provide privacy and security training for all of their staff who will access or interact with student data.
- All security and privacy assurance provided by the vendor shall be memorialized in a formal contract or related data-sharing agreement.

Sub-vendor compliance. If the vendor employs any sub-vendors for any component of their product or system, the vendor will certify that the sub-vendor will also comply with any relevant requirements set out for the primary vendor.

Vendor equirements

- The vendor shall provide regular training to administrators and other staff on effective use of the product.
- The vendor shall provide the results of any bias audits they have conducted on their product, as well as information about how any concerns or problems uncovered by the audit have been addressed. If the vendor has not performed such an audit, they must do so within *[insert time period]* of receiving a contract with the school and will take steps to mitigate any issues uncovered within *[insert time period]* of completion of the audit.

Privacy-first design. The vendor will provide the school with information about how their system has been designed with privacy and security in mind.

Efficacy assessment. The vendor will provide the school with any assessments they have performed or commissioned to assess the product's efficacy.

Product accessibility. The product shall be accessible in *[insert list of languages used in the school community]* and shall be accessible via *[insert accessibility needs required by the student body]*.

Impact assessment. The vendor shall provide the results of any impact assessments or other equity evaluations the vendor has done or commissioned.

cdt.org

cdt.org/contact

Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

202-637-9800

@CenDemTech

CENTER FOR
DEMOCRACY
& TECHNOLOGY