Supplemental Information

Pursuant to Education Law § 2-d and § 121.3 of the Regulations of the Commissioner of Education, NYSED is required to post information to its website about its contracts with third-party contractors that will be provided Access to or receive Disclosure of Student Data and/or APPR Data.

1. **Name of Contractor:** President and Fellows of Harvard College

2. **Description of the exclusive purpose(s) for which the Student Data and/or APPR Data will be used:**

To efficiently deploy resources to develop a robust educator pipeline, states (and districts) can generate new insights using their state longitudinal data regarding the current and prokected supply of qualified educators, a nuanced perspective of the factors that produce the geographically and subject-specific shortages typically observed in the educator labor market, and evidence-based strategies to attract, retain, and develop educators. While NYSED currently collects data regarding educator certification, employment and teaching assignments in New York public schools, and evaluation ratings, as well as basic data on shortages, this information had long been stored in separate databses that were not interoperable and did not include student-level data from educator preparation programs. This greatly limited the state's ability to generate useful reports and analyses of key issues related to educator shortages, preparation program quality, and educator effectiveness, diversity, retention, and mobility, to inform decisions related rto policy, practice, and funding. However, New York's statewide longitudinal data system (SLDS) will integrate data from P-12, higher education, and workforce data sets. With improved interoperability comes the need to design and generate new reports based on the linked datasets and to analyze those reports to answer important questions about the state's educator workforce, and the Strategic Data Project's partnership will build NYSED's capacity to do that work. Specifically, we will generate a research diagnostic that will answer the following questions: What is the landscape of teacher demand for the state? What are the characteristics of the current and potential educator workforce in the state? To what extent are the state's education varying preparation program pathways fulfilling teacher workforce needs?

3. **Type(s) of Data that Contractor will be provided:**

Yes Student Data

No APPR Data

4. Contract Term:

Contract Start Date: 03/03/2025

Contract End Date: 09/03/2028

5. **Subcontractor use and written agreement requirement:**

No Contractor will use Subcontractors.

If Contractor plans to use Subcontractors, Contractor will not utilize Subcontractors without a written contract that requires the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Contractor by state and federal laws and regulations and this contract.

Contractor agrees to bind its Subcontractors by written agreement.

6. **Data Transition and Secure Destruction**

Yes Contractor agrees that the confidentiality and data security obligations under this DPA will survive the expiration or termination of this contract but shall terminate upon Contractor’s certifying, that Contractor and its Subcontractors:

a. Are unable to Access any Information provided pursuant to this contract; and
b. Securely transfer Disclosed Student Data and APPR Data to NYSED, or at NYSED’s option and written discretion, a successor contractor in a format agreed to by the Parties; and
c. Securely deleted and destroyed Disclosed Student Data and APPR Data.

7. Challenges to Data Accuracy

Yes Contractor agrees that parents, eligible students, teachers, or principals who seek to challenge the accuracy of Student Data or APPR Data will be referred to NYSED and if a correction to data is deemed necessary, NYSED will notify Contractor. Contractor further agrees to facilitate such corrections within 21 days of receiving NYSED’s written request.

8. Secure Storage and Data Security

Please indicate where Student Data and/or APPR Data will be stored:

Using a cloud or infrastructure owned and hosted by a third party.

Using Contractor owned and hosted solution.

Yes Other:

Personally identifiable information and other sensitive information will be stored in CEPR's secure data environment at Harvard University. CEPR's secure data environment is certified by Harvard University IT (HUIT) to house data of security level 4 (DSL4 -High Risk Confidential Information) and operates on independent and secure networks that are not routed to the rest of the university. or any public address space, with no direct internet access. The CEPR secure environment is hosted on a private RFC1918 IP address space on a dedicated VLAN. It is isolated from all other network systems through ACLS and firewalls, and outbound traffic is blocked unless there is an explicit exception. Physical servers are housed in locked server rooms at the Massachusetts Green High Performance Computing Center (MGHPCC). Physical access to MGHPCC is restricted via electronic lock to authorized users only. Access control and electric door locks are monitored at all times with alarms to alert security cameras or Harvard campus police for any breach. The data security plan for the CEPR has been approved by the HUIT data security team.

Please describe how data privacy and security risks will be mitigated in a manner that does not compromise the security of the data:

The Center for Education Policy Research (CEPR) at Harvard University has robust data security infrastructure and practices in place that it has used over the course of its decade-long history of working with education data from agencies across the country. CEPR's data security infrastructure and practices to protect data include, but are not limited to: Password protections; Administrative procedures; Encryption; Firewalls. Personally identifiable information and other sensitive information will be stored in CEPR's secure data environment at Harvard University. CEPR's secure data environment is certified by Harvard University IT (HUIT) to house data of security level 4 (DSL4 -High Risk Confidential Information) and operates on independent and secure networks that are not routed to the rest of the university or any public address space, with no direct internet access. Electronic data analysis on sensitive data (DSL3 -Medical Risk Confidential Information and DSL4) will be performed on servers in the secure CEPR data environment. A dedicated CEPR VPN realm for remote access to the secure environment is the only way to access this system remotely via remote desktop. Access to the VPN requires 2-factor encrypted authentication. Our team follows institutional safeguards to reduce risk. These include requiring users to sign non-disclosure agreements and agree to the remote access policy. Users only have access to the data through their individually assigned (non-shared) user accounts. Accounts are requested through a Portal requiring approval by the CEPR Data Manager, and all group membership (e.g., to a specific project) require approval by the CEPR Data Manager. The servers enforce Harvard standard password complexity rules and require a minimum password length of 12 characters. Servers and the applications that process the confidential information are designed so that passwords cannot be retrieved by anyone (including system administrators). Data is organized by research project diretor and CEPR Data Management team and is granted on a need-to-know basis. Continued access is reviewed monthly by CEPR Data Management team and project leadership to ensyure adherence to Harvard and CEPR data security policies and DUA terms. Obsolete accounts are promptly disabled and removed from the system when they no longer have a reason under the access policy to access the information (e.g., they change jobs or leave the university). Study staff will go through FERPA and data security training with CEPR's data manager, as well as training on any protocols that have been developed for this project, including CITI Human Subject Research and Information Privacy Security training. Additionally, all Harvard staff must complete information Security Awareness training.

9. Encryption requirement

Yes Contractor agrees that Student Data and APPR Data will be encrypted while in motion and at rest.

10. Contractor Certification.

Contractor certifies that Contractor will comply with, and require its Subcontractors to comply with, applicable State and Federal laws, rules, and regulations and NYSED policies.

Contractor’s Name President and Fellows of Harvard College