MASTER SERVICES AGREEMENT

BETWEEN THE DISTRICT OF COLUMBIA GOVERNMENT THROUGH THE D.C. OFFICE OF THE STATE SUPERINTENDENT OF EDUCATION AND URBAN INSTITUTE

FOR THE DISTRICT OF COLUMBIA EDUCATION RESEARCH PRACTICE PARTNERSHIP

I. INTRODUCTION

This **MASTER SERVICES AGREEMENT** ("Agreement") is entered into between the **DISTRICT OF COLUMBIA GOVERNMENT** ("District"), a municipal corporation, acting by and through the **D.C. OFFICE OF THE STATE SUPERINTENDENT OF EDUCATION**, ("OSSE"), and the **URBAN INSTITUTE** ("Urban"). The District, through OSSE, and Urban, shall be collectively referred to herein as the "Parties." The Parties enter into this Agreement to organize, constitute, and implement the District of Columbia Education Research Practice Partnership ("RPP").

II. AUTHORITY FOR AGREEMENT

This Agreement is subject to and authorized by the provisions of the District of Columbia Education Research Practice Partnership Establishment and Audit Act of 2018[1] (D.C. Official Code § 38-785.01, et seq.) ("RPP Act"), the Family Educational Rights and Privacy Act [Pub. L. 90-247, 80 Stat. 783 (Jan. 2, 1968), as codified at 20 U.S.C. § 1232g], and the U.S. Department of Education's implementing regulations [34 C.F.R. § 99 et seq.].

III. BACKGROUND

The RPP Act created the RPP to conduct independent education-related research to support improvement in the District's public schools and public charter schools, to publicly report the findings of the research and to benefit the Council's legislative and oversight responsibilities. The RPP, in consultation with the Advisory Committee, as established by the RPP Act, will approve all research and evaluation projects.

OSSE is the state education agency ("SEA") for the District of Columbia. OSSE serves as the District's liaison to the U.S. Department of Education and works closely with public and public charter schools in the District of Columbia to achieve its key education functions. The mission of OSSE is to work urgently and purposefully, in partnership with education and related systems, to sustain, accelerate, and deepen progress for District students with the goal of closing the achievement gap and ensuring people of all ages and backgrounds are prepared to succeed in school and in life.

[1] code.dccouncil.us/dc/council/code/titles/38/chapters/7E/

As the SEA, and in accordance with the federal Family Educational Rights and Privacy Act ("FERPA"), and in particular 34 CFR 99.31(a)(6), OSSE is empowered to disclose educational records to educational researchers to carry out research studies for the purpose of developing, validating or administering predictive tests, administering student aid programs, and/or improving instruction. OSSE collects educational data from publicly funded District of Columbia local education agencies ("LEAs") and schools and has adopted a policy and procedure for re-disclosure of educational records to educational researchers for the purposes of carrying out permissible educational studies.

Urban Institute is a 501(c)(3) tax-exempt research organization dedicated to elevating the debate on social and economic policy. Urban Institute will partner with other education research organizations, which together form the DC Education Research Collaborative ("Collaborative"), and which collectively will serve as the RPP.

Urban, together with the Collaborative constitutes the RPP, which is an independent, non-governmental entity under the RPP Act.

IV. GOAL AND OBJECTIVES

The RPP will conduct independent education-related research that will support improvement in the District's public schools, including research to identify instructional practices that increase student achievement, educational equity, and school improvement based on rigorous research methods; provide the research necessary to inform and assess instructional practices in District public schools; evaluate existing instructional practices to determine their impact on student academic achievement and progress; and otherwise assist the District with research aimed to improve instruction and student outcomes in the District.

The purpose of the RPP is to provide actionable, easily consumable, independent research to the education sector, stakeholders, and the public. The RPP will receive guidance from an Advisory Committee of 21 members with expertise in the research process related to student learning, school improvement, and urban education policy.

This Agreement defines certain requirements and responsibilities governing the partnership between the District and Urban for implementing the RPP to support cooperation and collaboration on education-related research project as defined herein; and will be supplemented by future Data-Sharing Memoranda of Agreements (hereinafter "data sharing agreements" and/or "MOAs") that are intended to be specific to support data sharing for each research project approved by Urban, with feedback from the Advisory Committee established in furtherance of the RPP Act. The agreed-upon template for future data sharing MOAs is incorporated by reference into this Agreement as Appendix A.

The subsequent sections of this agreement outline the agreed-upon operational protocols and understandings governing research projects approved by Urban, with feedback from the Advisory Committee established by the RPP Act.

V. RESEARCH PROJECT DEFINED

A. "Research Project" shall mean, collectively, the set of activities aimed at answering a set of research questions that are within the scope of the RPP's research agenda, this Agreement, and any executed data-sharing MOA.

B. Any and all Research Projects performed in furtherance of the RPP Act shall be subject to this Agreement as well as specific MOAs used to support specific research projects.

C. Prior to performing any Research Project, Urban shall submit a written proposal to the Advisory Committee for feedback. Urban will also consult with the District in advance of proposing research projects to the Advisory Committee to ensure data availability and to avoid duplication of effort.

D. A Research Project proposal, for which the Advisory Committee has had the opportunity to provide feedback pursuant to D.C. Code section § 38-785.05(b)(1), shall be referred to as an "Approved Research Project".

E. Prior to using any District-owned data for an Approved Research Project, the District and Urban shall enter into an appropriate MOA that incorporates the Approved Research Project proposal, to be signed by an authorized representative of all respective parties providing data to support the Approved Research Project.

F. Urban shall not directly approach any District agency for data without first notifying and making reasonable good faith efforts to coordinate with and through OSSE, as further provided in Section VII(C).

G. With the exception of any MOA that allows for data retention beyond the period of time necessary to conduct the Approved Research Project, the terms and conditions of any MOA in furtherance of an Approved Research Project may supplement but may not modify the provisions of this Agreement. In the case of any conflict of terms between this Agreement and any Approved Research Project proposal or corresponding MOA, this Agreement shall control.

VI. PROCESS OF COLLABORATION

A. In order to support the establishment and operation of the RPP, it is expected that the RPP and OSSE will meet on a routine basis and establish protocols for those meetings. These protocols are anticipated to evolve as the RPP matures, and as such these are specified not in the body of this Agreement but in Appendix F.

B. Appendix F will include details regarding:
   i. Meetings;
   ii. Reporting;
   iii. Interim review of project status and deliverables; and

iv. Technical means and methods.

C. Appendix F will be reviewed at least annually by the Parties. Any updates that are agreed by both Parties will be made in writing at least annually, though more frequent updates are permitted if agreed to by the Parties.

VII. CONFIDENTIAL INFORMATION, DISTRICT DATA AND URBAN DATA DEFINED

A. In the performance of this Agreement, Urban or the District may have access to or receive certain information that is not generally known to others ("Confidential Information").

B. **Confidential Information**, broadly defined, may include but is not limited to Staff Data, Student Data, and School Level Data, including but not limited to: name, address, student identification number, Social Security Number, phone number, email address, gender, date of birth, ethnicity, race, foster care status, disabilities, school, grade, course grades, statewide assessment data, after school activities, highest grade completed, discipline history, criminal history, free or reduced-price lunch qualifications, housing status, income, household income or payroll information, college enrollment records, Free Application for Federal Student Aid ("FAFSA") information, and unpublished school information, and District financial information.

C. It is understood that Confidential Information may include data from other District agencies that OSSE is in possession of and obtained through a duly executed data sharing agreement. OSSE cannot re-disclose these data from other District agencies without permission. As provided for in this Agreement, in cases where such data are needed, Urban shall request permission from OSSE, which will facilitate negotiations with the respective District agencies whose data is sought. In the event that OSSE or the respective District agency are unresponsive, Urban shall have the rights afforded to them under DC Official Code §38-785.05(d) of the RPP Act.

D. It is understood and agreed that Confidential Information may also include proprietary or confidential information of third parties provided to Urban by either the District or other third parties, as described herein.

E. It is further understood and agreed that Confidential Information may include Urban-collected data (as further defined in this Agreement). Any data collected by Urban that constitutes proprietary, personal, or confidential data about the District and/or its constituents shall be subject to an applicable data sharing agreement, which shall explicitly reference the existence of such confidential information prior to sharing any such data with the District.

F. **District Data**: Pursuant to a fully executed MOA in furtherance of an Approved Research Project, the District may provide Urban with Confidential Information. Such information may include (i) "Student Data" comprised of (a) personally identifiable student-level data, (b) de-identified student-level data, or (c) aggregate-level student data; (ii) "Staff Data" comprised of (a) personally-identifiable staff level data, (b) de-identified staff-level data, or (c) aggregated staff-level data; and (iii) School-Level Data comprised

of information or data not generally known to the public which identifies or could reasonably be used to identify a particular public or public charter school and which is not student data or staff data.

G. **Urban Data**: Urban may collect other data independently or merge District data with data from other sources in a manner that preserves confidentiality of the data as provided for in this Agreement. Urban will share data it collected with the District to the extent permissible under law and under the terms of Urban's agreement with the respective data owners.

VIII. INTELLECTUAL PROPERTY AND OWNERSHIP OF DATA

A. Any and all District Data shall at all times be and remain the property of the District.
B. Any and all intellectual property developed by the District shall at all times be and remain the property of the District.
C. Unless otherwise specified in a particular MOA, the District acknowledges and agrees that all intellectual property developed by Urban shall be and remain the property of Urban.
D. All Urban-collected data that was obtained exclusively by and through duly executed written consent shall at all times be and remain the property of Urban.

IX. DISTRICT DATA AVAILABILITY AND DATA COLLECTION

A. The Parties agree that Urban shall, to the extent possible, implement research projects using existing data already collected by the District.

B. Should an Approved Research Project arise for which the District does not currently own or have rights to the data but does wish to collect it directly, it is acknowledged that the District will need to engage in planning, development, and testing work, including engaging with LEAs, before such data will be ready for provision to Urban and use in the Approved Research Project. These efforts are acknowledged to be limited by agency staffing and capacity, as well as availability of agency funding.

C. Urban shall consult with the District before initiating new data collections that the District wishes to administer directly.

X. DATA AND INFORMATION: SHARING, USE, RETENTION, SECURITY, BREACH AND DESTRUCTION

A. <u>JOINT RESPONSIBILITIES</u>

1. The Parties shall enter into a written data sharing MOA for each Approved Research Project, in compliance with FERPA and other relevant federal and local laws. In those cases where data is owned by any third party(s), the MOA may be subject to limitations of any data sharing agreements executed between OSSE and such third party(s) and between Urban and such third party(s).

2. The subsequent pieces of this Section will be reiterated in the data sharing MOAs to be negotiated for specific projects.

B. RESPONSIBILITIES OF THE DISTRICT

1. The District shall provide existing data to Urban, as permissible under any MOA executed pursuant to section A of this paragraph.

C. RESPONSIBILITIES OF URBAN

1. Prohibited Use of District Data by Urban:

a. Urban shall not use any District Data for any purpose not specifically identified in the associated MOA, including for any other research project or purpose, regardless of whether such research project or purpose is internal (within another department) or external to Urban, unless such other research project or purpose is explicitly described in any future MOA associated with this Agreement.
b. Urban shall not release any District Data except as specifically authorized under any future MOA pursuant to this Agreement.
c. Publicly available discussions, presentations and reports based on District Data shall not include information that would make it possible to identify a child, student, educator (including a teacher or other staff), or classroom unless the District grants specific permission in writing to do so.
d. In general, Urban shall not retain any District Data except as specifically authorized under any future MOA pursuant to this Agreement or future modification to this Agreement.
e. Urban shall not disclose Confidential Information except to those of its employees or agents, and Collaborative members and their employees or agents, who have a need to know the Confidential Information and any such disclosure shall incorporate all provisions set forth by the District.
f. Any use, release or retention of Confidential Information not specifically documented in this Agreement or any corresponding data sharing MOA shall also be considered a material breach of this Agreement.

2. Allowable Use of District Data by Urban: Subject to the provisions of the applicable data sharing MOA(s), the terms of this Agreement, all applicable state, federal and local laws, executive orders, and ordinances, and all applicable District rules and policies pertaining to data use, data confidentiality and data suppression as may be issued, enacted and/or amended from time to time, Urban may:

a. Perform and undertake the Approved Research Project explicitly described in the applicable MOAs;
b. Use aggregated data in publications resulting directly from the Research Project performed from an executed MOA without written approval from the District, provided that no such publication shall contain personally identifiable Confidential Information or District Data and that the District receives a preview copy prior to publication, as required in paragraph XII.
c. Analyze aggregated data generated across multiple executed MOAs in publications and presentations without additional written approval from the District, provided that the District may review any and all such publications, as required in paragraph XI, provided that in all such publications and presentations, Urban maintains confidentiality in the manner provided for this Agreement.
d. Publish aggregated data from education records, provided that Urban adheres to disclosure avoidance guidelines from the U.S. Department of Education and OSSE's Student Privacy and Data Suppression Policy, both of which are incorporated by reference into this Agreement as Appendixes D and E, respectively.
e. Retain certain data under specific circumstances, to be negotiated with the District, in accordance with an executed MOA for a specific purpose in furtherance of the RPP's work and a specific Approved Research Project and pursuant to paragraph IX.C.4 of this Agreement.

3. Security.

a. The Parties to the Agreement will use, restrict, safeguard, and dispose of all information related to services provided by this Agreement in accordance with all relevant federal and local statutes, regulations, policies, and guidance, including but not limited to FERPA, HIPAA, IDEA, and the District's laws and policies in furtherance of same, as they may be subsequently enacted, issued and/or amended.
b. Urban's information security and data management practices shall meet the following the National Institute of Standards and Technology (NIST) (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf) standard security definition:
    i. **Confidentiality:** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]. The unauthorized disclosure of information is considered a loss of confidentiality.

ii. **Integrity:** "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information.

iii. **Availability:** "Ensuring timely and reliable access to and use of information…" [44 U.S.C., Sec. 3542] A loss of availability is the disruption of access to or use of information or an information system.

c. Urban and its employees and agents will store data disclosed to Urban related to this Agreement and future MOAs in a manner that will preserve the confidentiality, integrity, and availability of all data and will ensure that this information is not disclosed to anyone other than responsible Urban employees and its employees, contractors, agents and Collaborative members for the purposes of implementing the Agreement and any MOAs.

d. Before the first Approved Research Project, and accompanying data sharing MOA, Urban, will provide OSSE with written security policies, including any technical requirements, data destruction guidelines, or how their practices align with the NIST Sanitization Guidelines referenced in Appendix B.

e. Prior to sharing data with Urban, its employees or agents, Urban will provide OSSE with a written data security plan describing the following minimum information security standards and send it to Gwen.Rubinstein@dc.gov or such other person as may be designated by the District and OSSE.datasharing@dc.gov:

i. **Identity, Credential, and Access Management**: how the authentication and authorization of individuals and systems to the data being accessed is ensured;

ii. **Auditability and Alerting:** how regular and irregular oversight potentially detect malicious activity and reduce risk of collusion, including a checklist suggesting how OSSE may audit Urban's adherence with the terms of this agreement;

iii. **System Security:** how IT systems are maintained, and vulnerabilities are managed, to reduce the risk of security incidents, as well as incident response plans should an event occur;

iv. **Data Stewardship and Destruction:** how the chain of custody is proactively maintained (for users and systems) and how data is effectively erased to minimize the likelihood of inadvertent access; and

v. **User Training and Education:** how policies and information security standards are communicated.

These policies can be in any format, but preference for industry-standards is preferred- such as "System and Organization Controls (SOC)," "SysAdmin, Audit, Network, and Security" (SANS) templates.

f. Upon request, Urban and its agents shall provide the District with written confirmation of where Confidential Information and/or District Data is stored, transmitted and processed either under a specific Approved Research Project and pursuant to a respective MOA or all data received under this Agreement, as well as a list of users who have had access to the data.

g. All work with Confidential Information and/or District Data for the RPP shall be conducted in the secure computing environment(s) led, owned, controlled and administered by Urban. Regardless of the computing environment, Urban agrees to retain full control of all data supplied by the District, particularly to prevent unauthorized access and unauthorized re-disclosure.

h. Urban, and its employees and agents, shall not store or retain confidential data locally, including intermediate or temporary data files that contain PII and any data files that could potentially lead to the disclosure of PII, on personal computers or networks, including on local devices such as removable or portable storage devices, laptops, or systems or analytics platforms outside the direct administration and control of Urban as required by subparagraph f.

i. Urban must notify OSSE, within 24 hours of the date on which Urban becomes aware of any data incident, as defined in OSSE's Data Incident Plan (osse.dc.gov/sites/default/files/dc/sites/osse/publication/attachments/Data%20Incident%20Plan.pdf). The written notification shall be sent to Gwen.Rubinstein@dc.gov and OSSE.datasharing@dc.gov. OSSE will provide notice to the District's Office of the Chief Technology Officer and to the Office of Risk Management, and collectively which may take any actions authorized it by law to remediate the breach, including, without limitation, exclusion of Urban from future access to educational data. Failure to provide notification under this paragraph is grounds for termination of the Agreement, as well as potentially other legal and financial penalties.

j. Urban shall provide OSSE with a plan for monitoring compliance with the documented information security practices by their staff and agents, as well as information technology, and submit an annual report to OSSE on the outcomes of the monitoring compliance. Annual reports shall be submitted to Gwen.Rubinstein@dc.gov and OSSE.Datasharing@dc.gov.

4. Data Destruction or Retention.

a. As provided in Section VII [*Intellectual Property and Data Ownership*], the District retains full ownership rights to the information in the education records it provides to Urban. Unless specifically noted as an exception in the data sharing MOA specific to an individual Approved Research Project, Urban and its agents agree to destroy all information:
   i. At the District's request in the event of a default or data incident;
   ii. When the data are no longer needed to achieve the Approved Research Project's purposes;
   iii. Upon termination of this Agreement pursuant to Section XIX; or
   iv. As otherwise required by District or federal law.

b. Upon completion of the Approved Research Project, Urban must revoke access to these data from all employees and agents, except for a fixed number of data custodians, to be agreed by the Parties, even if it's anticipated they will have access for a subsequent Approved Research Project.

c. In instances where the Parties agree that Urban may retain the data after the completion of an Approved Research Project, the MOA governing the Approved Research Project shall either identify at the outset or be modified to include the terms and purpose of re-use, retention, and destruction, and any clauses within this Master Services Agreement that do not apply.

d. When a subsequent Research Project referencing the same data is approved, Urban may then provide access to the retained data to the necessary researchers, reducing the need for retransmitting the data between OSSE and Urban.

Urban shall confirm in writing to the District its compliance with the terms of this section within 10 business days after the expiration of an Approved Research Project. This includes acknowledgement of OSSE's decision whether Urban is permitted to retain, or must destroy, the relevant data. The written notification shall be sent to Gwen.Rubinstein@dc.gov and OSSE.datasharing@dc.gov.

XI. INSTITUTIONAL REVIEW BOARD

Urban warrants that its research activities comply with the U.S. Department of Education's regulations governing the protection of human subjects in research found in Part 97 of Title 34 of the Code of Federal Regulations. When required by such regulations, Urban shall obtain approval from the appropriate Institutional Review Board prior to submitting any report issued by Urban under this Agreement to OSSE for advance review as further set forth herein.

XII. ADVANCE REVIEW OF REPORTS AND PRESS RELEASES

A. At least 30 days prior to the publication of any analysis or report issued by Urban under this Agreement or any other subsequent data sharing MOA, Urban shall provide an electronic copy of the analysis or report work in a draft format suitable for commenting to OSSE.

B. Urban shall make an electronic copy of any interim work products (scripts, analysis artifacts, etc.) available to OSSE upon request.

C. If OSSE does not respond within the 30-day advance review period, Urban shall be authorized to release and publish the Approved Research Project.

D. Upon completion of the initial 30-day review period, OSSE may request and Urban shall grant one (1) extension of the review period by an additional 30 days. Granting of this extension of the review period shall not be unreasonably withheld.

E. After receipt and review of the draft analysis or report, OSSE and Urban shall coordinate to discuss solutions for any noted issues that do not comply with this Agreement.

F. Urban shall not publish any version of a report containing information that has been identified by the District as noncompliant with this Agreement, and for which written notice has been sent to Urban detailing each instance of non-compliance.

G. No fewer than 10 business days prior to the dissemination of any press release related to any Approved Research Project provided pursuant to this Agreement or any executed MOA, where such press release explicitly references data or support from the District of Columbia, OSSE, or any District governmental agency, Urban shall provide copies of such press releases to the District for written approval. Urban shall not, without the express written consent of an authorized representative of the District, use any intellectual property belonging to the District, including, but not limited to, logos (including for any agency or school), during or after the performance or the

delivery of any Approved Research Project, nor may Urban photograph or film within any District school or facility. The District's approval will not be unreasonably withheld.

XIII. COMPLIANCE AND MONITORING

A. The District will periodically monitor Urban's compliance with the terms of this Agreement. Appendix C, which is incorporated by reference into this Agreement, provides a checklist for monitoring that may occur under this Agreement.
B. Urban will respond within a reasonable time to the District's requests for any information, reports, or other assurances of Urban's or of Urban's agents' or Collaborative members' or agents' ongoing compliance with this Agreement.

XIV. HIPAA COMPLIANCE

To the extent applicable for any Approved Research Project, the District and Urban shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules").

A. Urban warrants to the District that it is familiar with or will become familiar with the requirements of the Privacy Rules and will comply with all applicable requirements in the course of this Agreement, to be further set forth in any subsequent data sharing MOA.
B. Urban warrants that it will cooperate in good faith with the District, including good faith cooperation and coordination with District privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

XV. NON-DISCRIMINATION

In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Official §§ 2-1401.01, *et seq*. ("Act") the District of Columbia does not discriminate on the basis of actual or perceived: race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, place of residence or business, and status as a victim or family member of domestic violence, a sexual offense, or stalking. Sexual harassment is a form of sexual discrimination which is prohibited by the Act. In addition, harassment based on any of the above-protected categories is prohibited by the Act. Discrimination in violation of the Act will not be tolerated. During the performance of this Agreement, Urban and its agents and employees shall comply with the Act. Violators will be subject to disciplinary action.

During the performance of this Agreement, Urban and its agents and employees shall comply with Section 504 of the Rehabilitation Act of 1973, as amended. This Act prohibits discrimination against disabled people in federally funded programs and activities. *See* 29 U.S.C. § 794 et *seq*. Violators will be subject to disciplinary action.

During the performance of this Agreement, Urban and its agents and employees shall comply with the Americans with Disabilities Act of 1990 (ADA). The ADA makes it unlawful to discriminate in employment against a qualified individual with a disability. *See* 42 U.S.C. § 1210 *et seq*. Violators will be subject to disciplinary action.

XVI. FREEDOM OF INFORMATION ACT APPLICABILITY AND LIMITATION

The District of Columbia Freedom of Information Act of 1976 (DCFOIA), Pub. L. 90-614, D.C. Official Code §§ 2-531, *et seq.* (2001), provides for the disclosure of public information. Specifically, the law provides that "any person has a right to inspect, and at his or her discretion, to copy any public record of a public body, except as otherwise expressly provided by §2-534, in accordance with reasonable rules that shall be issued by a public body after notice and comment, concerning the time and place of access." Further, a "public record" has been defined by the District of Columbia Public Records Management Act of 1985 as "all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials, regardless of physical form or characteristics prepared, owned, used in the possession of, or retained by a public body" and includes "information stored in an electronic format." D.C. Official Code §2-502 (2011).

This serves as notification that information/documentation submitted to the District pursuant to this Agreement, or in connection with the transaction of the business related to this Agreement, is subject to public disclosure in response to a Freedom of Information Act request. Any information that is not specifically exempt by D.C. Official Code § 2-534(a) may be disclosed upon a proper request, in accordance with DCFOIA.

To the extent that information and/or documentation is requested of the RPP, as an independent non-governmental entity, the RPP is entirely exempt from the requirements of the District of Columbia Freedom of Information Act (DCFOIA) as further set forth in the RPP Act, specifically D.C. Official Code §§ 38-785.01(5) and 38-785.02.

XVII. INSURANCE

A. Urban hereby warrants and represents that it is insured or self-insured, and that it has and shall maintain during the term of this Agreement adequate coverage for all Research Projects being performed under this Agreement and in furtherance of the RPP Act. The insurance required herein shall be primary to and will not seek contribution from any other insurance, reinsurance or self-insurance including any deductible or retention, maintained by the Government of the District of Columbia. Insurance coverage shall be at least as broad as the District's minimum insurance requirements which are:

1. Workers' Compensation and Employers' Liability Insurance. Workers' Compensation and Employers' Liability Insurance covering all employees, staff, contractors, and agents who are engaged in furthering a Research Project under this Agreement and Employers' Liability coverage, in accordance with the statutory mandates of the District of Columbia or the jurisdiction in which the contract is performed. Minimum insurance limits shall be as follows: $500,000 per accident for injury; $500,000 per employee for disease; and $500,000 for policy disease limit, or other covered occurrence.

2. Commercial General Liability Insurance. Commercial General Liability (CGL) insurance shall have limits of liability of not less than $1,000,000 each occurrence, a $3,000,000 general aggregate (including a per location or per project aggregate limit endorsement, if applicable) limit., CGL coverage shall include liability for all ongoing and completed operations, including ongoing and completed operations under all subcontracts, and shall cover claims for personal or bodily injury, including without limitation sickness, disease or death of any persons, damage to or destruction of property, including loss of use resulting therefrom, personal and advertising injury, and including coverage for liability (including the tort liability of another assumed in a contract) and acts of terrorism (whether caused by a foreign or domestic source). Contractual liability for the insurance agreement and products/completed operations coverage maintained for not less than two (2) years following termination of this Agreement or completion of all Research Projects.

3. Automobile Liability Insurance. When any motor vehicle and equipment (whether owned, non-owed, borrowed, or hired) is used in connection with the Research Project to be performed, Urban shall provide Automobile Liability Insurance with minimum per accident limits equal to the greater of (i) the limits set forth in the Urban's commercial automobile liability policy or (ii) $1,000,000 per occurrence combined single limit for bodily injury and property damage and $5,000,000.00 in the aggregate for bodily injury and property damage.

4. Cyber Liability and Privacy & Security Coverage. Cyber Liability and Privacy & Security Coverage for damages arising from a failure of computer security, or wrongful release of Confidential Information, including expenses for notification as required by applicable District and Federal laws. Coverage shall be sufficiently broad to respond to the duties and obligations and shall include, but are not limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. Limits of liability shall be not less than $2,000,000 per occurrence or claim, and $2,000,000 aggregate. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring

expenses with limits sufficient to respond to these obligations. Coverage shall also include failure to prevent transmission of malicious code. The policy shall be a claims-made policy with any prior acts exclusion predating the date of this Agreement. Such coverage shall either be maintained continuously for a period of 2 years after expiration or termination of this Agreement. This insurance requirement will be considered met if the general liability insurance includes an affirmative cyber endorsement for the required amounts and coverages.

5. Professional Liability Insurance (Errors & Omissions). Urban shall provide Professional Liability Insurance (Errors and Omissions) to cover liability resulting from any error or omission in the performance of professional services under this Contract. The policy shall provide limits of $2,000,000 per claim or per occurrence for each wrongful act and $3,000,000 annual aggregate. The Contractor warrants that any applicable retroactive date precedes the date the Contractor first performed any professional services for the Government of the District of Columbia and that continuous coverage will be maintained or an extended reporting period will be exercised for a period of at least ten years after the completion of the professional services.

B. Insurance – Additional Insured. Urban shall have its general liability insurance endorsed to provide that the District of Columbia Government, a municipal corporation, and its successors and/or assigns is listed as "Additional Insured" on a primary basis without recourse or right of contribution for liability arising from the work.

C. Insurance Certificate. Urban shall require its insurer(s) to submit insurance certificate(s) to the District evidencing coverage in accordance with the terms set forth herein, prior to commencing work and on an annual basis, naming the District as an additional insured as follows:

District of Columbia Government, its successors and/or assignees
c/o Office of the State Superintendent of Education
1050 First Street NE
Washington, DC 20002

Urban shall promptly deliver updated certificates of insurance, endorsements indicating the required coverages, and/or certified copies of the insurance policies when requested. If the insurance initially obtained by Urban expires prior to completion of the period of performance, renewal certificates of insurance and additional insured and other endorsements shall be furnished to the District prior to the date of expiration of all such initial insurance. For all coverage required to be maintained after completion, an additional certificate of insurance evidencing such coverage shall be submitted to the District on an annual basis as the coverage is renewed (or replaced).

D. Urban shall carry all required insurance until all contract work is accepted by the District of Columbia, and shall carry listed coverages for ten years for construction projects following final acceptance of the work performed under this contract and two years for non-construction related contracts.

E. These are the required minimum insurance requirements established by the District of Columbia. HOWEVER, THE REQUIRED MINIMUM INSURANCE REQUIREMENTS PROVIDED ABOVE WILL NOT IN ANY WAY LIMIT Urban's LIABILITY UNDER THIS CONTRACT.

F. Property. Urban and its Collaborative partners are solely responsible for any loss or damage to their personal property, including but not limited to tools and equipment, scaffolding and temporary structures, rented machinery, or owned and leased equipment.

G. Measure of Payment. The District shall not make any separate measure or payment for the cost of insurance and bonds.

H. NOTIFICATION. Urban shall ensure that all policies shall be given thirty (30) days prior written notice in the event of coverage and / or limit changes or if the policy is canceled prior to the expiration date shown on the certificate. Urban shall provide with ten (10) days prior written notice in the event of non-payment of premium.

I. DISCLOSURE OF INFORMATION. Urban agrees that the District may disclose the name and contact information of its insurers to any third party which presents a claim against the District for any damages or claims resulting from or arising out of work performed by Urban, its agents, employees, servants, or subcontractors in the performance of this contract.

J. CARRIER RATINGS. All insurance for Urban and its agents, employees, servants, or subcontractors required in connection with this contract shall be written by insurance companies with an A.M. Best Insurance Guide rating of at least A- VII (or the equivalent by any other rating agency) and licensed in the in the District.

XVIII. EVENT OF DEFAULT

Events of default by Urban ("Events of Default") include, but are not limited to, the following:

A. Any material misrepresentation by Urban in the inducement or the performance of this Agreement;
B. Breach of any term, condition, representation, or warranty made by Urban in this Agreement;
C. Failure of Urban to perform any of its obligations under this Agreement;
D. Action or failure to act by Urban that negatively affects the safety or welfare of students or District staff; and
E. Failure to conduct any research in a manner that is consistent with the Approved Research Project and corresponding MOA.

XIX. REMEDIES

A. The occurrence of any event of default permits the District to declare Urban in default. The District shall give Urban an opportunity to cure the default within not less than 30 days unless extended

by the District ("Cure Period"). Whether to declare Urban in default is within the sole discretion of the District.

B. The District shall give Urban written notice of the default in the form of a cure notice ("Cure Notice"). The District shall also indicate any present intent it may have to terminate this Agreement, subject to Urban's right to cure. It is understood and agreed that any such decision to terminate the Agreement in whole or in part is final and effective upon giving the notice, subject to Urban's right to cure. The District may give a default notice ("Default Notice") if Urban fails to effect a cure within the Cure Period given in the applicable Cure Notice. When a Default Notice with intent to terminate is given, as provided in this paragraph, Urban must discontinue any and all work in furtherance of the Research Project, unless otherwise directed in the notice.

C. Following the giving of notice hereunder and the expiration of any Cure Period, if no adequate cure is made, the District may invoke any or all of the following remedies:
   1. Terminate this Agreement in whole or in part or any subsequent MOAs, effective at a specified time by the District;
   2. Suspend the current Research Project in whole or in part during the designated Cure Period if the default results from an action or failure to act by Urban, which affects the safety or welfare of students or District staff; and/or
   3. Receive from Urban any and all damages incurred as a result or in consequence of an Event of Default as finally determined and awarded by a court of competent jurisdiction.

D. If the District's election to terminate this Agreement for default under this paragraph is determined by a court of competent jurisdiction to have been wrongful, then in that case the termination is to be considered an early termination pursuant to Section XXIV.

XX. INDEMNIFICATION

Urban, on behalf of itself and any agents and/or contractors shall indemnify and hold harmless the District of Columbia Government, including when acting by and through OSSE, and its officers, agents and employees against any and all claims, losses, damages or liabilities, actually incurred, to which any such person may become subject, insofar as such losses, claims, damages or liabilities (or actions in respect of such losses, claims, damages or liabilities) arise out of, or are based on, the performance of this Agreement, or any alleged act or omission by Urban and its agents and/or contractors, in connection with this Agreement unless the losses, claims, damages or liabilities arise from any gross negligence or willful misconduct by the District or OSSE or any such officer, agent or employee thereof.

XXI. CONFLICTS OF INTEREST; DISCLOSURE

Urban represents and covenants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services under this Agreement. Urban further covenants not to employ any person having such known interests

in the performance of this Agreement. Urban further warrants that no amount shall be paid directly or indirectly to an employee or official of Urban, other than wages and/or compensation in the regular course of its business, in exchange for work performed in connection with any research contemplated or performed in furtherance of this Agreement. Urban further warrants and agrees that any employee, agent, consultant to, researcher for and member of Urban shall refrain from serving as a member of the Advisory Committee. Urban further warrants that any and all conflicts of interests, either actual or apparent, shall be duly disclosed to the District in a timely manner, to be determined by and between the District, through OSSE, and Urban in collaboration meetings as further set forth in Section VI. Urban will flow this requirement to the Collaborative to the extent that employees and members of the Collaborative shall refrain from serving on the Advisory Committee, in order to ensure the independence of the RPP and the research conducted in furtherance thereof.

XXII. DEBARMENT AND SUSPENSION

Urban certifies, to the best of its knowledge and belief, that it, its current and future principals, are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency.

XXIII. EFFECTIVE DATE

This Agreement shall be effective upon execution by the date of the last signatory.

XXIV. DURATION/TERMINATION

The period of this Agreement is from the date of the last signatory through September 30, 2026, unless terminated in writing by the Parties prior to the expiration, provided that the Parties shall, ninety (90) days prior to termination, engage in discussions to negotiate, renew, modify and/or extend this Agreement for an additional five (5) year term in furtherance of DC Official Code §38-785-02(b)(3).

XXV. NOTICE AND POINTS OF CONTACT

Notices required under this agreement shall be sent to the appropriate points of contact listed below.

The following individuals will serve as points of contact under this Agreement:

Office of the State Superintendent of Education
Office of the General Counsel
1050 First Street NE, 3rd Floor
Washington, DC 20002
Attn: General Counsel

Office of the State Superintendent of Education
Office of the State Superintendent
1050 First Street NE, 3rd Floor
Washington, DC 20002
Attn: Chief of Staff

Matthew Chingos
Vice President, Education Data & Policy
Urban Institute
500 L'Enfant Plaza SW
Washington, DC 20024
(202) 833-7200
MChingos@urban.org

XXVI. ENTIRE AGREEMENT AND MODIFICATIONS

This Agreement constitutes the entire agreement and understanding between the Parties. This Agreement shall supersede any prior promises, agreements, representations, undertakings or implications whether made orally or in writing between the Parties relating to the subject matter of this agreement.

The Parties hereto execute this Agreement as follows:

DISTRICT OF COLUMBIA GOVERNMENT, acting by and through the Office of the State Superintendent of Education

_____ 10/05/2021

DR. CHRISTINA GRANT
Acting State Superintendent of Education

Date

URBAN INSTITUTE

DocuSigned by:
Nani Coloretti
6DED1B34822D46D...

10/1/2021

NANI COLORETTI
Senior Vice President for Financial and Business Strategy

Date

APPENDIX A
MASTER SERVICES AGREEMENT
BETWEEN THE DISTRICT OF COLUMBIA AND
URBAN INSTITUTE
FOR EDUCATION RESEARCH PRACTICE PARTNERSHIP

RESEARCH STUDIES DSA TEMPLATE FOLLOWS THIS PAGE

EDUCATIONAL DATA ACCESS AND USE AGREEMENT
BETWEEN THE OFFICE OF THE STATE SUPERINTENDENT OF EDUCATION AND

URBAN INSTITUTE
FOR RESEARCH STUDIES

I. INTRODUCTION

This **EDUCATIONAL DATA ACCESS AND USE AGREEMENT** ("Agreement") is entered into between the **DISTRICT OF COLUMBIA, OFFICE OF THE STATE SUPERINTENDENT OF EDUCATION** ("OSSE") and URBAN INSTITUTE ("Urban"), collectively referred to herein as the "Parties".

II. BACKGROUND

OSSE is the State Education Agency (SEA) for the District of Columbia; and OSSE, as the SEA, in accordance with the Federal Family Educational Rights and Privacy Act (FERPA), and in particular 34 CFR 99.31(a)(6), is empowered to disclose educational records to educational researchers to carry out research studies for the purpose of developing, validating or administering predictive tests, administering student aid programs, and/or improving instruction. Urban is a 501(c)(3) tax exempt research organization who has partnered with OSSE through a Master Services Agreement to organize, constitute, and implement the District of Columbia Education Research Practice Partnership ("RPP"). OSSE collects educational data from publicly funded District of Columbia Local Education Agencies (LEAs) and schools and has adopted a policy and procedure for disclosure of education records to educational researchers for the purposes of carrying out permissible educational studies.

III. PROGRAM GOAL, SCOPE AND DURATION

The purpose of this Agreement is to facilitate exchange of data from education records that is necessary to further the work of Urban and the Research Practice Partnership (RPP) per the Master Services Agreement executed between Urban and OSSE on [INSERT DATE OF EXECUTION].

The RPP's work on [ENTER DESCRIPTION OF PURPOSE] requires education records currently controlled by [ENTER NAME OF EDUCATIONAL AGENCY OR INSTITUTION]. This work incorporates an Approved Research Project, titled '….', which will have a duration from [BEGINNING DATE TO END DATE]. Together, the RPP's work and associated Approved Research Project(s) will hereafter be referred to as the 'Study'.

For the furtherance of the Study and for validation purposes, Urban will retain an archive copy of the data for the duration of this Agreement not to exceed the term date identified in Section XI below.

This Educational Data Access and Use Agreement is based on the following principles:

A. The parties agree to comply with the provisions of FERPA in all respects. For purposes of this Agreement, "FERPA" includes any amendments or other relevant provisions of federal law, as well as all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations and reauthorization when effective. Nothing in this Agreement may be construed to allow either party to maintain, use, disclose or share student information in a manner not allowed by federal law or regulation.

B. In accordance with FERPA, and in particular 34 CFR 99.31(a)(3)(iv) and 99.35, OSSE is a state education authority.

This is placeholder language in the case that IDEA is implicated.

[Note: If IDEA is relevant, enter the following as paragraph C: The parties agree to safeguard and protect student records subject to this agreement in a manner consistent with confidentiality provisions contained in Part B of the Individuals with Disabilities Education Act [IDEA] 20 U.S.C. 1400, and implementing regulations 34 CFR Part 300 §§ 300.610 through 300.627.]

C. The Parties acknowledge that OSSE in its role as the State Education Agency for the District of Columbia is responsible for protecting the confidentiality of personally identifiable information in educational records and for ensuring that disclosure of such personally identifiable information complies with all applicable laws.

The Parties further acknowledge that Urban is responsible for protecting the confidentiality of personally identifiable information in educational records and for ensuring that disclosure of such personally identifiable information complies with all applicable laws in a manner consistent with and identical to OSSE's responsibilities under the law.

D. The Parties agree that the terms in this Agreement will have the definitions ascribed to them in the Family Educational Rights and Privacy Act [Pub. L. 90-247, 80 Stat. 783 (Jan. 2, 1968), as codified at 20 U.S.C. § 1232g], and the U.S. Department of Education's implementing regulations [34 C.F.R. § 99 et seq.].

IV. SCOPE OF SERVICES

A. RESPONSIBILITIES OF OSSE

1. OSSE will provide to Urban the data elements described in Appendix A, which is incorporated into this agreement by reference. Any changes made to Appendix A shall be agreed to in writing by the Parties.

B. RESPONSIBILITIES OF URBAN

1. Urban will not retain or release personally identifiable information provided by OSSE except as specifically authorized under this Agreement.

2. Urban will use and store data disclosed to Urban pursuant to this Agreement in a manner that will preserve the confidentiality of personally identifiable information.

3. Urban will not use or re-disclose data disclosed to Urban for any reasons not pursuant to the purposes of this Agreement outlined in Section III., or to any person, entity, or government agency not otherwise engaged in the furtherance of the RPP's Study. Any authorized recipients receiving re-disclosed data will be subject to the requirements of this Agreement, as well as additional restrictions and controls on their access to the data by Urban, as established by the Master Services Agreement (MSA) executed by OSSE and Urban.

4. Urban will respond within a reasonable time to OSSE's requests for any information, reports, or other assurances of Urban's ongoing compliance with this Agreement.

5. OSSE retains full ownership rights to the information in the education records it provides to Urban. Urban agrees to destroy all personally identifiable information in Appendix A:

    a. At OSSE's request in the event of a default or data incident;
    b. When the data are no longer needed to achieve this Agreement's purposes as outlined in Section III.;
    c. Upon termination of this agreement pursuant to section XI; or
    d. As otherwise required by State or Federal law.

    Urban shall confirm in writing to OSSE its compliance with the terms of this paragraph within five (5) business days of destroying the data. The written notification shall be sent to Gwen Rubinstein (Gwen.Rubinstein@dc.gov) and OSSE.datasharing@dc.gov.

6. Urban will comply with OSSE's requirements for data destruction by following the NIST Sanitization Guideline indicated within the approved data destruction plan

listed in Appendix (B) or by following a OSSE-approved unique data destruction plan listed in Appendix (B).

7. In the event of a breach of this Agreement in the form of an unauthorized re-disclosure of data that is not otherwise permissible pursuant to this Agreement, Urban must notify OSSE of the breach within 24 hours of the date on which Urban became aware of the breach. The written notification shall be sent to Gwen.Rubinstein@dc.gov and OSSE.datasharing@dc.gov. OSSE may take any actions authorized it by law to remediate the breach, including, without limitation, exclusion of Urban from future access to educational data. Failure to provide notification under this paragraph is grounds for termination of the Agreement.

8. Failure to follow the terms of this agreement may result in OSSE requiring Urban to follow a compliance plan, as defined by OSSE.

V. INSTITUTIONAL REVIEW BOARD

Urban warrants that its Study activities comply with the U.S. Department of Education's regulations governing the protection of human subjects in research found in Part 97 of Title 34 of the Code of Federal Regulations. When required by such regulations, Urban shall obtain approval from the appropriate Institutional Review Board prior to submitting the Study to OSSE for review pursuant to paragraph 6 of this Agreement.

VI. ADVANCE NOTICE OF PUBLICATION

A. At least 30 days prior to the publication of the Study, Urban shall provide an electronic copy of the Study in its final format to OSSE by emailing the Study to Gwen Rubinstein (gwen.rubinstein@dc.gov) and OSSE.datasharing@dc.gov.

B. Publication not only includes the final publication of the Study, but any release of the Study to any third party, both formally and informally.

C. OSSE shall review the advance copy of the Study for compliance with this Agreement and all applicable laws.

D. Upon completion of the compliance review in paragraph VI (C), and prior to the end of the 30-day period in paragraph VI (A), OSSE shall send Urban written notice of any identified compliance issues. Such written notice may be sent to Urban in electronic format.

E. Upon receipt of the notice identified in paragraph VI (D), Urban shall coordinate with OSSE to remediate the identified compliance issues. If the process of

remediation is not completed to OSSE's satisfaction within the 30-day period identified in paragraph VI (A), Urban shall delay publication of the Study until such time as all identified issues have been resolved to the satisfaction of OSSE.

F. Urban shall not publish any version of the Study containing information that has been identified by OSSE as noncompliant with the terms of this Agreement, relevant federal and local law and for which notice has been sent to Urban pursuant to paragraph VI (D).

VII. AUTHORITY FOR AGREEMENT

This Agreement is subject to the provisions of the Family Educational Rights and Privacy Act [Pub. L. 90-247, 80 Stat. 783 (Jan. 2, 1968), as codified at 20 U.S.C. § 1232g], and the U.S. Department of Education's implementing regulations [34 C.F.R. § 99 et seq.].

This is placeholder language in case IDEA is implicated.

[Note: If IDEA is relevant, add: Part B of the Individuals with Disabilities Education Act [IDEA] 20 U.S.C. 1400, and implementing regulations 34 CFR Part 300 §§ 300.610 through 300.627.]

VIII. COMPLIANCE AND MONITORING

OSSE may periodically monitor Urban's compliance with the terms of this agreement.

IX. INFORMATION SECURITY

The Parties to the Agreement will use, restrict, safeguard and dispose of all information related to services provided by this Agreement in accordance with all relevant federal and local statutes, regulations, policies and guidance.

The parties will adhere to generally accepted policies on information security, access and employee controls in the handling of personally identifiable confidential information. Such policies will adhere to best practices and standards within the education community related to information security and will include technical, operational and physical controls.

X. EFFECTIVE DATE

This Agreement shall be effective upon execution by the date of the last signatory.

XI. DURATION/TERMINATION

The period of this Agreement is from [date], through [date], unless terminated in writing by the Parties prior to the expiration. The Parties may extend the term of this Agreement. Such extensions shall be agreed to in writing by the Parties.

XII. NOTICE AND DATA POINTS OF CONTACT

Notices required under this agreement shall be sent to the appropriate points of contact listed below.

The following individuals will serve as data points of contact under this Agreement:

Gwen Rubinstein
Division of Data, Assessment & Research
Office of the State Superintendent of Education
1050 First Street NE, 4th Floor, Washington, DC 20002
Gwen.Rubinstein@dc.gov

[Other organization contact]
[Name of Entity]
[Contact information]

XIII. ENTIRE AGREEMENT and MODIFICATIONS

This Agreement constitutes the entire agreement and understanding between the Parties. This Agreement shall supersede any prior promises, agreements, representations, undertakings or implications whether made orally or in writing between the Parties relating to the subject matter of this agreement. The terms and conditions of this Agreement may be modified only upon prior agreement of the Parties. Such modification must be executed in writing and be signed by the duly authorized signatories of Urban and OSSE.

The Parties execute this Agreement as follows:

_____ 10/05/2021

Dr. Christina Grant, Acting State Superintendent — Date
Office of the State Superintendent of Education

_____ _____

[Signatory Authority] — Date
Urban Institute

Appendix A: List of Data Elements to be shared by OSSE

EDUCATIONAL DATA ACCESS AND USE AGREEMENT
BETWEEN THE OFFICE OF THE STATE SUPERINTENDENT OF EDUCATION AND

URBAN INSTITUTE
FOR RESEARCH STUDIES

Field #	Field	Description
1	USI	Unique 10-digit number for each student record
2	SECONDARY_ID	LEA student ID
3	SCHOOL_TYPE	DCPS or PCS
4	LAST_NAME	Student's last name
5	FIRST_NAME	Student's first name
6	MIDDLE_NAME	Student's middle name
7	GENDER	Male or Female
8	DOB	Student's Date of Birth
9	ADDRESS1	Student's address line 1
10	ADDRESS2	Student's address line 2
11	CITY	Student's city of residence
12	STATE	Student's state of residence
13	ZIP	Student's residential zip code
14	PRIMARY_SCHOOL_CODE	OSSE-assigned unique school identification number
15	PRIMARY_SCHOOL_NAME	Official state name of school
16	LEA_CODE	OSSE-assigned unique LEA identification number
17	LEA_NAME	Official state name of LEA

APPENDIX B
EDUCATIONAL DATA ACCESS AND USE AGREEMENT
BETWEEN THE OFFICE OF THE STATE SUPERINTENDENT OF EDUCATION AND
URBAN INSTITUTE
FOR RESEARCH STUDIES

DATA DESTRUCTION PLAN

The Office of the State Superintendent of Education (OSSE) requires all third parties to submit a data destruction plan as part of the process for creating data sharing agreements, in alignment with best practices recommended by the US Department of Education[1] under the Family Educational Rights and Privacy Act (FERPA).[2]

Data Sharing Agreement Expiration Date: [INSERT DATE]

Data Destruction Deadline: [INSERT DATE]

CATEGORIES OF DATA DESTRUCTION

Clear	A method of sanitization that applies programmatic, software-based techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
Purge	A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
Destroy	A method of sanitization that renders Target Data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data.

DATA STORAGE TYPES USED AND DESTRUCTION METHODS PROPOSED[3]

Data Storage Type	Data File Description	Destruction Category	Destruction definition	Additional details on methods
Office Equipment, Mobile Devices, Paper, External	Describe the categories of data that will be stored within this type (use data	Clear, Purge, Destroy, Other	Insert relevant information from Appendix A of NIST Guidelines	Please describe specifics on how data files will be removed from this media type

[1] Privacy Technical Assistance Center, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf

[2] 20 U.S.C. § 1232g; 34 CFR Part 99

[3] For reference, please apply definitions found in Appendix A of the NIST Media Sanitization Guidelines.

Locally Attached Hard Drives	appendix in MOA for reference)			

By execution of this Educational Data Access and Use Agreement, Urban certifies that that all copies of data files listed and described, in all media, and by all individuals with access, will be destroyed by the methods indicated and the date indicated on this form. In addition, Urban will submit a Certificate of Data Destruction to OSSE within five days of data destruction, as required.

APPENDIX B
MASTER SERVICES AGREEMENT
BETWEEN THE DISTRICT OF COLUMBIA AND
URBAN INSTITUTE
FOR EDUCATION RESEARCH PRACTICE PARTNERSHIP

DATA DESTRUCTION PLAN

The District of Columbia requires parties to submit a data destruction plan as part of the process for creating data sharing agreements, in alignment with best practices recommended by the US Department of Education[2] under the Family Educational Rights and Privacy Act (FERPA)(20 U.S.C. § 1232g; 34 CFR Part 99).

Data Sharing Agreement Expiration Date: September 30, 2031

Data Destruction Deadline: October 7, 2031

CATEGORIES OF DATA DESTRUCTION

Clear	A method of sanitization that applies programmatic, software-based techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
Purge	A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
Destroy	A method of sanitization that renders Target Data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data.

DATA STORAGE TYPES USED AND DESTRUCTION METHODS PROPOSED

Data Storage Type	Data File Description	Destruction Category	Destruction definition	Additional details on methods
Office Equipment, Mobile Devices, Paper, External Locally Attached Hard Drives	Describe the categories of data that will be stored within this type (use data appendix in MOA for reference)	Clear, Purge, Destroy, Other	Insert relevant information from Appendix A of NIST Guidelines[3]	Please describe specifics on how data files will be removed from this media type

[2]Privacy Technical Assistance Center, studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf

[3] For reference, please apply definitions found in Appendix A of the NIST Media Sanitization Guidelines.

By execution of this Master Service Agreement, Urban Institute certifies that that all copies of data files listed and described, in all media, and by all individuals with access, will be destroyed by the methods indicated and the date indicated on this form. In addition, Urban Institute will submit a Certificate of Data Destruction to the District within five days of data destruction, as required.

APPENDIX C
MASTER SERVICES AGREEMENT
BETWEEN THE DISTRICT OF COLUMBIA AND
URBAN INSTITUTE
FOR EDUCATION RESEARCH PRACTICE PARTNERSHIP

This checklist will help Urban and OSSE plan for monitoring of compliance with this agreement. The questions will help prepare for a review under this Master Services Agreement (MSA). Urban should use the following questions to brainstorm specific methods for demonstrating compliance with the agreement.

Agreement Requirement: In alignment with your responsibilities under the agreement, locate documentation of practices surrounding:	**Questions to Help You Prepare: These questions will help you respond to monitoring:**	**Self-Assessment: What specific documentation can you show to demonstrate compliance with this agreement? Who is responsible? Where is this document located?**
Data Retention or Release	• Have you retained or released data, including PII or PHI, beyond the scope of the agreement?	
PII and PHI Data Usage and Storage	• Are the data stored on secure servers in a secure data environment? Are the data encrypted and password protected? • Are only named individuals and roles able to securely access the data for the purpose of retention for a third-party audit? • What type of documents or logs (for example access logs, data governance meeting notes, proof of training, etc.) that could demonstrate compliance?	
Data Disclosure	• Are there documented requests to disclose or re-disclose data shared from the District beyond the purpose of the agreement, if such re-disclosures occurred?	

Proof of Data Use	• Were the data used only for the purpose for which they were shared, as described in the agreement?	
Communications	• How long did it take to respond to requests for information, reports, destruction, or other assurances from the District, if any? • Did you notify the District of any change in point(s) of contact or access or other pertinent information?	
Data Destruction	• Do the agreement terms include any interim data destruction requirements? If so, do you have proof they were followed? • If the agreement has ended, have you destroyed data received from the District under the agreement?	
Breach Notification	• How quickly did you contact the District if you became aware of any potential data breach?	
Information Security	• What polices or documentation do you have on information security, access, and employee controls in the handling of data that will demonstrate compliance? • What policies or documentation do you have of any training or education provided to employees or contractors about data privacy and security?	

APPENDIX D

MASTER SERVICES AGREEMENT
BETWEEN THE DISTRICT OF COLUMBIA AND
URBAN INSTITUTE
FOR EDUCATION RESEARCH PRACTICE PARTNERSHIP

US DEPARTMENT OF EDUCATION GUIDELINES ON DISCLOSURE AVOIDANCE FOLLOWS THIS PAGE

Privacy Technical Assistance Center

For more information, please visit the Privacy Technical Assistance Center: http://ptac.ed.gov

Frequently Asked Questions—Disclosure Avoidance

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on http://ptac.ed.gov.

Purpose

This document is intended to provide general guidance to State and local educational agencies and institutions about the best practice strategies for protecting personally identifiable information from education records (PII) in aggregate reports. The paper provides suggestions on how to ensure that necessary confidentiality requirements are met, including compliance with the Family Educational Rights and Privacy Act (FERPA). The information is presented in the form of responses to frequently asked questions (FAQs), followed by a list of additional resources at the end.

Please note that the current brief document is designed to highlight key issues surrounding the use of disclosure avoidance methods. The U.S. Department of Education plans to conduct additional training on best practices for data disclosure avoidance, which will cover specific strategies in greater depth.

FAQs: Disclosure Avoidance of Personally Identifiable Information in Aggregate Reporting

Question: *What is the definition of "disclosure" and "disclosure avoidance"?*

Answer: "Disclosure" means to permit access to or the release, transfer, or other communication of PII by any means. Disclosure can be authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party (e.g., a researcher). Disclosure can also be unauthorized or accidental. An unauthorized disclosure can happen due to a data breach or a loss (see PTAC's Data Security: Top Threats to Data Protection brief at http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf for more information and security tips). An accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified.

"Disclosure avoidance" refers to the efforts made to reduce the risk of disclosure, such as applying statistical methods to protect PII in aggregate data tables. These safeguards, often referred to as

disclosure avoidance methods, can take many forms (e.g., data suppression, rounding, recoding, etc.).

Question: *If I am only publishing aggregate data tables, do I still need to be concerned about disclosure avoidance?*

Answer: Yes. The aggregation of student-level data into school-level (or higher) reports removes much of the risk of disclosure, since no direct identifiers (such as a name, Social Security Number, or student ID) are present in the aggregated tables. Some risk of disclosure does remain, however, in circumstances where one or more students possess a unique or uncommon characteristic (or a combination of characteristics) that would allow them to be identified in the data table (this commonly occurs with small ethnic subgroup populations), or where some easily observable characteristic corresponds to an unrelated category in the data table (e.g., if a school reports that 100% of males in grade 11 scored at "Below Proficient" on an assessment). In these cases, some level of disclosure avoidance is necessary to prevent disclosure in the aggregate data table.

Question: *What legal obligation do educational agencies and institutions have to protect PII in aggregate reports?*

Answer: Under FERPA, educational agencies and institutions reporting or releasing data derived from education records are responsible for protecting PII in the reports from disclosure. The U.S. Department of Education also states, in reporting achievement results under section 1111(h) of the Elementary and Secondary Education Act of 1965, as amended (ESEA), to "not use disaggregated data for one or more subgroups… to report achievement results… if the results would reveal personally identifiable information about an individual student" and to "implement appropriate strategies to protect the privacy of individual students" (34 CFR §200.7). Further, "to determine whether disaggregated results would reveal personally identifiable information about an individual student" (34 CFR §200.7), States are instructed to follow FERPA requirements (34 CFR §99).

Question: *What issues should educational agencies and institutions consider to successfully balance privacy protection requirements with data disclosure requirements?*

Answer: Since the release of any data carries at least some element of risk, it may not possible to entirely eliminate the risk of accidental data disclosure. However, organizations disclosing the data in the form of public aggregate reports are responsible for minimizing any such risk while still meeting the disclosure requirements and providing as much useful and transparent information to the public as possible. Before each planned release of student data, an organization must determine the acceptable level of risk of disclosure. This means that in each specific case, the entity disclosing the data should evaluate the risk of PII disclosure within the context that the data will be used, and

choose a safeguard strategy that is the most appropriate for that particular context.

Question: *Is public reporting of data for small groups ("small cells") the same thing as a disclosure?*

Answer: Reporting unrounded frequency counts in small cells, such as an exact number of students in a small group, does not by itself constitute a disclosure; however, the smaller the cell size, the greater the likelihood that someone might be able to identify an individual within that cell, and thus the greater the risk of disclosure. Many statisticians consider a cell size of 3 to be the absolute minimum needed to prevent disclosure, though larger minimums (e.g., 5 or 10) may be used to further mitigate disclosure risk.

Question: *What standard is used to evaluate disclosure risk?*

Answer: The FERPA standard for de-identification assesses whether a "reasonable person in the school community who does not have personal knowledge of the relevant circumstances" could identify individual students based on reasonably available information, including other public information released by an agency, such as a report presenting detailed data in tables with small size cells (34 CFR §99.3 and §99.31(b)(1)). The "reasonable person" standard should be used by State and local educational agencies and institutions to determine whether statistical information or records have been sufficiently redacted prior to release such that a "reasonable person" (i.e., a hypothetical, rational, prudent, average individual) in the school community should not be able to identify a student because of some well-publicized event, communications, or other similar factor. School officials, including teachers, administrators, coaches, and volunteers, are not considered in making the reasonable person determination since they are presumed to have inside knowledge of the relevant circumstances and of the identity of the students.

Question: *What are some of the commonly used disclosure avoidance techniques?*

Answer: Some of the most commonly used disclosure avoidance methods include data suppression, blurring, and perturbation. When deciding which method to apply in a specific situation, it is important to evaluate the different methods in terms of their effects on the utility of the data and the risk of disclosure.

- *Suppression* involves removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This method may often result in very little data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of PII (e.g., complementary suppression of one or more non-sensitive cells in a table so that the values of the suppressed cells may not be calculated by subtracting the reported values from the row and column totals). Correct application of this technique generally results in low risk

of disclosure; however, it can be difficult to perform properly because of the necessary calculations (especially for large multi-dimensional tables). Further, if additional information related to the suppressed data is available elsewhere, the suppressed cells may potentially be re-calculated.

- *Blurring* is used to reduce the precision of the disclosed data to minimize the certainty of identification. Examples of blurring include rounding, aggregating across different populations or geographies, and reporting percentages and ranges instead of exact counts. This method may affect the utility of the data by reducing users' ability to make inferences about small changes in the data. Similarly, blurring methods that rely on aggregation across geographies or subgroups may interfere with time-series or cross-sectional data analysis. Applying this technique generally ensures low risk of disclosure; however, if any unblurred cell counts or row and/or column totals are published (or are available elsewhere), it may be possible to calculate the values of sensitive cells.

- *Perturbation* involves making small changes to the data to prevent identification of individuals from unique or rare population groups. Examples of this technique include swapping data among individual cells (this still preserves the marginal distributions, such as row totals) and introducing "noise," or errors (e.g., by randomly reclassifying values of a categorical variable). This method helps to minimize the loss of data utility as compared to other methods (e.g., compared to the complete loss of information due to suppression); however, it also reduces the transparency and credibility of the data. Therefore, perturbation is often considered inappropriate for public reporting of program data, from an accountability perspective. Applying this technique generally ensures low risk of disclosure, as long as the rules used to alter the data (e.g., the swapping rate) are protected. This requires securing the information about the technique itself as well as restricting access to the original data, so that perturbation rules cannot be reverse-engineered.

Question: *Does the U.S. Department of Education require educational agencies and institutions to use specific data disclosure avoidance techniques?*

Answer: The Department does not mandate a particular method, nor does it establish a particular threshold for what constitutes sufficient disclosure avoidance. These decisions are left up to the individual State and local educational agencies and institutions to determine what works best within their specific contexts.

As a general recommendation, in aggregate publically available reports, whenever possible, data about individual students (e.g., proficiency rates presented as cross-tabulated tables) should be combined with data from a sufficient number of other students to disguise the attributes of a single student. When this is not possible, data about small numbers of students should not be published.

Moreover, under the ESEA, each State must establish a minimum sub-group size (e.g., number of

students in a table cell) below which it will not publically report assessment data. This threshold value and other reporting rules should be specified in the documents describing the State's data reporting policies and practices implemented to protect student privacy, such as in the State Accountability Workbook (www.ed.gov/admins/lead/account/stateplans03/index.html). Minimum cell sizes adopted by the States range from 5 to 30 students, with a majority of States using 10 as their minimum (NCES 2011-603). Please note that simple suppression of small subgroups may not be sufficient to protect the privacy of all students, since the suppressed numbers can often be easily calculated by subtracting the reported subgroups' totals from the all-student totals or by comparing the school and district enrollment information. In some cases, complementary suppression of additional non-sensitive cells may be necessary.

Question: *What practical suggestions can the U.S. Department of Education provide to educational agencies and institutions to help them implement recommended disclosure avoidance techniques?*

Answer: The Department strongly suggests using a computer program to apply disclosure limitation methods, as some techniques may be difficult to implement accurately by hand. In particular, to ensure correct application of data suppression method, care should be taken when suppressing any complementary cells. Lastly, it is preferable, from a data user perspective, to apply consistent methods year to year and to use the same disclosure avoidance strategies for similar types of data releases.

Question: *Does the U.S. Department of Education intend to release more in-depth guidance on data disclosure avoidance techniques in the future? What topics will it cover?*

Answer: Yes, the Department is currently working on developing best practices for States to consider when designing and adopting their own disclosure avoidance strategies. The best practices document will review different disclosure avoidance techniques and their applicability across different contexts, and will be supplemented by examples and definitions of any relevant statistical terminology.

Additional Resources

The resources below include links to federal regulations and several guidance and best practices resources. These include some draft recommendations developed by the National Center for Education Statistics (NCES) in published Technical Briefs. While these recommendations may not be appropriate for every situation, they may provide a better understanding of the issues involved in selecting and applying disclosure avoidance methods to education data.

- *Case Study #5: Minimizing Access to PII: Best Practices for Access Controls and Disclosure Avoidance Techniques.* Privacy Technical Assistance Center (Oct 2012): http://ptac.ed.gov/sites/default/files/case-study5-minimizing-PII-access.pdf

- Code of Federal Regulations - Title 34: Education. *Disaggregation of data*. 34 CFR §200.7: www.gpo.gov/fdsys/pkg/CFR-2011-title34-vol1/pdf/CFR-2011-title34-vol1-sec200-7.pdf

- FERPA regulations, U.S. Department of Education: www.ed.gov/policy/gen/reg/ferpa

- *FERPA regulations amendment*.U.S. Department of Education (December 9, 2008): www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf

- *FERPA regulations amendment*. U.S. Department of Education (December 2, 2011): www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

- *Frequently Asked Questions—Disclosure Avoidance.* Privacy Technical Assistance Center (Oct 2012): http://ptac.ed.gov/sites/default/files/FAQs_disclosure_avoidance.pdf

- Privacy Technical Assistance Center (PTAC), U.S. Department of Education: http://ptac.ed.gov

- *SLDS Technical Brief 3: Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting* (NCES 2011-603): http://nces.ed.gov/pubs2011/2011603.pdf

- *Statistical Policy Working Paper 22 - Report on Statistical Disclosure Limitation Methodology.* Federal Committee on Statistical Methodology, Office of Management and Budget (1994): http://fcsm.gov/working-papers/wp22.html

- *Technical Brief: Statistical Methods for Protecting Personally Identifiable Information in the Disclosure of Graduation Rates of First-Time, Full-Time Degree- or Certificate-Seeking Undergraduate Students by 2-Year Degree-Granting Institutions of Higher Education* (NCES 2012-151): http://nces.ed.gov/pubs2012/2012151.pdf

Glossary

Education Program is defined as any program principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Education records means records directly related to a student and maintained by an educational agency or institution, or by a party acting on behalf of the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Personally identifiable information (PII) from education records includes information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

APPENDIX E
MASTER SERVICES AGREEMENT
BETWEEN THE DISTRICT OF COLUMBIA AND
URBAN INSTITUTE
FOR EDUCATION RESEARCH PRACTICE PARTNERSHIP

OSSE STUDENT DATA SUPPRESSION POLICY FOLLOWS THIS PAGE

DISTRICT OF COLUMBIA
OFFICE OF THE STATE SUPERINTENDENT OF
EDUCATION

STUDENT PRIVACY AND DATA SUPPRESSION POLICY

Effective November 2020

I. Authority	The Office of the State Superintendent of Education (OSSE) collects, analyzes, stores, and reports on many public data. OSSE has the authority to adopt and implement policies that increase the security of these data. As a state education agency (SEA), OSSE has a responsibility to apply data suppression to remove identifiable information from data releases under the federal Family Educational Rights and Privacy Act (FERPA)[1], As the lead state agency for early learning services, OSSE has similar responsibilities under Parts B and C of the Individuals with Disabilities Education Act (IDEA) [2]. Further, as any data release carries some level of risk of disclosure, and no method of suppression can completely eliminate risk, SEAs must assess the level of disclosure risk and evaluate that risk against FERPA's confidentiality standard. This standard prohibits the release of information that would permit a "reasonable person in the school community… to identify [an individual] within reasonable certainty."[3]
II. Applicability	This policy applies to all FERPA and IDEA protected data as well as other student data which OSSE releases publicly or to parties as requested, including instances under data sharing agreements unless otherwise negotiated. OSSE will apply this policy to data releases and data sharing agreements from the date of publication of this policy. Some though not all historical files may be updated to meet this standard. This policy will undergo periodic review to ensure all standards remain applicable to OSSE's data practices. OSSE reserves the right to update this policy based on these reviews.
III. Rationale	This policy aligns the agency with the best practices under FERPA. In doing so, this policy will strengthen OSSE's internal data protection and privacy practices by setting requirements about the methods for and full scope of verifiable data suppression for all data released by OSSE. In creating this policy, OSSE aims to balance the values of public transparency, student privacy, equity in reporting and consistency of practice throughout all data releases.
V. Policy	OSSE will apply consistent suppression rules to all published data files unless noted as an exception per Section VII below. The suppression rules listed below will be applied in the order listed. 1. Denominators less than 10 and their corresponding percentages shall be reported

[1] Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
[2] Individuals with Disabilities Education Act (IDEA) (20 U.S.C. § 1400 et seq.)
[3] United States Department of Education, Office of Management letter to Louisiana Department of Education, April 2016

as n<10.

2. Data shall be top- and bottom-coded variably based on the denominator according to the table below. This provides the greatest amount of information while protecting personally identifiable information.

Denominator	Suppression level
10-20	<=10% and >=90%
21-100	<5% and >95%
101-1000	<1% and >99%
1001+	<.1% and >99.9%

3. In instances in which both the numerator and denominator are reported and the percentage (whether or not that percentage is reported in the file) would be top- or bottom-coded (e.g., 99.5% with a denominator of 150), OSSE shall suppress the numerator (i.e., "DS"), leave the denominator unsuppressed, and top- or bottom-code the related percentage. If only the denominator and percentage are reported, then data shall be top- and bottom-coded as outlined in (2) and the denominator shall not be suppressed.

4. Data shall be complementarily suppressed (denoted as "DS") in instances in which cells would be able to be identified by subtracting one or more subtotals from a total. The “DS” shall be applied to the cell with the next smallest denominator (or to multiple cells as required).

IV. Definitions

Blurring:

- A method of suppression that involves reducing the precision of the disclosed data to minimize identification. Examples include rounding, aggregating across different populations or geographies, and reporting percentages in ranges instead of exact counts.[4]

Bottom Coding:

- Suppress with a bottom-code; is a lower limit on all published values for a variable. [5]

Complementary Suppression/Dual Suppression:

- To reach the desired protection for risky cells, it is necessary to suppress additional non-risky cells, which is called dual suppression or complementary suppression. OSSE inserts “DS” to denote any instance of this method.[6]

Data:

- Expressed information representing facts in a variety of qualitative and quantitative forms, including aggregate, individual level, and personally identifiable information.

Data Release:

- Publication of aggregate data accessible to the public.

Data Sharing Agreement:

- Data sharing agreements are legal documents between two or more parties that codify the terms and conditions for the sharing and use of data. OSSE requires written

[4] PTAC “Data De-identification: An Overview of Basic Terms” https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf

[5] SLDS Technical Brief “Statistical methods for Protecting Personally Identifiable Information in Aggregate Reporting”

[6] PTAC “Frequently Asked Questions- Disclosure Avoidance” https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FAQs_disclosure_avoidance.pdf

	agreements when sharing personally identifiable information from education records with third parties. **Disclosure:** • A disclosure, permitting access to or the release, transfer or other communication of personally identifiable information contained in education records by any means.[7] **Minimum n-size:** • To have a minimum sample size; The minimum number (n) of students necessary to publish a student subgroup without jeopardizing privacy.[8] **Personally Identifiable Information (PII):** • PII is information that, alone or in combination with other data, can be linked to a specific student, including but not limited to:[9] o Name of student, parents, or other family members; o Address of student, parents, or other family members; o Personal identifier, such as a Social Security Number, unique student identifier (such as OSSE's USI), or biometric record; and o Indirect identifiers, such as date of birth, place of birth, or mother's maiden name. **Suppression:** • When releasing aggregate data, withholding or removing select data from a cell to prevent the identification of individuals in small counts, typically based on n-size. [10] **Top Coding:** • Suppress with a top-code for a variable; is an upper limit on all published values of that variable. [11]
VI. OSSE Expectations for Data Suppression Review	OSSE expects all publicly released data and reports to go through a thorough Quality Assurance process to ensure the data suppression applied meets the standards stated in this policy as part of the existing technical quality assurance process. This expectation applies to any third party releasing data on behalf of OSSE as well as any internal release. OSSE staff can reference internal guidance for futher information on this process.
VII. Exceptions	OSSE reserves the right to allow exceptions to this policy to maintain an appropriate balance of transparency and privacy in circumstances where the general policy does not do so. As a standard exception, basic school and school district enrollment counts, disaggregated by gender and race/ethnicity are excluded from this policy. Any other exceptions will be noted in OSSE Student Privacy and Data Suppression Policy Exceptions and within the data notes tab for the specific file upon publication, where applicable.
IX. Further Information	For more information on this policy, please contact Jenny Sanchez at Jennifer.Sanchez@dc.gov and (202) 899-6135.

[7] SLDS Technical Brief "Statistical methods for Protecting Personally Identifiable Information in Aggregate Reporting"
[8] DQC "Understanding Minimum N-Size and Student Data Privacy: A Guide for Advocates"
[9] Privacy Technical Assistance Center, http://ptac.ed.gov/glossary/personally-identifiable-informationeducation-records
[10] PTAC "Data De-identification: An Overview of Basic Terms"
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf
[11] SLDS Technical Brief "Statistical methods for Protecting Personally Identifiable Information in Aggregate Reporting"

APPENDIX F
MASTER SERVICES AGREEMENT
BETWEEN THE DISTRICT OF COLUMBIA AND
URBAN INSTITUTE
FOR EDUCATION RESEARCH PRACTICE PARTNERSHIP

Process of Collaboration

Pursuant to Section VI of this Agreement, this Appendix establishes details on various process of collaboration in which Urban and the District will engage. These protocols are anticipated to evolve as the RPP matures, and this Appendix will be renegotiated at least annually unless otherwise agreed to by the Parties.

A. Period: This Appendix covers the period beginning on the date of execution of the Agreement and will last for 12 months.
B. Meetings:
    i. Urban and OSSE will meet regularly, unless both Parties agree to cancel an instance of a meeting.
    ii. OSSE will manage and initiate these meetings in an attempt to ensure alignment on data access and needs by both the District and the RPP.
    iii. Meetings will be held virtually until and unless the Public Health Emergency permits in person convenings and both Parties agree to do so
    iv. Meeting agenda items will be solicited in advance from Urban and the complete agenda will be shared at least 48 hours in advance of the meeting
        1. Standing agenda items will include reporting as described in Section C below, and updates on technical means and methods.
C. Reporting:
    i. Urban shall report to OSSE on:
        1. The status of proposed and approved research projects, including timelines and anticipated review deadlines
        2. The status of review of in-process MOAs
        3. The status of or changes to RPP/Collaborative structure
        4. The status of the technology development in Urban's environment to store District data
    ii. OSSE shall report to Urban on
        1. The status of in-process MOAs
        2. The status of any in-process research compliance review
D. Technical means and methods
    i. Upon completion of a data sharing MOA for an approved research project, OSSE will initiate the technical process of sharing data by secure means:
        1. OSSE will upload files with relevant data notes included

2. OSSE will grant access to a specified Urban representative to download these data and load into Urban's technology environment
3. OSSE will inform Urban when the data are available
4. Urban will inform OSSE that they have successfully accessed the files

ii. Upon receipt of the data, Urban takes full responsibility for the stewardship and protection of these data as described in this Agreement and in the associated data sharing MOA.