Article 5: Data Privacy and Sharing

Section 5.1: Directory Information

Policy 515 provides information about Directory Information—information that is considered public unless a parent or eligible student asks for it to be "private." To require consent prior to disclosure of Directory Information, the parent or eligible must submit a written request to the building principal within thirty days of the last publication of a notice given to parents. This written request must include the following information:

1. Name of student and parent, as appropriate
2. Home address
3. School presently attended by student
4. Parent's legal relationship to student, if applicable
5. Specific category or categories of Directory Information which is not to be made public without the parent's or eligible student's prior written consent.

The building principal emails the request to the Student Services and Ed-Fi Coordinator who marks the data as private on the student's record in Synergy.

Section 5.2: Student Surveys Administered by the District

Policy 520 governs the administration of student surveys by the district.

Section 5.3: Student Surveys Administered by Other Students

Students are expected to obtain prior approval from their teacher before administering a survey to students for a classroom assignment, club activity, or other school-related purpose. The student sends a written copy of the proposed survey as well as a written plan detailing the purpose of the survey and explaining how results will be used to his/her teacher or advisor. Students are not allowed to ask for another student's name in the survey.

Section 5.4: Parent Surveys

Except for routine matters (such as signing up for parent-teacher conferences or determining which students might be interested in the Online-Only Option), employees are expected to obtain prior approval before administering a parent survey. The employee provides their supervising administrator with a pdf version of the proposed survey, including an introductory paragraph for parents explaining the survey's purpose and how results will be used.

Unless otherwise indicated in the written plan, gender, race, and free/reduced lunch status, will not be requested from parents or retrieved from the student management system. If the intent of the survey is to share results by gender, race, and/or free/reduced lunch status, the Superintendent may request review by the Legislative and Policy Committee. Survey data results may be subject to the Minnesota Data Practices Act.

Section 5.5: Educational Data Privacy Agreements

Educational data privacy agreements with community organizations are presented to the Legislative and Policy Committee for review and then the board for approval.

Section 5.6: Authorization to Release Student Information

Prior to releasing non-public data to a Representative or Organization, the district receives signed releases from parents or eligible students. Signed student releases will be maintained by the Representative or Organization, Every Hand Joined (if data is shared through Every Hand Joined's datamart), and the Student Services and Ed-Fi Coordinator (majohnson@rwps.org). The Student Services and Ed-Fi Coordinator will email the authorization form to the student's school secretary who will add the student to the appropriate group for the Individual or Representative and keep a copy in the student's cumulative file.

**Section 5.7: Data Privacy and Sharing with Non-School Entities**

Background Information

Every Hand Joined and i3Works provide data management and analysis services for the district including, but not limited to, the following:

1.   Every Hand Joined uploads aggregate data from the Minnesota Department of Education and the National Student Clearinghouse into Tableau Server, an online platform of data tables and visualizations.   Student-level data is not available from this aggregate data. The data mart provides reports based on aggregate data that are shared with the public.

2.   Community partners also use the data mart to access student-level data, but only if the district and the community partner have a board-approved Educational Data Privacy Agreement and a signed Authorization to Release Student Information for each student. By submitting an opt-out form, the district will not share student-level data with Every Hand Joined for use by community partners. Opt-in and opt-out processes are described below.

3.   Every Hand Joined and i3works also provide other data management and analysis services for the district. This work does not result in student-level data being shared with community partners through Every Hand Joined's data mart.

Data Flow:

Data is transferred from the district's student data management system into Every Hand Joined's data mart as shown in the graphic below. Student-level data is uploaded into the data mart only if there is a signed Authorization to Release Student Information and there is no opt-out form.
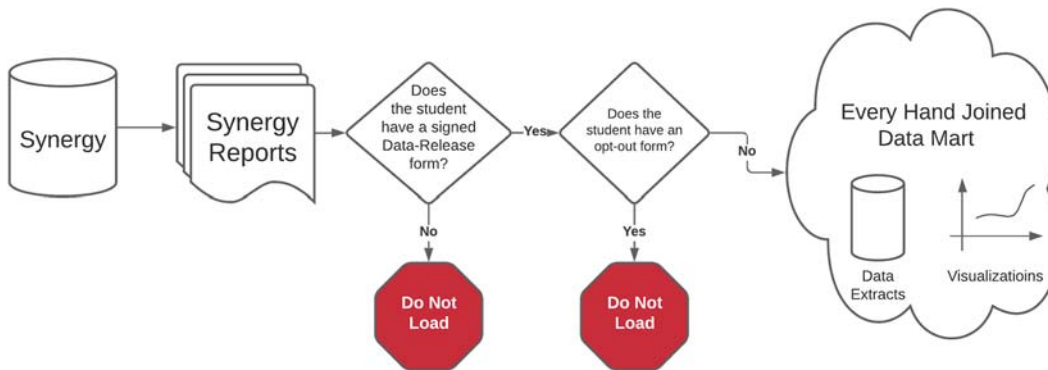
<u>Opt-Out of Data Sharing with Community Partners</u>

1.   Parents who wish to opt their children <u>out</u> of data sharing with a community partner through Every Hand Joined's data mart will noitify the Ed-Fi and Student Services Coordinator.

2.   The Ed-Fi and Student Services Coordinator adds the student(s) to the specific group in Synergy.

3.   Using a standard letter or email communication, the Ed-Fi and Student Services Coordinator notifies the parent that their student has been placed in a group that prevents their individual data from being shared with community partners through Every Hand Joined's data mart. The letter should also explain that data may still be shared with entities acting as school officials in accordance with Federal law.

4.   The student is automatically included in Synergy Report GRP401: Student Group List Report. GRP401 is used as a filter in the data upload process to the Every Hand Joined data mart.

<u>Opt-In Data Sharing with Community Partners:</u>

1.   Parents who wish to opt their children <u>in</u> the data sharing with a community partner through Every Hand Joined's data mart must submit an Authorization to Release Student Information to the authorized contact within the community partner.

2.   The authorized contact within the community partner ensures the form has been appropriately completed, signed and dated. The community partner maintains the original signed document.

3.   The authorized contact within the community partner scans and emails the completed form to the Ed-Fi and Student Services Coordinator (if the form is in English) or the Language Interpreter (if the form is not in English). The Interpreter attaches the English translation of the form and emails a scanned copy to the Ed-Fi and Student Services Coordinator.

4.   The Ed-Fi and Student Services Coordinator ensures the form has been appropriately completed, signed and dated. If there are issues with form completion, the Ed-Fi and Student Services Coordinator contacts the parent, Data Manager at Every Hand Joined, and authorized contact with the community partner to fully complete the form.

5.   The Ed-Fi and Student Services Coordinator adds the student with the Authorization to Release Student Information to the specific group in Synergy.

6.   The Ed-Fi and Student Services Coordinator notifies the parent with a standard letter or email that their student has been placed in a group that enables student-level data to be shared with the community partner.

7.   The Ed-Fi and Student Services Coordinator emails a scanned copy of the Authorization to Release Student Information to the appropriate building secretary so it can be added to the student's cumulative file.

8.   The Data Manager for Every Hand Joined ensures specific students were added to the appropriate Synergy group.

9.   If a School Board member is authorized to access student data because of his/her involvement with a community partner, roles should be kept separate—he/she can access data provided to the community partner for purposes of performing duties for the community partner, but should not use this as a way to gain information for use as a board member.

10.   System: The student is automatically included in Synergy Report GRP401: Student Group List Report. GRP401 is used as a filter in the data upload process to Every Hand Joined's data mart.

Section 5.8: Data Searches

The Superintendent, generally after consultation with the district's attorney, is authorized to conduct searches of school-owned technology devices as per board policy. If the search involves the Superintendent, authorization must come from the district's attorney. The following procedures are followed when data searches of employee technology are conducted:

1.   Requests are made to the Information Technology (IT) Systems Administrator unless the data search involves him/her or other arrangements are made with the district's attorney.

2.   The Information Technology Systems Administrator pulls log reports from system logs applicable to the investigation (for example, web filtering).

3.   If the investigation requires access to the actual computer, the technology department goes onsite, connects remotely, or takes the computer to the technology office depending on the circumstances.

4.   If the search involves potential illegal activity or otherwise controversial content, the technology department makes a copy of the drive to investigate to make sure the integrity of the original drive is kept intact.

5.   Two staff members are typically part of the investigation to ensure integrity of the process if ever called to testify in court.

6.   All findings are submitted to the Superintendent or district attorney for review. Typically, the technology department stores the computer, if seized, in a locked area until further notice.

7.   The technology department documents its work and findings as appropriate.