

Data Use in the Promise Partnerships – A Resource for Parents, Students, and Community Members

Page 1 – The Role of Data: Our Guiding Principles

- **Data as a flashlight.** Promise Partnership organizations believe that, with written consent from parents and guardians and protections like the ones described below, individual-level student information – combined with 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, and complete a degree or credential that leads to financial stability.
- **Shared accountability.** We believe that everyone in the community contributes to student success. Students, parents and guardians, school officials, community organizations, government organizations, businesses, and policymakers are all responsible for how every child is doing today and for achieving better, more equal results in the future. We believe that everyone involved in our children’s education should work together and have access to individual-level student information for the students that they support. We believe student information is **never** evidence of the success or failure of any one program, organization, sector, or group of people.
- **Ongoing professional development.** We believe students do best when they are surrounded by professionals in schools and in the community who are trained to use student information to help students succeed. We believe that we all need ongoing support on how to effectively use student information, and we are committed to providing that support.
- **Transparency.** 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. Click here for information on what information we are collecting, who is seeing it, and for what reasons ([link to page 2](#))

Page 2 – Helping Students through Data Sharing

We developed this webpage so to make it clear what information we are collecting, who is seeing it, and for what reasons. Please call United Way of Salt Lake at 801.736.7702 or email us at helpdesk@uw.org with questions or comments. Please include your contact information, so that we can respond.

Why are the Promise Partnerships collecting individual-level information, and what are they doing with it?

Individual-level student information is ONLY shared with a partner in a Promise Partnership if (1) a parent or guardian has given written consent to share information; (2) the partner has signed data confidentiality agreements and has received specific training; (3) the partner works in the student’s

community; (4) and the partner “needs to know” the information, because knowing it will help them support the student’s academic success.

When these conditions exist, here are some ways the Promise Partnerships use individual-level information:

- Before a partner works with a student, they use student information to set goals and plan programming that will address the student’s strengths and needs.
- While a partner works with a student, they use timely and quality student information to see how the particular student is doing. If a student is struggling in algebra, or not attending history class regularly, the information helps the partner work with parents and guardians and the student, so that the student does not get off track.
- Partners that have access to information meet with one another and with school officials to review information, collaborate, talk about what is working well, and make improvements to their work. Student information helps these partnerships support students, parents and guardians, and each other, and to understand which programs benefit students (and which ones need to be adjusted).

Partners are authorized to use information ONLY to promote students' educational success.

What information do Promise Partners share?

We only share information that promotes students’ academic success. Below are the specific data elements that we share.

Data Element	Purpose
<i>Shared from a student’s educational record that is maintained by their school</i>	
Student ID, student home address, and student date of birth	Helps us with data quality, by reducing duplicate records and allowing a student’s information to be easily tracked from school to school.
Race, Ethnicity, Gender, English Language Learner Status, Refugee Status, Primary Language, Country of Origin, and Free or Reduced Price Lunch Status	Helps us understand how to work most effectively with students. Helps us do analyses to address differences in student outcomes based on demographic categories.
Current and past educational institutions and current grade in school	Allows us to restrict access to student information so that only partners with a “need to know” get access to records. Helps us understand the programs and strategies that a student has had access to.
Credits earned and credits possible for current grading period; courses taken and grades achieved for current and past terms and grading periods; CPA and GPA; days absent and reasons for absences; attendance rate and absence category; state and district mandated tests taken and	Helps us understand how a particular student is doing and has done previously, so that targeted plans can be designed to help them improve. Allows us to connect students to specific interventions to support their strengths and challenges.

scores	
<i>Shared from community organizations</i>	
Information (i.e. dates of enrollment, contact with volunteers, dates of attendance and absence) about organizations and programs that a student attends during and outside of school time	Helps us understand which strategies are helping which students to be successful.

Who are you sharing it with and how are they using it?

We share information with community organizations, government organizations, and health care providers that work in our community (“partners”). Some of these partners provide programs before and after school and over the summer to reinforce what’s being taught in school. Others provide tutoring and mentoring, both during and outside of the school day. Others provide support to parents, guardians and families with skills classes, employment services, financial planning, housing, and other needs.

All of these partners have committed to protect information and work collaboratively with each other. For a full list of the partners that have access to information please visit www.uw.org/wherewework. The interactive map will take you to the partners in each Community School that we support.

Where are you sharing student information?

There are two main ways.

UWSL, as a coordinator and support of Promise Partners, purchased a cloud-based data management system (ClientTrack) that offers state-of-the-art security. Partners who have reviewed and signed certain data confidentiality agreements, received data security training, work in the student’s community, and have an appropriate “need to know” role, share individual-level student information through this secure system.

Also, partners share this information through carefully facilitated, closed-door meetings designed to create plans for individual students, and to understand which programs directly benefit students and which ones need to be adjusted.

How are you protecting it from breaches and unauthorized use?

We only collect student data when parents or guardians give written consent, the information is used to support student academic success, and the information is kept secure. Here are just some of the policies and practices we have in place to protect information. Please see our Contract, Data Privacy Terms and Conditions, and Data Sharing Terms and Conditions for a complete list ([link](#)).

Administrative and Technical Security Mechanisms

Practices related to the transmission of data and who has access to information

- **Single point of access** – Electronic information is only shared among partners through ClientTrack, our secure online data management system. *No student-level information may be downloaded from ClientTrack onto any physical hard drive.*

- **Limited user access** – UWSL staff limit access to information, giving users access to the minimum level of information that will allow normal functioning.
- **Patch management** – UWSL and ClientTrack staff ensure that all systems are current with system updates, patches, and security hotfixes.
- **Anti-virus management** – UWSL and ClientTrack staff run anti-virus software, are updated daily for new virus definitions, and are scanned regularly.
- **Account/password management** – UWSL staff keep active accounts up to date, and deletes or disables accounts that are no longer in use. ClientTrack users chose a strong password, change it every six months or in the event that the password is compromised, and lock their computer or sign out of the system when they leave. UWSL staff configure ClientTrack so that an inactive user is logged out after 15 minutes.
- **Identification and access management** – ClientTrack uses a single sign-on (SSO) technique so that users do not have to create a separate user account.
- **Audit trails and logging** – All activity is logged and auditable to understand which users take what action on what data. UWSL staff maintain an auditable log of individual-level information received and when.
- **Security audits**. ClientTrack contracts with a security firm to conduct a security audit and penetration testing of all data transfer system components and provides UWSL upon request with information as to when they completed security audits.
- **Encryption**. UWSL staff accept individual-level information only through a secure file transfer system that encrypts data prior to transmitting it. The ClientTrack software solution includes multiple technical safeguards designed to ensure that information is maintained and transmitted securely such as 128 bit encryption during transit, data hashing, and 256 bit encryption for data at rest.

Technical Security Mechanisms to Guard Against Breaches and Unauthorized Use

Practices related to the storage of data

- **Secure hosting and infrastructure** - ClientTrack complies with federal FedRAMP requirements (a federal certification for cloud services used by government agencies that indicates that data components are operating in a highly secure cloud infrastructure). ClientTrack maintains documentation that outlines its security management processes, intrusion detection methods, physical security controls, and regulatory compliance certifications.
- **Local machines** – UWSL and ClientTrack do not store individual-level information on local workstations when possible. All UWSL machines employ full-disk encryption.
- **Physical media** – UWSL requires that partners physically protect (i.e. lock in a secure cabinet) physical media (servers, hard drives, CDs, etc.) containing individual-level information and destroy it as soon as it is not needed. Any documents that include student data must be kept in secure and locked places.

Regulation and practices

Practices related to understanding and abiding by application privacy laws

- **FERPA and written consent** -- The collection, use, and sharing of information must comply with federal and state laws. These include the Family Educational Rights and Privacy Act (FERPA), a federal law designed to protect the confidential information of individuals related to education and the Health Insurance Portability and Accountability Act of 1996

(HIPPA), a federal law designed to protect the confidential information of individuals related to their medical care and history. No student-level information may be shared among partners, verbally or electronically, without appropriate written consent from a parent or guardian.

- **Training and agreements for users and staff** – Data entry into the online data management system may only be done by trained and certified users who have signed Data Privacy/Sharing end user agreements. Each ClientTrack employee and each UWSL employee with access to individual-level student information is required to sign and comply with Data Privacy/Sharing Policies and to participate in regular privacy trainings as a condition for employment.
- Information about students may be discussed only in discreet locations where other students cannot hear.
- Paper and digital records are destroyed once the student is no longer receiving services within a Promise Partnership. (We do maintain, as allowable by law, information that lets us do historical analyses.)

Any suspected violations of these security practices are brought to the Governance Committee of the UWSL Board of Directors.

What is a FERPA Waiver?

Students at UWSL Community Schools receive – with education – opportunities for health care, afterschool, tutoring, mentoring, English and citizenship classes, and other services. If the organizations offering these services can share select information about individual students, they can better support students academically and connect them to resources. A federal law called the Family Educational Rights and Privacy Act (FERPA) protects our students' educational information. It says that, if a parent or guardian gives written permission, organizations that help their students can share select educational information. By choosing to sign a FERPA Waiver ([FERPA Waiver link](#)), a parent or guardian allows information about his or her child's demographics, grades, enrollments, credit hours, GPA, attendance, and test scores to be shared with the community partners that work – at the request of the principal – in their school. The parent or guardian also allows information collected by community partners to be shared back with the school and with other partners. Student information is only used to help the student succeed in school and is not shared with anyone outside of our partnerships. The students of parents or guardians who choose not to sign a FERPA waiver can still receive services, and signature in no way affects any kind of immigration status.

When and how is physical and electronic information destroyed?

If a student's parent or guardian (or the student themselves, if he or she is over the age of 18) revokes in writing their consent to share information, UWSL will alter relevant data fields in ClientTrack, so that the student's identity is hidden. Please note that physical student information often exists in many places and that UWSL can only remove information from ClientTrack. To remove a student's information from other locations (such as a school record), a parent or guardian must contact the organization that holds the information.

Partners also shred (or place in a secure shred bin) physical student information that is no longer needed.

Who should I contact if I have questions?

We review questions and input regularly and thoughtfully. Please call United Way of Salt Lake at 801.736.7717 or email us at helpdesk@uw.org. Please provide your contact information, so that we can respond meaningfully and quickly to your comment.

Useful Documents

UWSL – with input from parents and guardians, school officials, legal counsel, national data privacy groups, and community partners – has created the following documents to explain and support the data sharing practices above.

FERPA Waiver

- Sample FERPA Waiver in Arabic, English, Burmese, Karen, Nepali, Somali, and Spanish (FERPA Waiver links)
- FERPA Video –
 - o https://www.youtube.com/watch?v=MRC1WHdZqog&list=PLlcpX_oDu_ySDOYQdAovTW4hIECwa6pN (English)
 - o https://www.youtube.com/watch?v=iQcRocSCZDI&list=PLlcpX_oDu_ySDOYQdAovTW4hIECwa6pN (Spanish)

ClientTrack

- ClientTrack Privacy Posting in Arabic, English, Burmese, French, Karen, Somali, Spanish, Swahili, Nepali, and Persian (links)
- ClientTrack End User Agreement (link)

Contractual Documents

- UWSL Contract, Data Privacy Terms and Conditions, and Data Sharing Terms and Conditions (link)