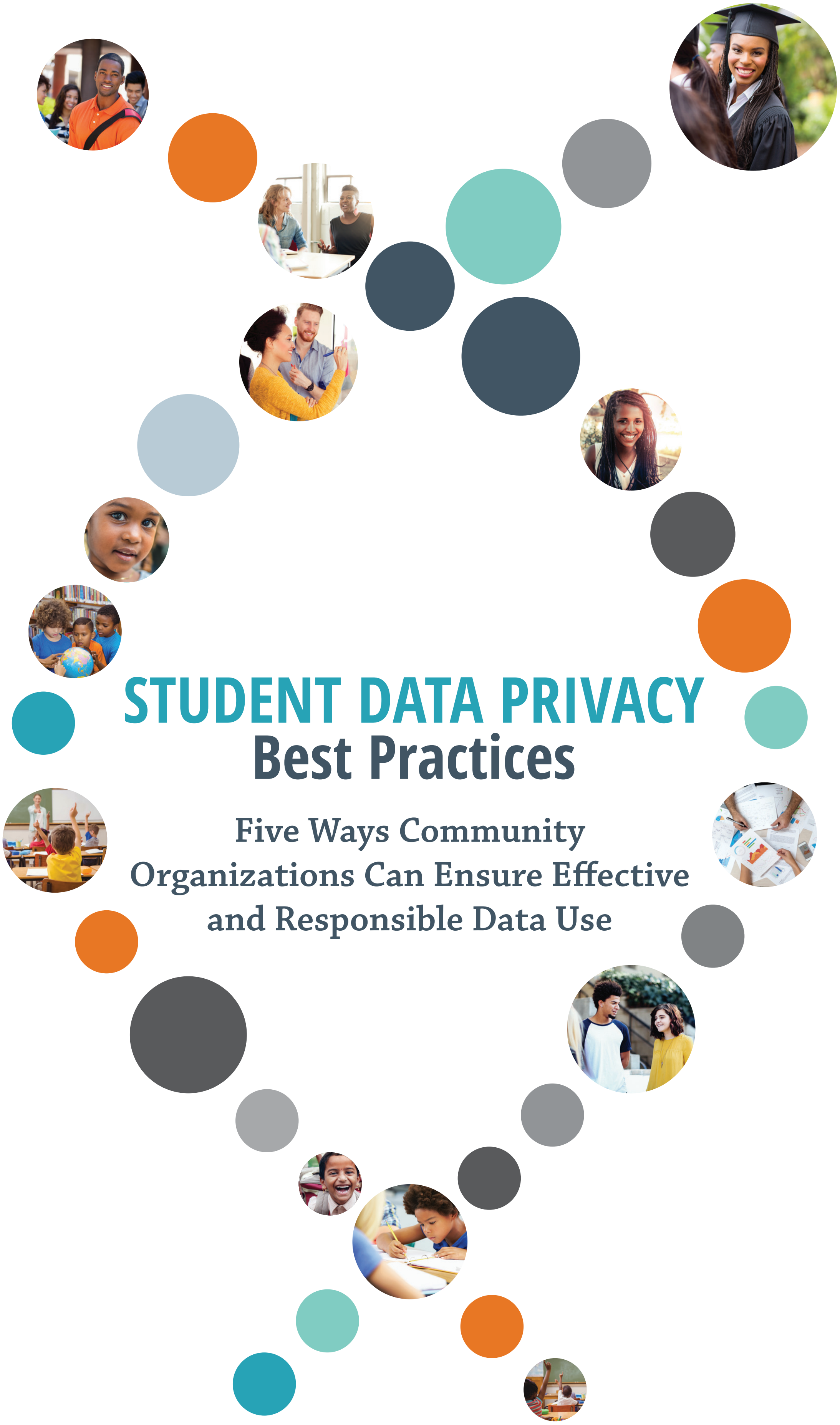
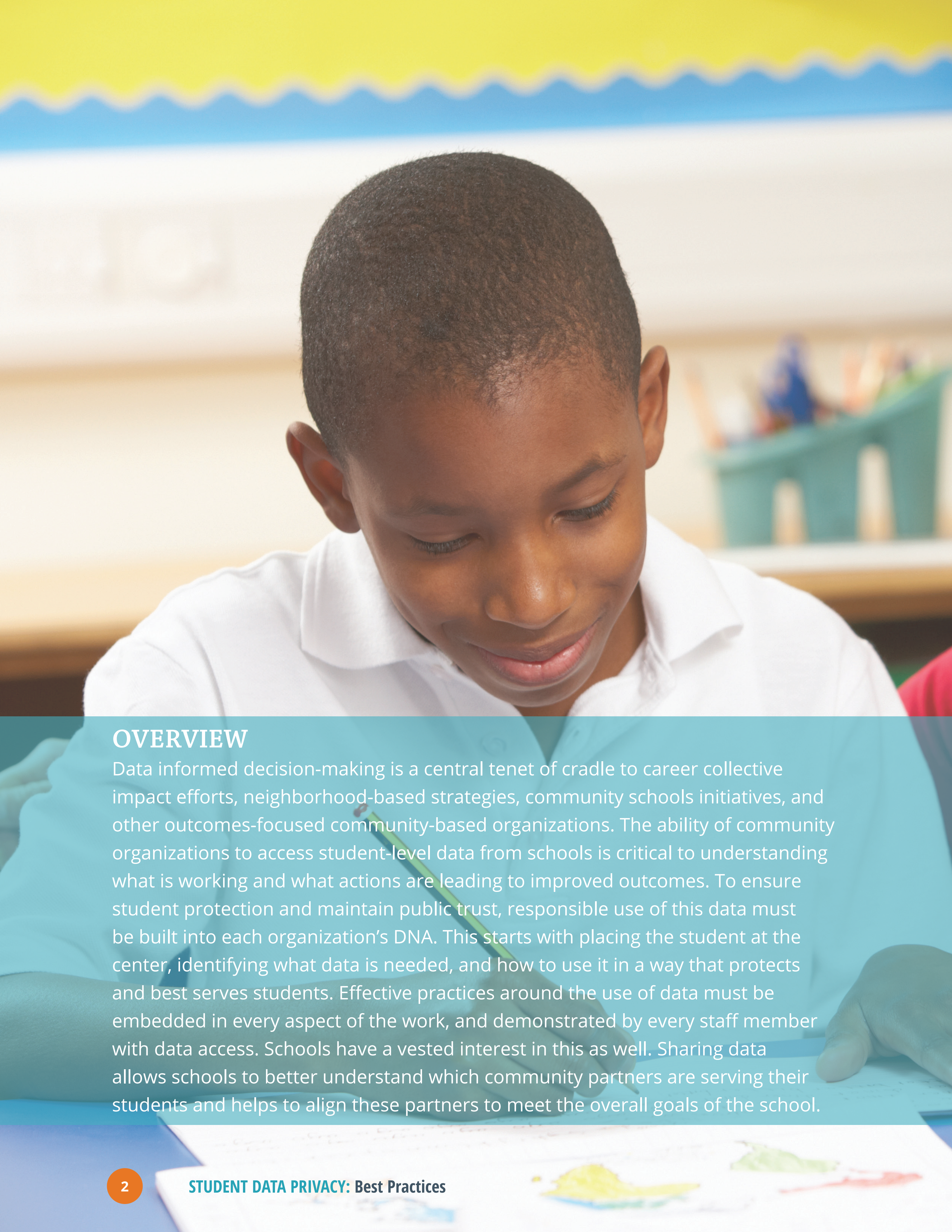


STUDENT DATA PRIVACY
Best Practices

Five Ways Community Organizations Can Ensure Effective and Responsible Data Use

StriveTogether

Every child. Cradle to career.



OVERVIEW

Data informed decision-making is a central tenet of cradle to career collective impact efforts, neighborhood-based strategies, community schools initiatives, and other outcomes-focused community-based organizations. The ability of community organizations to access student-level data from schools is critical to understanding what is working and what actions are leading to improved outcomes. To ensure student protection and maintain public trust, responsible use of this data must be built into each organization's DNA. This starts with placing the student at the center, identifying what data is needed, and how to use it in a way that protects and best serves students. Effective practices around the use of data must be embedded in every aspect of the work, and demonstrated by every staff member with data access. Schools have a vested interest in this as well. Sharing data allows schools to better understand which community partners are serving their students and helps to align these partners to meet the overall goals of the school.

In August 2014, StriveTogether convened a national task force to focus on effective practices of data protection and use. The task force consisted of local community practitioners and national experts in the areas of data use, school-community partnerships, student privacy, and data security. The charge to this task force was to recommend a core set of practices related to data sharing across systems. These recommendations would specifically address the practices of community-based organizations—including cradle to career collective impact initiatives, place-based initiatives, and community schools initiatives—that have access to personally identifiable information about students in the schools and districts in which they work.

The primary goal of this document is to provide general guidance to enable cradle to career partnerships and community-based organizations to learn, employ, and demonstrate best practices to protect student privacy. The scope of these practices applies to any community-based organization that is accessing personally identifiable information (PII) about students. PII refers to information that can be used on its own or with any other information to identify an individual.

The secondary goal of this document is to establish the guidelines that can inform further work to better simplify and organize the privacy ecosystem to be more efficient, equitable and accessible. These guidelines can also be used to provide broad specifications for developers and funders of technology solutions aimed at creating more secure and seamless student data privacy and sharing solutions.

An initial set of practices began with practitioner input. These practices were vetted and developed further by members of the task force and can be summarized under five primary topic areas:

1. Foster a culture for using data,
2. Fully integrate all privacy regulations into your practices,
3. Develop policies to share and protect data,
4. Employ strong data security strategies, and
5. Be transparent about why and how you use data.

Before diving into the practices, there is a set of overarching principles that guide this work.

GUIDING PRINCIPLES OF DATA USE

While the practices outlined on the following pages are mostly tangible actions that can be taken in using and protecting student data, there is a set of overarching principles we can use to guide the work.

- **Shared responsibility.** Everyone in the community has a stake in student success. Students, parents and guardians, school officials, community organizations, government organizations, businesses, and policymakers are all responsible for how every child is doing right now and for achieving better, more equitable results in the future. Access to individual-level information on students by those working with them is critical to enable personalized learning.
- **Data as a flashlight.** With the appropriate consent and safeguards, individual student information—used together with observations and expertise from parents and guardians, community organizations, and students—helps every student to start kindergarten ready to learn, excel in their education, graduate high school ready for college or career, and complete some form of postsecondary education that leads to a meaningful career. Data use for program evaluation helps us understand what is working and what needs to be improved.
- **Data for learning and continuous improvement.** Accountability is important and data is critical for that purpose, but we value the use of data as a tool for learning and continuous improvement, as well. This means that data is used to inform decisions on a consistent basis, and to measure how effective those changes were to improve student outcomes.

- **Student privacy at the forefront.** Our use of any student data includes an assurance that data is protected. This means that laws like FERPA describe the absolute minimum requirements for ensuring privacy; we will seek to further protect student privacy whenever we can. At the same time, any systems used to interact with the data must be highly secure and redundantly protected from breach or loss.

- **Share data only when necessary.** Sometimes large swaths of data are shared because of technical or practical limitations. There should be a valid, reviewed, and approved reason for all pieces of data. This principle carries to partners and vendors, as well; just because we legally can share large amounts of data, we should not do so unless for a specific educational purpose.

- **Transparency of data use and practice.** We believe in being clear about what student information we are collecting, who it is being shared with and for what reasons, and how it is being protected. It should also be easy for parents or students to find out what data is being collected, stored, and shared.

DATA PROTECTION & USE

EFFECTIVE PRACTICES FOR COMMUNITY-BASED ORGANIZATIONS

This paper is written for professionals in community-based organizations who are working with or seeking to work with schools to access or share data on the students they are serving. It is also aimed at policymakers and funders who have a role in enabling effective and responsible data use. Ultimately, leaders drive this work, and it is incumbent upon leaders across multiple organizations and at all levels to make it happen.

What follows is intended to be a high level set of practices that organizations can use as a checklist when setting about this work. We hope it will also raise the level of awareness and conversation about the use of data in communities and what measures need to be taken to safeguard this data. This paper is intended to provide general guidance. It is not legal advice, and it should not be treated as such.

The majority of the practices below apply to all organizations working with student-level data. In addition, some practices apply specifically to organizations with a technology infrastructure or those working with vendors:

🛢 **Practices that apply specifically to organizations with a more robust technology infrastructure, including servers and a managed network environment.**

🌐 **Practices for organizations that are working with external providers where data is hosted offsite (i.e. data warehouse vendors and nonprofit performance management system vendors).**

1) Foster a culture for using data

Organizations execute effective practices in collecting, analyzing, and using data.

1. **Appropriate data use:** Staff within organizations should be able to explicitly state how data can be used within the context of local data sharing agreements and be prepared to communicate those parameters of data use with all parents, students, and community stakeholders.

2. **Data collection, interpretation, and analysis:**
   - Datasets released by the school districts should be as complete as possible, reflecting the entirety of what is recorded about a particular subject.
   - Work with data owners to understand the nature and limitations of the data you collect and time periods it is collected (i.e. absence data and calculation of attendance rate, medical compliance data with a cutoff date for collecting the data). Include data dictionaries when available.
   - Results should not exploit inappropriate forms of analysis or rely on statistical anomalies to produce a desired result.

- Be aware of data suppression guidelines for the data you are working with, ensuring that PII data isn't inadvertently disclosed.

3. **Communication and dissemination:**
   - Disclose the data source and the variables being compared; offer context for interpreting results.
   - Communicate results of analysis to data providers first, helping to ensure data quality and maintain trust.
   - Data should always be interpreted in the context of existing community partners and networks who are working together to advance common goals.
   - Credit those who provide the data as well as the efforts of collaborative partners in collecting or maintaining the data.

4. **Families are central:** Families play a central role when it comes to collecting and sharing data, especially in working with the population of younger children. Provide families opportunities to contribute information that goes beyond test results, including information on student interests, goals, accomplishments, and learning that happens out of school.

5. **Designate an intermediary:** Where multiple organizations in a community are seeking to access data from schools, designate an intermediary to play a coordinating role and help to streamline processes and requests.

6. **Regular review:** Staff using data stay up–to-date with privacy issues and best practices, both locally and across the nation (i.e. attend webinars and workshops hosted by Dept. of Education's Privacy Technical Assistance Center (PTAC) and the Data Quality Campaign; monitor news and social media for awareness of emerging trends; and host local conversations to continuously improve local practice).

7. **Training and support for community partners:** Require initial and ongoing training and technical support for local community organizations on the best practices of collecting, interpreting, and using available data for the purpose of student success.

8. **Develop a learning culture:** Communicate results to relevant stakeholders and foster trust building based on the insights. Involve district and organizational leadership in conversations early in developing effective questions throughout the process of analysis.

2) Fully integrate all privacy regulations into your practices

Organizations understand and abide by all applicable student and child privacy laws.

1. **Family Educational Rights and Privacy Act (FERPA):**
   - FERPA sets the minimum standard for the protection of student records; organizations should strive to provide protections beyond those required by FERPA and other federal/state laws.
   - Identify clearly the authority under FERPA that allows the sharing of data and work with your local district(s) to determine the appropriate exemption. The most common FERPA exemptions for community-based organizations include: Written consent, de-identified data, research studies, audit/evaluation, and contractor/agent of the district. Examples can be found in the StriveTogether/DQC Data Sharing Playbook.
   - Understand what "FERPA Compliant" means for a vendor. Ask questions to understand how vendors protect data consistent with one the appropriate FERPA exceptions for your situation.

2. **Health Insurance Portability and Accountability Act (HIPAA):** Organizations have an understanding of HIPAA and how it relates to FERPA and education records. A school is subject to HIPAA only if it provides medical care and electronically transmits health information as part of a "covered transaction" (e.g., billing). Additional guidance is available through the U.S. Department of Education and the Guidance Document for Promise Neighborhoods.

3. **Children's Online Privacy Protection Act (COPPA):** Organizations have an understanding of COPPA and how it relates to FERPA and education records. The primary goal of COPPA is to place parents in control over what information is collected from their young children online. It applies to children under age 13.

4. **Understand and follow all regulations:** Be well informed about what is allowable by all applicable laws, including federal, state, and local. Work with legal experts (within the school district or community) to build or buy the capacity to understand and abide by the laws.

3) Develop policies to share and protect data

Organizations establish policies including processes and procedures to share and protect data.

1. **Data-sharing agreements (DSAs): Best practices regarding DSAs will be followed. Best practices include:**
   - Clearly stated purpose of the sharing of data
   - Signature from the owners of the data
   - Explanation of limited data use to the specific educational purpose
   - Explanation of how to enable the sharing of PII only with people who have legitimate interest in supporting that purpose and no other purpose
   - Retention and destruction clause that limit the retention of student data beyond the required period of use, and requires destruction of those data at that point
   - "Project authorization" forms for each project, identifying the specific variables, years, level of observation, and files names if known
   - Explanation about the frequency of data updates, in the cases where the same data will be needed to be updated on an ongoing basis
   - Statement that the receiving organization will not enter into a third-party data sharing agreement, unless explicitly stated and the third party is identified and held to the stated educational purpose
   - Disclosure and dissemination rules that identify what happens to derivative products of the covered data sets (what is learned from the data). Provide data analyses and learnings back to the school district, unless agreed to otherwise

- Clear legal ramifications outlined if data users do not comply with terms of data sharing agreements, including possible financial penalties and legal action
- A period of agreement and a process to amend the agreement. Ideally an agreement would be in effect for the duration of the initiative or until terminated by either party

2. **Written consent:** Where written parent/guardian consent governs the sharing of data, the process of obtaining consent is owned by the school district, but often managed by districts and community-based organizations together. Data custodians in community organizations will work with districts to develop processes, procedures, and documents for securing written consent as needed. Where possible, data systems will accommodate parent consents.

3. **Staff Confidentiality or Acceptable Use Agreements:** Will be signed by all who have access to the PII that is in the organizations control, identifying appropriate uses and standards of conduct.

4. **Privacy provisions in contracts:** All contracts with vendors who will create or provide data services are expected to contain privacy provisions that ensure students' data is used for educational purposes only, ensure students' personal information is not used to target advertising to students or families, and ensure that data security, retention, and destruction policies are in place. 🌐

5. **Data security plan:** Have a data security plan that would cover administrative, technical and physical security of the data and its transfer as described in the next section.

6. **Data communications response plan:** Establish a response team and create a security response plan document for addressing security breaches or other issues arising from disclosure of data.

7. **Designate a "chief data officer":** The leader of the organization should identify a staff person to be designated as the chief data custodian. This person is responsible for the management and delivery of data throughout the organization. This person should also:
   - Maintain a log of all current data sharing agreements,
   - Maintain a list of the individuals who have access to PII internally, including who has access to the physical servers, if applicable,
   - Maintain a log of external people who are given PII (e.g., contractors performing analyses as allowed in the DSA),
   - Ensure that individuals who have access to PII have adequate training on secure data transmission methods and all related data protection policies and effective practices,
   - Maintain high-quality documentation to ensure that the technology and processes related to the data collection process are functioning properly, especially as changes are made over time to improve it,
   - Be a public facing figure who members of the public can contact with data use/privacy questions and concerns.

4) Employ strong data security strategies

Organizations employ strong administrative, technical, and physical data security strategies to guard against breaches and unauthorized use.

Administrative Security—*practices for controlling who can access data and how*

1. **Limited user access:** Limit access to the data using the least-privilege principle (limiting access to the minimum level that will allow normal functioning). Develop role based permissions where applicable. Review the user list and permissions on a periodic basis.
2. **Account/password management:** User accounts need to be kept up to date, and accounts no longer in use are to be disabled or deleted. Good practice is to require strong/complex passwords and regular changing of passwords. 🛢 🌐
3. **Identification and access management:** Unless technically impractical, data systems will use single sign-on (SSO) so that users do not have to create a separate user account. 🛢 🌐
4. **Two factor authentication:** Unless technically impractical, data systems will also employ multi-factor authentication for certain roles, providing an extra layer of user security. 🛢 🌐
5. **Audit trails and logging:** All user activity is logged and auditable to see who took what action on what data. Additionally, an auditable log of data received, as well as when and how the data were received, must be maintained. 🛢 🌐

Technical Security—*practices for protecting the files and records stored inside your computer(s)*

1. **Encryption**
   - For data in motion: All data is encrypted and transmitted over secure connections (physical media, encrypted electronic mail, or secure ftp).
   - For data at rest: Data is encrypted when sitting at rest, even for a short period of time (full disk encryption or individual file encryption is built into most operating systems and document repositories).
2. **Limited network access:** Connections to and from data systems will only be allowed from trusted servers, controlled by firewalls and/or network address filtering. 🛢 🌐
3. **Patch management:** Ensure all systems are kept up to date with system updates, patches, and security hotfixes. A procedure for regular patch management should be established and automated with a patch management deployment tool.
4. **Anti-virus management:** All systems, including local, end user, or hosted with a vendor, should be running anti-virus software, updated daily for new virus definitions, and systems should be scanned regularly.

Physical Security—*practices for protecting the physical machines that hold records*

1. **Secure hosting and infrastructure:** All data components will operate either in organization control or in highly secure cloud infrastructure. Cloud providers are expected to comply with FedRAMP requirements (a federal certification for cloud services used by government agencies). Cloud providers should provide documentation that outlines their security management processes, intrusion detection methods, physical security controls, and regulatory compliance certifications. 🛢 🌐
2. **Local machines:** Data is not stored on local workstations when possible, only on a secured machine designated for that purpose. Any machine accessing data by network or otherwise should employ full-disk encryption. 🛢

3. **Physical media:** Media (servers, hard drives, CDs, DVD's, etc.) containing PII must be physically protected (e.g., locked in a secure server cabinet and periodically checked) and wiped clean or destroyed as soon as not needed.

Overall Security

1. **Designate a "chief security officer":** Identify a staff person responsible for directing the information security policies that are meant to protect organizational assets from internal as well as external threats, from employees and vendors to cyber criminals and hackers.
2. **Purchase cyber liability insurance coverage as an added protection and require it of any vendors you may be working with.**
3. **Security audits:**
   - Permit security audits to be conducted by districts and schools if desired, granting the right to audit or conduct other monitoring activities of the organization's policies, procedures, and systems with regard to the use of PII.
   - Contract with a security firm or government agency to conduct a security audit and penetration testing of all data transfer system components.
   - Ask vendors if they have completed security audits.

5) Be transparent about why and how you use data

Organizations are transparent about their data sharing practices and use.

1. **Communication before delivery:** Publish as much information about intents and practices on organizations' web sites to clearly articulate goals and objectives. This kind of transparency allows for dialogue and learning throughout the process:
   - What information is collected
   - Why it is collected
   - How it is used
   - With whom it is disclosed

2. **Iterative building approach:** Foster an iterative building approach, allowing for adaption to changing needs as the systems and staff structures are built. As privacy standards and security concerns are discussed and improved, systems can adapt quickly and improve.

3. **Develop a learning culture:** Communicate results to relevant stakeholders on an ongoing basis to help build trust throughout the learning. Data sharing isn't the destination; it's a journey.

RELATED RESOURCES

- U.S. Dept. of Ed. Privacy Technical Assistance Center (PTAC)
- StriveTogether/Data Quality Campaign—Data Drives School-Community Collaboration: 7 Principles for Effective Data Sharing
- FERPA|SHERPA: A one-stop shop for service providers, parents, school officials, and policy makers to guide responsible uses of student data
- Measuring Performance: A Guidance Document for Promise Neighborhoods on Collecting Data and Reporting Results
- National Neighborhood Indicators Partnership: Lessons on Local Data Sharing and Key Elements of Data Sharing Agreements
- Coalition for Community Schools: Evaluation Toolkit
- SIF Association—Data Privacy, Security and Interoperability
- Center for Technology in Government, University at Albany
- Common Sense Media School Privacy Zone
- Afterschool Alliance—Afterschool Programs Using Data to Better Serve Students
- Wallace Foundation—Data Sharing Strategies that Work
- Resilient Networks and NLET—A Trust Network to Support Children
- CoSN: Protecting Privacy in Connected Learning, including a Toolkit, and Infographic

TASK FORCE MEMBERS

Erica Bernabei, Promise Neighborhoods Institute, Washington, D.C.
Matt Deevers, Summit Education Initiative, Akron, Ohio
John Dicello, Chicago Public Schools, Chicago, Illinois
Gordon Freedman, National Laboratory for Education Transformation, Santa Clara, California
Larry Fruth, Schools Interoperability Framework (SIF) Association, Washington, DC.
Kacey Guin, Seeding Success Partnership, Memphis, Tennessee
Matt Harris, Puget Sound Educational Service District, Seattle, Washington
Josh Hawley, Ohio Education Research Center, Columbus, Ohio
Leah Hendey, Urban Institute, Washington, D.C.
Reuben Jacobson, Coalition for Community Schools, Washington, D.C.
Chris Kingsley, Data Quality Campaign, Washington, D.C.
Marcy Lauck, National Laboratory for Education Transformation, Santa Clara, California
Lisa Neilson, Ohio Education Research Center, Columbus, Ohio
Theresa Pardo, Center for Technology in Government, University at Albany, New York
Danya Pastuszek, Promise Partnerships of Salt Lake, Salt Lake City, Utah
Michael Robbins, Span Learning, Washington, D.C.
Mary Jean Ryan, Community Center for Education Results, Seattle, Washington
Andrew Sahalie, Community Center for Education Results, Seattle, Washington
Greg Wong, Pacifica Law Group, Seattle, Washington
Geoff Zimmerman, StriveTogether Staff, Cincinnati, Ohio

StriveTogether
Every child. Cradle to career.

One West Fourth Street, Suite 200
Cincinnati, OH 45202

513.929.1150

@strivetogether

www.strivetogether.org

ABOUT STRIVETOGETHER

StriveTogether is a national, nonprofit network of 70 communities that supports the success of every child, cradle to career. We provide coaching, connections and resources to local partnerships and work together to accelerate progress in education. Communities using our approach have seen dramatic improvements in kindergarten readiness, academic achievement and postsecondary success. The Cradle to Career Network reaches 8 million students, involves more than 10,200 organizations and operates in 30 states and Washington, D.C.