*(The following agreement is a TEMPLATE and sets forth a data sharing agreement between organizations. If you plan on sharing data with a governmental organization, please check if they have their own template they would prefer to use before utilizing this template. Both parties should review and edit the document together – and consult with each party’s respective legal counsel – to reflect the specific nature and scope of their data sharing agreement.* ***This template is offered as a resource for organizations contemplating data sharing but shall not be construed as an instrument providing legal, financial, or data sharing advice.****)*

*Please review the tool created by the Actionable Intelligence for Social Policy linked* [*here*](https://aisp.upenn.edu/wp-content/uploads/2020/06/AISP-Intro-.pdf) *before you begin filling out the Data Sharing Agreement form.*

**Data Sharing Agreement**

**Between**

**[Insert Providing Organization Name]**

**And**

**[Insert Requesting Organization Name]**

This Data Sharing Agreement (“Agreement”) is entered by and among the **[Providing Organization Legal Name ]**(“Providing Organization Nickname”), located at [Providing Organization Address] and **[Requesting Organization Name]** (“Requesting Organization Nickname ”) located at [Requesting Organization Address]. This Agreement shall be effective as of [Enter Effective Date] (“Effective Date”).

1. **PURPOSE AND INTENDED USE OF DATA SHARING.**

*Describe the purpose of the data-sharing agreement between the Providing Organization and Requesting Organization. Describe why the sharing initiative is necessary, objectives and benefits the Requesting Organization hopes to achieve.*

1. **DEFINITIONS**.
   1. User. Includes any person with access to covered data.
   2. Public Information is information that can be freely given to anyone.
   3. Sensitive Information is all other information that is confidential, private, personal, or otherwise sensitive in nature. Sensitive Information includes the following:
      1. Personally Identifiable Information, including an individual's name; address; date of birth; student ID number assigned by a school district, local education agency, or state education agency or partner organization.
   4. Data Steward. The Data Steward has supervisory authority and is ultimately responsible for all tasks related to the management of data under this Agreement and ensures compliance with all applicable agreements and regulatory requirements. The Data Steward reports any compliance issue or breach to the [Providing Organization Nickname].
   5. Data Manager. The Data Manager is the supervisory authority for the [Providing Organization Nickname] and will be responsible for assuring the safe and secure transfer of the data from [Providing Organization Nickname] to [Requesting Organization Nickname].
   6. Include all other definitions that are necessary to understand the agreement fully.
2. **TERM AND TERMINATION.**
   1. **Term.** This Agreement shall be in effect for [time length] from the Effective Date and thereafter shall renew for [term length] terms until terminated in accordance with 2b.
   2. **Termination.** This Agreement may be terminated by any party with thirty (30) days written notice to the other parties. In the event of the termination of the Agreement, the Parties shall, upon request, (1) delete all data containing individually identifying information obtained under this Agreement; and (2) certify in writing within ten (10) business days that all copies of the data stored on cloud-based or local servers, backup servers, backup media, or other media have been permanently erased or destroyed.
3. **DESCRIPTION OF DATA.**
   1. [Data set name] Data Set. [Providing Organization Nickname] shall share with [Requesting Organization Nickname] according to the specifications set forth in [EXHIBIT A]. The data shared shall be limited to the data elements mutually agreed upon by the parties. The designated representative of each party will agree on specific data elements and data and record and file formats.
4. **DATA TRANSFER AND ACCESS.**
   1. *Describe how the data will be transferred from the Providing Organization to the Requesting Organization, the frequency in which the transfer will occur, and how the requesting organization will access the transfer.*
   2. The Data Steward at the [Requesting Organization Nickname] will have primary access to the data upon transfer, and all other users that are to have access to the data are named below:
      1. [Insert other names and roles of any additional people who will have access to the data].
   3. All creation, use, and/or transmittal of linked, de-identified, and/or limited data sets created under this Agreement is subject to the specific terms of this Agreement. Under no circumstances will any data sets subject to the terms of this document be released to any party unless the proposed use of the data set is explicitly authorized by the execution of an approved Data Sharing Agreement or amendment.
5. **DATA SECURITY.**
   1. Both parties agree to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data to prevent unauthorized use or physical or electronic access to it and to report violations of this Agreement. Appropriate administrative, technical, and physical safeguards include, but are not limited to:
      1. Users must only save Sensitive Information on personal computers that are approved for storage of such information.
      2. Users shall put in place reasonable safeguards and security procedures for its environment, including, but not limited to, using password-protected spreadsheets, using password-protected computers, prohibiting password sharing among users, prohibiting unauthorized data downloads and distribution of data; requesting that users do not leave the computer unattended and/or set a timeout to lock an unattended computer, installing antivirus software with current updates and a supported operating system with current patches and updates.
      3. Parties shall provide periodic training for Users on internal security policies and procedures and on applicable state and federal legal requirements for protecting the privacy of individuals.
6. **COMPLIANCE.**
   1. Compliance with this Agreement includes, but is not limited to:
      1. Integrity Audits. To ensure compliance with this Agreement and the protection of [incomplete sentence?]
      2. Compliance with all federal, state, and local laws and regulations.
   2. In order to protect Sensitive Information, the Data Manager shall have the right to make, via designated Users, unannounced visits to the [Requesting Organization Nickname] for purposes of inspecting computer equipment and reviewing the security arrangements that the Program Administrator is maintaining with respect to Sensitive Information. Program Administrators will fully and promptly cooperate with the Data Manager and will assist them in completing those inspections. The Data Manager must coordinate access with the Data Steward.
   3. [Providing Organization Nickname] may temporarily suspend, block, or restrict access to Sensitive Information when it reasonably appears necessary to do so to protect the integrity, security, or functionality of Sensitive Data or to protect the organization from liability.
   4. Breach of This Agreement. If at any time a User of either party determines that there has been a breach of the security protocols or violation of this Agreement (including, but not limited to any unauthorized release, access use, or modifications of covered data), the User shall promptly take such reasonable steps as are necessary to prevent any future similar breaches and promptly notify the Data Steward and/or the Program/Contract Administrator and/or the Data Manager of the breach. The Data Manager and Program Administrator will identify the steps taken to prevent any future similar breaches and report to the Data Steward within 24 hours of their discovery.
   5. Reported Violations. The Data Manager and Data Steward will issue a report identifying any privacy and security breach on covered data by a User. [Requesting Organization Nickname] will have three (3) business days to comply and put in place corrective measures to prevent any future similar breaches. Failure to comply within this time frame will result in temporary or permanent termination of access to covered data and possibly termination of this Agreement.
   6. Indemnification. In the event of a breach of this Agreement by [Requesting Organization Nickname], including a failure to comply with all federal, state, and local laws and regulations, [Requesting Organization Nickname] agrees to fully defend, indemnify, protect and hold harmless [Providing Organization Nickname], including its officers, employees, and agents, from any claims, demands or liability of any kind or nature arising from or related to the actions of [Requesting Organization Nickname], including its officers, employees, and agents.
7. **MODIFICATION.** The Parties may amend this Agreement by mutual consent, in writing, at any time. This Agreement may be terminated by either party with thirty (30) days’ written notice.
8. **SIGNATURES.** By the signatures of their duly authorized representatives below, the [Providing Organization Nickname] and [Requesting Organization Nickname] agree to all of the provisions of this Data Sharing Agreement

**[Providing Organization Full Name] [Requesting Organization Full Name]**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**By: By:**

**Title: Title:**

**Date: Date:**

**EXHIBIT A.**

Describe the data being provided in this agreement. (Be specific – include variables names, descriptions, format, level of security/sensitivity.)