District Public Employee and Partner Agreement
Data Security and Privacy Policy

District Public ("DP") uses student data only for the purposes of assisting schools in better serving their students. As a DP employee or contractor, you are responsible for taking all reasonable efforts to protect student and company data from unauthorized use. Below are the steps you are required to take in order to do so:

1. Data sharing. Never share any student, school, or company data with anyone besides DP staff or the school principal or staff to whom it pertains, except to those the school principal has provided consent to share it with.

1. Personally identifiable data: Never request personally identifiable student data not needed for analysis, such as addresses, phone numbers, and birth dates. When such data is inadvertently acquired by District Public, immediately notify DP and remove it from any and all files in which it appears.

2. Data storage: Only store student data on the Google Drive encrypted with Boxcryptor, or on the unencrypted Google Drive folders that are shared exclusively with DP staff and the school principal and staff to whom the data pertains. District Public will request all data to be sent from principals via a designated "Files Received from School" Google Drive folder set up for each client school and will provide principals instructions on how to post files there.

3. Data removal: Remove any analysis or raw data that includes student data from other locations on which it may temporarily reside, including, but limited to, emails and downloads folders, at least once every two weeks.

4. DP computer and email use: All data analysis must be done only on DP-owned devices. These devices must have full hard drive encryption and must have anti-virus software installed and running. All DP business must be conducted exclusively using @district-public.com email addresses. Emails that contain student data must be deleted as soon as the file has been retrieved and saved down into DP's encrypted drive.

5. Two-factor authentication: Employees and partners are responsible for maintaining two-factor authentication on their @district-public.com email addresses and Google Drive access.

6. Virtual Private Networks: Employees and partners must use a virtual private network when accessing publicly available internet connects, for example in coffee shops and airports.

By signing below, I agree that I have read and understood District Public's data security and privacy policy, and that I will make my best effort to follow these policies.

Printed Name: _____

Position: _____

Signature: _____ *Date:* _____