Data Sharing Agreement: Community College District 512 & School Districts

DATA SHARING AGREEMENT

Between

Harper College District 512

And

TWP HS District 211

TWP HS District 214

Community Unit School District 220

This Data Sharing Agreement is intended to cover circumstances in which the above-named districts need access to data that contains personally identifiable information (social security numbers, names, etc.) belonging to current and former students. These circumstances include the following purposes intended to improve educational opportunities for the residents of these districts:

1. **Increase collaboration between secondary and post secondary systems;**
2. **Reduce the need for College remediation;**
3. **Promote greater awareness of post secondary educational options including financial aid and academic resources;**
4. **Create seamless transition systems from secondary education to postsecondary education;**
5. **Ensure that individuals who are members of special populations have the opportunity to access and succeed;**
6. **Develop career pathways that contain multiple entry and exit points to facilitate student success and lifelong learning;**
7. **Increase curricular alignment and reduce curricular duplication;**
8. **Support the development of integrated and applied curricular content;**
9. **Increase the opportunities for students to earn college credit while enrolled in high school;**
10. **Increase the opportunities for students to obtain marketable postsecondary certificates or degrees that support their career goals;**
11. **Create professional development programs designed to simultaneously engage and support secondary and postsecondary partners;**
12. **Utilize data for program improvement.**

1.0 Period of Agreement

The period of this Agreement shall be in effect from September 2010 until terminated in writing by a partner organization.

2.0 Constraints on Use of Data

Data supplied by the parties to this Agreement or collected by on behalf of the parties' students, prospective students, employees or alumni is the property of the parties to this Agreement and shall not be shared with third parties without the written permission of the parties to this Agreement. Data shall not be sold or used, internally or externally, for any purpose not directly related to the scope of work defined in this Agreement without the written permission of the parties to this Agreement.

3.0 Data Security

The parties to this Agreement shall employ industry best practices, both technically and procedurally, to protect the data from unauthorized physical and electronic access. Methods employed are subject to annual review and approval by the parties to this Agreement.

3.1.1 Data Elements

Data shared shall be limited to the data elements specifically defined and authorized by the parties to this Agreement. If one or more of the parties wishes to collect additional data, they must submit a request in writing to the other parties. Under no circumstances shall any of the parties collect any information classified as Sensitive or Confidential without the express written approval of the parties to this Agreement.

3.2 Data Categories

The following definitions shall be used to classify data for security purposes:

Normal: The least restrictive class of data. Although it must be protected from unauthorized disclosure and/or modification, it is often public information or generally releasable under procedures of for processing public records requests. Examples of this class of data are: class schedules, course catalogs, general ledger data, and employee demographic statistics.

Sensitive: This class includes data for which specific protections are required by law or for which agencies are obligated to prevent identity theft or similar crimes or abuses. Examples of this class of data are: peoples' names in combination with any of the following: driver's license numbers, birth date, student ID number (SID), address, e-mail addresses, telephone numbers. Also included are: agency source code or object code, agency security data, education records including papers, grades, and test results, or information identifiable to an individual that relates to any of these types of information.

Confidential: Access to these elements are tightly controlled and audited. Examples of these data are: Social Security Numbers (SSN), financial profiles, medical data, and disciplinary records.

3.3 Data Handling Requirements

Data handling requirements may vary depending on the classification of data shared with each of the parties. However, it is anticipated that most data shared with the parties to this Agreement will involve a mix of data classes including Sensitive and possibly Confidential information. Therefore, whenever data elements are aggregated for collection, transmission, or storage, the aggregate data shall be handled using the protocols that apply to the most sensitive data element.

5.1 Personnel

5.2 Access to Data

The parties to this Agreement shall limit access to Sensitive and Confidential data to those staff members with a well-defined business need.

5.3 Security Training

The parties to this Agreement shall provide periodic training for staff on internal security policies and procedures, and on applicable state and federal legal requirements for protecting Sensitive and Confidential data.

5.2 Criminal Background Checks

The parties to this Agreement shall certify that all staff members with access to confidential information have been subjected to a bone fide criminal background check and have no record of any felony convictions. Any exceptions to this requirement must be approved in writing by the parties to this Agreement.

5.3 Prohibition on Mobile Devices and Removable Media

The parties to this Agreement shall have a written policy prohibiting the transfer or storage of unencrypted customer information on employee mobile devices or removable storage media for any reason. This policy shall be made available to each employee individually and shall be strictly enforced.

6.0 Compliance with Applicable Laws and Regulations

The parties to this Agreement shall comply with all applicable federal laws and regulations protecting the privacy of citizens including the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). Where applicable, the parties to this agreement shall also comply with all provisions of the Financial Services Modernization Act (the “Gramm-Leach-Bliley Act”).

7.0 Indemnification

The parties to this Agreement shall defend, indemnify, release, and hold said parties harmless from and against all Claims, Losses, and Expenses when arising out of or incidental to this Agreement regardless of the negligence or fault of the person.

8.0 Amendments and Alterations to this Agreement

The parties to this Agreement may amend this Agreement by mutual consent, in writing, at any time.