The Measures of Effective Teaching Longitudinal Database
Data Access Plan
August 12, 2012

Purpose

This document describes the content from the MET project that will be housed in the MET Longitudinal Database, the processing that will occur to those data prior to being made available, the disclosure risk evaluation and protections taken, and the tools that will be used for disseminating the data and to whom. These procedures are designed to allow the research community to maximize the analytical value of the MET Longitudinal Database while providing the strongest possible protections for subjects described in the data.

Background

In 2011, the Bill & Melinda Gates Foundation awarded the University of Michigan a grant to build the Measures of Effective Teaching (MET) Longitudinal Database (LDB). The University of Michigan was tasked with acquiring all of the MET data collection including the video classroom observation sessions and their accompanying metadata and artifacts, the multiple sets of scores for the observation sessions, the student supplemental assessment data, and the various survey collections. The University of Michigan was asked to provide researchers secure access to this rich data set to allow for further analysis on effective teachers and teaching beyond the initial project's research questions and to digitally preserve the collection.

The MET Longitudinal Database project will preserve MET data and provide a web-based access tool that allows authorized researchers to utilize a wide variety of MET data files to conduct IRB- approved research studies. The University of Michigan is committed to a comprehensive approach to protecting data, including both legal and technical safeguards. The Inter-university Consortium for Political and Social Research (ICPSR), which will archive and disseminate the MET data, has systems and protocols to ensure data security and minimize disclosure risk.[1]

Access

The MET Longitudinal Database will be available:
- To academic researchers
- Under a customized restricted-use data agreement signed by an authorized official at the researcher's institution (See Appendix I Restricted-Use Data Dissemination Agreement Between School Districts and ICPSR/University of Michigan, Appendix A Restricted Data Use Agreement)
- For research purposes approved by an ethical review board
- Through secure remote access (i.e. researcher will not receive a copy)
- Under threat of severe professional sanctions applied to research misconduct, such as the violation of confidentiality of research subjects.

---

[1] Disclosure risk is the possibility that sensitive data can be linked to a specific person or organization, revealing information about the subject that otherwise would not be known or known as fully.

Researchers must file plans with an ethical review board (e.g. IRB) and agree to data security and disclosure prevention techniques. The contracting process requires interested data users to provide a research plan, IRB approval or a formal waiver, curriculum vitae for the principal investigators, and signed pledges of confidentiality from each research team member. The data user's institution and the University of Michigan are bound to contractual obligations through a signed, finalized agreement. Access to the restricted-use quantitative and video data is thus dependent on a user having an approved and valid agreement. The restricted-use data agreement obligates the researcher's institution to impose severe sanctions if terms of the agreement are violated.

Quantitative data in the MET Longitudinal Database will be accessed by approved researchers through a Virtual Data Enclave (VDE), which is similar to the environment used by ICPSR data processors. After authentication, the VDE presents the user a complete desktop operating system, which is running on a server at University of Michigan. The VDE desktop opens in a window on the user's desktop, but the two systems (VDE and user's local desktop) are completely independent of and separate from each other. Files cannot be moved across systems. Users working in the VDE cannot download the data files; cannot copy and paste files to another location; can only access restricted files when logged onto the ICPSR secure system; can only access the system via approved IP addresses; can only access a designated suite of programs; and can receive only printouts or results that have been reviewed for disclosure risk. All files created within the VDE will be subject to review for disclosure risk before delivery to the researcher outside the VDE and researchers are only able to remove data analysis, not actual data. Also, researchers will only receive access to data they need to conduct the research in their application. If a researcher does not need access to the videos, the videos will not be provided to them.

The video data in the MET Longitudinal Database will be accessed by approved researchers through a web-based, secure access, video streaming application, using standard formats and open-source web application technologies. This application will allow for searching, browsing, and playback of available MET videos. Users will not be able to download or cache the videos, and resource location information will be hidden. Authenticated users can search and browse the video collection and view selected videos and accompanying metadata and artifacts in this secure environment.

MET Longitudinal Database (LDB) Content

Quantitative Data
We propose to include the following types of data in the database: teacher-level files including demographic characteristics, survey results, and pedagogical knowledge assessment results; section-level (classroom-level) files including state and supplemental assessment results, video scoring results, and computed value-added measures; student-level files including demographic characteristics, survey results, and assessment results; videos from all teachers providing supplemental consent, and principal survey results.

Data Processing Procedures
All data are handled in a secure computing environment. The data are transferred securely to ICPSR via encrypted removable media, a custom-built electronic deposit system, or other

secure file transfer protocols. The data are placed directly into a secure, virtual computing environment. This work area is restricted to authorized data processors, who can access but cannot remove data (e.g. email and local disk drives are not accessible from this environment).

Once the quantitative data are received, the University of Michigan team will review the files to ensure data assets are complete, accurate, readable, and usable for secondary analysis. In addition, this process will assure that respondent confidentiality is protected. Major data processing steps include:
- Evaluating extant file structures and defining study and data file structures
- Checking data against documentation to assure completeness of files, protect against wild codes, document missing codes, and document any problems if discovered
- Checking for confidential information contained within the quantitative data, and transforming data to prevent disclosure while maintaining data integrity
- Creating data definition fields, such as variable and value labels
- Standardizing missing data codes
- Performing quality control checks, including consistency of responses and skip patterns;
- Resolving data and documentation issues in consultation with MET Partners
- Making appropriate adjustments to the quantitative data to produce final data files
- Producing archival and dissemination files.

Identification fields will be unique to the LDB, and they will not match IDs in external or operational databases. Internal LDB IDs will allow data to be linked across instruments within the LDB. For example, videos may be linked to survey data describing the same teacher. The LDB will allow linkage by teacher, section, school, district, observation session and student. The University of Michigan will receive all of the original field operational IDs, use them to ensure proper linking across files, and then will replace all of the field operational IDs with MET LDB specific IDs that will be used in the LDB version of all files. Researchers will never have access to the original IDs.

By the end of the process, ICPSR staff will produce a full suite of quantitative data and documentation files including raw data (ASCII) files, data definition statements compatible with the most popular statistical analysis packages (i.e., SPSS, SAS and Stata) and system files for each of these packages. Documentation will also provide users with instructions on the use of ASCII files in the software package "R". Complete data documentation ("codebooks") will be produced in PDF format and will include detailed information on each variable (e.g., variable name and label, value labels, question text, universe statements, and missing data definitions) as well as displays of univariate frequency distributions.

Disclosure Protections for Quantitative Data
ICPSR will assure that all direct identifiers[2] are removed from the MET LDB. Each dataset will also be evaluated for indirect identifiers[3] that may be used in combination to re-identify a unique individual. The risk of re-identification may be minimized by removing or recoding (coarsening) dates, geographic locations, and values with small counts. In some cases, random

---

[2] Direct identifiers include name, address, Social Security Number, telephone and/or FAX numbers, employee ID number, driver license number, email address, medical record numbers, biometric identifiers, photographs, audio and/or video files, other linkable data.
[3] Indirect identifiers include sex, race, age, income, employment, family size, or other demographic data.

noise may be added to numeric variables or values may be swapped across cases to make it more difficult to match known characteristics of individuals (students, teachers, schools) to their representations in the dataset. Decisions to alter the data in these manners will be made in consultation with the project PIs and project officers at the Bill & Melinda Gates Foundation.

LDB Video Collection

Protocols for Teacher-supplied Videos
Classroom videos for the MET project were collected under protocols designed to protect the rights and confidentiality of teachers and students. Before video capture began, agreement to participate was requested from teachers and the parents of students through IRB-approved informed consent forms and letters. Informed consent procedures were administered by school districts and differed among districts. Since the informed consent statement for teachers did not clearly include future dissemination of the videos, teachers are being asked to sign a second informed consent agreement for this phase of the project allowing their videos to be included in the MET database and used for approved research purposes. Only videos with appropriate consent will be made available to researchers.

Documents and training provided to teachers and School Project Coordinators (SPC) throughout MET data collection emphasized the importance of informed consent and processes to accommodate non-consented students.
- Teachers were given talking points to use when discussing the video capture process with their students ("MET Project Video Teacher Resources: Talking With Students About Video Capture"). Students were told not to use any full names during filming to protect the privacy of their classmates, and teachers described procedures for concealing students whose parents did not want them to be filmed.
- The panoramic camera included a privacy device that blocked thirty degrees of the camera's field, and students without consent were seated in this area. SPCs were instructed on the use of this device, as well as on camera positioning for both panoramic and handheld cameras to ensure non-consented students were not seen on camera ("Video Plus Capture Protocols").
- Before a video capture session could begin, the software attached to the camera rig required the SPC to confirm that protocols to protect students who did not consent to video capture were being followed ("MET Project Video QuickGuide: Performing a Video Capture").
- After filming, videos were uploaded to a secure MET project website to await teacher approval. Teachers were instructed to review each video, answer questions about the video, and upload related documents. If a non-consented student was inadvertently filmed, the teacher was asked to flag the video to prevent it from being used. Videos were not released for project use until they were submitted by the teacher through this online system ("MET Project Video Teacher Resources: MET Project Video Teacher Overview").

Evidence in the videos themselves suggests that appropriate measures were followed to protect students who did not consent to be filmed. Staff at the University of Michigan School of Education are currently reviewing the videos that will be used in the LDB. Among approximately 5800 lessons reviewed so far, 423 used the privacy device to block a section of

the classroom from the panoramic camera. A number of videos include conversations in which the teacher is positioning a student to be in the area concealed from the camera. Reviewers have also noticed 32 videos in which the camera was running before or after a lesson and captured students from a different class. These videos are being flagged for editing, and the affected portion will be removed.

Processing Procedures

The video collection will include all videos that pass the quality checking process. All complete video captures of a classroom observation will be quality checked. These include both the videos that were scored as well as those that were not. Quality checks are performed on video, audio, metadata and artifact quality before videos are included in the Longitudinal Database. Each video will have the following metadata: focal topic, subject, grade, district ID, date created, duration, teacher ID, session ID, school ID, and period. Researchers will be able to search and browse these dimensions to discover relevant videos.

The MET Project video files delivered to ICPSR contain the UUID in their names. Each video file name consists of the UUID followed by an underscore, followed by either a "b" (blackboard) or a "p" (panorama), followed by a standard file extension (mp4). Prior to storing the files in Archival Storage ICPSR will rename each file, substituting a seemingly random string of characters for the UUID. The pseudo-random characters will be derived from the video content, not the UUID, and it will be impossible for anyone outside of ICPSR to map a file name to a UUID.

Dissemination Schedule

The MET Longitudinal Database will be opened to researchers in three phases. First, data will be made available to the MET Project research partners, who collected the MET data and are in the process of conducting the original planned analyses. Second, a limited group of researchers will be allowed to compete for grants to use the MET LDB. The competition for these grants will be announced in summer 2012. As part of their data access agreements, these initial user groups will provide feedback to help the University of Michigan development team improve the LDB system. In the third phase, the LDB will become available to all qualified researchers subject to the requirements described above. Expanded access is expected to begin in September 2013.

Appendix I
Restricted-Use Data Dissemination Agreement Between School Districts and
ICPSR/University of Michigan

THE <ORGANIZATION NAME>
AND
THE REGENTS OF THE UNIVERSITY OF MICHIGAN on behalf of the
MEASURES OF EFFECTIVE TEACHING LONGITUDINAL DATABASE,
INTER-UNIVERSITY CONSORTIUM FOR POLITICAL AND SOCIAL RESEARCH

RESTRICTED-USE DATA DISSEMINATION AGREEMENT

This Agreement, dated as of the _____ of _____, 2013 by and between <Organization Name>, having an office at <full address of organization> and the REGENTS OF THE UNIVERSITY OF MICHIGAN (MICHIGAN) on behalf of the MEASURES OF EFFECTIVE TEACHING LONGITUDINAL DATABASE, INTER-UNIVERSITY CONSORTIUM FOR POLITICAL AND SOCIAL RESEARCH, having its principal place of business at The University of Michigan, Institute for Social Research, 1131 Perry Building , (330 Packard Street), Ann Arbor, Michigan, 48106-2321, defines the terms of the confidential relationship between the aforementioned parties.

WITNESSETH:

WHEREAS the Inter-university Consortium for Political and Social Research (hereinafter referred to as ICPSR) is a member-based consortium that provides data archiving services;

WHEREAS the Measures of Effective Teaching (hereinafter referred to as MET) Longitudinal Database is a project funded by the Bill & Melinda Gates Foundation at ICSPR that acquires all of the MET data collection including the video classroom observation sessions and their accompanying metadata and artifacts, the multiple sets of scores for the observation sessions, the student supplemental assessment data, and the various survey collections (MET Data);

WHEREAS <Organization Name> has provided MET Data and related documentation to Michigan for the purpose of allowing MICHIGAN to distribute the materials as described in a separate Restricted Use Data Transfer and Processing Agreement;

NOW, THEREFORE, for and in consideration of the premises and mutual promises and benefits set forth herein, the parties hereto hereby agree as follows:

1.   Definitions.

a. MET DATA. As used herein, "MET Data" shall mean the data received from RAND Corporation now and in the future,<Organization> consisting of student administrative and assessment data and teacher administrative data;

b. THIRD-PARTY USER. As used herein, .

c. RESTRICTED DATA USE AGREEMENT. As used herein, "Restricted Data Use Agreement" shall mean the use agreement, appended to this Agreement as Appendix A, made between MICHIGAN and a third-party user to give the third-party user access to the MET Data.

2.   Purpose of Data Transfer.

A copy of the MET Data is being provided on a non-exclusive basis to MICHIGAN for the purpose of making the data available to third-party users under the terms of the Restricted Data Use Agreement attached as Appendix A.

3.   Terms of Data Deposit.

a. <Organization Name> agrees to provide a copy of the MET Data related documentation to MICHIGAN solely for the purposes described in this Agreement; MICHIGAN does not acquire any ownership in or rights to the dataset hereby but is permitted to use the data in order for MICHIGAN to carry out its obligations hereunder.

b. <Organization Name> shall notify MICHIGAN of any conditions imposed by <Organization Name>'s Institutional Review Board (IRB) with regard to the MET Data and the deposit thereof with MICHIGAN. Upon notice by <Organization Name> to MICHIGAN, all such conditions shall be become incorporated into this Agreement. Should MICHIGAN be unable or unwilling to agree to such conditions, or violate the terms thereof, this Agreement shall terminate.

c. Ownership of Data. <Organization Name> has implicit and explicit copyright to the MET Data and has the right to make it available through MICHIGAN. <Organization Name> retains ownership of the MET Data and retains full rights to use and distribute the MET Data.   This Agreement does not preclude the release of the MET Data in other instances by <Organization Name>.

d. MICHIGAN may not alter the MET Data except for the limited purposes of standard MET data processing and protecting confidential information; MICHIGAN may not transform, modify, edit, alter, or produce new variables or combine the MET Data with any other datasets or in any manner change the dataset in any other way without the express written authorization of <Organization Name>.

e. MICHIGAN may release the MET Data or files derived therefrom to third-party users only under the terms of a Restricted Data Use Agreement, an agreement between MICHIGAN and a third-party user (See Section 4 below and Appendix A);

4.   Maintenance and Enforcement of MICHIGAN Restricted Data Use Agreement.

a. MICHIGAN hereby agrees that it will maintain in confidence the MET Data with the same degree of care that MICHIGAN uses under routine MICHIGAN procedures for restricted-use classification. MICHIGAN may not disclose the MET Data to any third-party user except through a Restricted Data Use Agreement.

b. MICHIGAN will administer the MET Data Restricted Use Agreement between MICHIGAN and third-party users, to include determination of third-party user and institutional eligibility, communication with third-party users, and enforcement of the restricted-use policies, as described in the Restricted Use Agreement. <Organization Name> will not participate in the administration of the Restricted Data Use Agreement, except in cases where MICHIGAN has notified <Organization Name> of a breach of a MET Data Restricted Use Agreement.

c. <Organization Name> will not provide direct assistance to third-party users with respect to the MET Data; <Organization Name> will communicate with MICHIGAN to answer third-party user questions related to the MET Data and format, but not questions related to MET Data interpretation and secondary analysis. <Organization Name> reserves the right to decline to address any question(s).

d. MICHIGAN will alert <Organization Name> in the event that a Restricted Use Agreement is breached by a third-party user. <Organization Name> reserves the right to take action against a third-party user if MICHIGAN, <Organization Name>, or other parties have identified a breach of a MET Data Restricted Use Agreement, whether or not MICHIGAN takes action against the third-party user.

e. MICHIGAN, to the extent allowed by the law, indemnifies and will hold <Organization Name> harmless for any disclosure of the MET Data by MICHIGAN unless expressly authorized by the terms of this Agreement. MICHIGAN shall not use or disclose the MET Data received from or on behalf of <Organization Name> except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by <Organization Name>. In the event that MICHIGAN should receive a request or demand, including by means of subpoena or other legal process for any or all of the MET Data, or seeking information of whatever nature regarding this Agreement, the MET Data, or any third party-user having entered into or who has sought to enter into a third-party Restricted Use Agreement, MICHIGAN shall immediately notify <Organization Name> thereof and give <Organization Name> the opportunity to oppose such request or demand.

5.   Term of Obligations. All obligations under this Agreement shall be perpetual. <Organization Name> intends for MICHIGAN to: 1) preserve the MET Data in the MICHIGAN repository in perpetuity and 2) disseminate the MET Data to users under a Restricted Data Use Agreement. However, <Organization Name> or MICHIGAN may cancel this agreement with written notice. In the event of cancellation by <Organization Name> or MICHIGAN, MICHIGAN will immediately cease dissemination of the MET Data and terminate all Restricted Use Agreements involving the MET Data, allowing three months after written notification of cancellation to provide time for current third-party users of the MET Data to be notified and to return the MET Data, as outlined in the Restricted Use Agreement.

6.   Remedies. MICHIGAN agrees that the disclosure of the MET Data outside of the Restricted Use Agreement and without <Organization Name>'s express written consent may cause <Organization Name> irreparable harm and that any breach or threatened breach of this Agreement by MICHIGAN may entitle <Organization Name> to seek injunctive relief, in addition to any other legal or equitable remedies available to it in any court of competent jurisdiction.

7.   Entire Agreement/Amendments/Waiver. Each party agrees that this written Agreement embodies the entire understanding between <Organization Name> and MICHIGAN and supersedes and replaces any and all prior understandings, negotiations, arrangements, and agreements, whether oral or written, relating to such MET Data. No amendment or modification of this Agreement shall be effective unless made or agreed to in writing by authorized representatives of both parties hereto. Failure by either party hereto to enforce any rights under this Agreement shall not be construed as a waiver of such rights nor shall a waiver by either party hereto in one or more instances be construed as constituting a continuing waiver or as a waiver in other instances.

8.   Governing Law. This Agreement shall be governed by, interpreted, enforced and construed in accordance with the laws of the State of Michigan.

9.   Headings/Counterparts. The headings in this Agreement are for convenience of reference only and shall not affect its interpretation. This Agreement and any amendment hereto may be executed in counterparts and all such counterparts taken together shall be deemed to constitute one and the same instrument.

FOR <Organization Name>:   FOR MICHIGAN:

By:_____   By:_____

Title:_____   Title:_____

Date:_____   Date:_____

10

APPENDIX A

Restricted Data Use Agreement

The Restricted Data Use Agreement, appendices, and attachments are completed through ICPSR's online data access request system. This Appendix comprises the legal text needed as part of the Restricted Use Data Dissemination Agreement.

Inter-university Consortium for
Political and Social Research P.O.
Box 1248
Ann Arbor, Michigan 48106
www.icpsr.umich.edu

**Agreement for the Use of Confidential Data
from the
Measures of Effective Teaching Longitudinal Database
at the
Inter-university Consortium for Political and Social Research (ICPSR)**

I. DEFINITIONS

A. "Investigator" is the person primarily responsible for analysis and other use of Confidential Data obtained through this Agreement.

B. "Research Staff" are persons authorized by the Investigator's institution, excluding the Investigator, who will have access to Confidential Data obtained through this Agreement. Research Staff include project staff or students conducting dissertation or thesis research.

C. "Participants" are persons, other than Investigator and Research Staff, who will be provided access to Confidential Data by the Investigator. For example, research subjects who will view videos included in the Confidential Data as part of an IRB approved research protocol are Participants for this agreement. Institution is responsible for ensuring Participant compliance with all aspects of this agreement.

D. "Institution" is the university or research institution at which the Investigator will conduct research using Confidential Data obtained through this Agreement.

E. "Representative of the Institution" is a person authorized to enter into contractual agreements on behalf of Investigator's Institution.

F. "Confidential Data" consist of data, images, videos and any objects derived from them with information that is linkable to a specific individual either directly or indirectly, and for which the individual (whether a person or organization) has the expectation that the information will not be released in a manner allowing public identification of the individual or causing some harm to the individual.

G. "Private Person" means any individual (including an individual acting in his official capacity) and any private (i.e., non-government) partnership, corporation, association, organization, or entity (or any combination thereof), including family, household, school, neighborhood, health service, or institution.

H. "ICPSR" is the Inter-university Consortium of Political and Social Research.

I. "Restricted Data Contracting System" ("RDCS") is the web-based system for data contracts at ICPSR.

J. "Data Security Plan" is a component of this Agreement, found as Attachment A, which specifies permissible computer configurations for use of Confidential Data through Investigator responses to a series of questions, and records what the Investigator commits to do in order to keep Confidential Data secure.

K. "Deductive Disclosure" is the discerning of an individual's identity or confidential information through the use of known characteristics of that individual. Disclosure risk is present if an

unacceptably narrow estimation of an individual's confidential information is possible or if determining the exact attributes of the individual is possible with a high level of confidence.

L. "Derivative" is a file, video, image, or statistic derived from the Confidential Data that poses disclosure risk to any Private Person in the Confidential Data obtained through this Agreement. Derivatives include copies of the Confidential Data received from ICPSR, subsets of the Confidential Data, and analysis results that do not conform to the guidelines in Section VI.G.

II. DESCRIPTION OF DISCLOSURE

Deductive disclosure of an individual's identity from research material is a major concern of federal agencies, researchers, and Institutional Review Boards. If a person is known to have participated in ANY study or if information is known to be included in files or a database from which the Confidential Data were obtained, then a combination of his or her personal characteristics may allow someone to determine which record corresponds to that individual. Investigators and Institutions who receive any portion of Confidential Data are obligated to protect the individual's confidential information from deductive disclosure risk by strictly adhering to the obligations set forth in this Agreement and otherwise taking precautions to protect the Confidential Data from non-authorized use.

III. REQUIREMENTS OF INVESTIGATORS

A. Investigators must meet the following criteria:

      1. Have a PhD or other terminal degree; and

      2. Hold a faculty appointment or research position at Institution.

B. The Investigator assumes the responsibility of completing the RDCS online application and required documents, reports, and amendments. The Investigator agrees to responsibly manage and use Confidential Data and implement all Confidentiality Data security procedures per the Data Security Plan.

C. The Investigator will provide ICPSR any publications or public presentations derived from the Confidential Data.

IV. REQUIREMENTS OF INSTITUTION

The Institution must meet the following criteria:

A. Be an institution of higher education, a research organization, a research arm of a government agency, or a nongovernmental, not for profit, agency.

B. Have a demonstrated record of using Confidential Data according to commonly accepted standards of research ethics and applicable statutory requirements.

V. OBLIGATIONS OF ICPSR

In consideration of the promises made in Section VI of this Agreement, ICPSR agrees to:

A. Provide access to the Confidential Data requested by the Investigator in the Confidential Data Order within a reasonable time of execution of this Agreement by appropriate ICPSR officials. Quantitative Confidential Data will be made available via the Virtual Data Enclave, a secure remote-access work space. Video files and accompanying metadata will be made available via the MET LDB online secure streaming system. Access to both requires proper authentication. ICPSR will provide instructions on establishing user accounts within a reasonable amount of time after the execution of the agreement.

B. Provide electronic documentation of the origins, form, and general content of the Confidential Data, in the same time period and manner as the Confidential Data.

ICPSR MAKES NO REPRESENTATIONS NOR EXTENDS ANY WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED. THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE USE OF THE CONFIDENTIAL DATA WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS. Unless prohibited by law, Investigator and Institution assume all liability for claims for damages against them by third parties that may arise from the use or disclosure of the Confidential Data.

VI. OBLIGATIONS OF INVESTIGATOR, RESEARCH STAFF, AND INSTITUTION

Confidential Data provided under this Agreement shall be accessed by the Investigator, Research Staff, Participants, and Institution in strictest confidence and can be disclosed only in compliance with the terms of this Agreement. In consideration of the promises in Section V of this Agreement, and for use of Confidential Data from ICPSR, the Investigator, Research Staff, Participants, and Institution agree:

A. That the Confidential Data will be used solely for research or statistical purposes relative to the research project identified on the Application for Obtaining Confidential Data accompanying this Agreement, and for no other purpose whatsoever without the prior consent of ICPSR. Further, no attempt will be made to identify private persons, no Confidential Data of private person(s) will be published or otherwise distributed, and Confidential Data will be protected against deductive disclosure risk by strictly adhering to the obligations set forth in this Agreement and otherwise taking precautions to protect the Confidential Data from non-authorized use.

B. To supply ICPSR with a completed RDCS online Application for Obtaining Confidential Data that will include the following:

1. A signed Agreement

2. A Research Plan describing inquiry and publications consistent with the objectives of the Measuring Effective Teaching Project to advance knowledge about effective teachers and teaching.

3. Data Security Plan

4. Confidential Data Order Summary specifying which files and documentation are requested

5. Supplemental Agreement with Research Staff signed by each Research Staff member

6. Pledges of Confidentiality for the Investigator and each Research Staff member and Participant

7. A copy of a document signed by the Institution's Institutional Review Board (IRB) approving or exempting the research project

8. Investigator curriculum vitae

C. To comply fully with the approved Data Security Plan at all times relevant to this Agreement.

D. That no persons other than those identified in this Agreement or in subsequent amendments to this Agreement, as Investigator, Research Staff or Participant and who have executed this Agreement, be permitted access to the contents of Confidential Data files or any files derived from Confidential Data files.

E. To not disclose or otherwise make available to current and former employees of the Charlotte-Mecklenburg Schools, Dallas Independent School District, Denver Public Schools, Hillsborough County Public Schools, Memphis City Schools, and New York City Department of Education ("School Districts") any Confidential Data derived from the School District for which they are a current or former employee. Investigators, Research Staff, and Participants must disclose to ICPSR any current or past affiliations with the School Districts.

F. That within one (1) business day of becoming aware of any unauthorized access, use, or disclosure of Confidential Data, or access, use, or disclosure of Confidential Data that is inconsistent with the terms and conditions of this Agreement, the unauthorized or inconsistent access, use, or disclosure of Confidential Data will be reported in writing to ICPSR.

G. That, unless prior specific approval is received from ICPSR, no attempt under any circumstances will be made to link the Confidential Data to any individual, whether living or deceased, or with any other dataset, including other datasets provided by ICPSR.

H. To avoid inadvertent disclosure of private persons by being knowledgeable about what factors constitute disclosure risk and by using disclosure risk guidelines, such as but not limited to, the following guidelines in the release of statistics or other content derived from the Confidential Data.[4]

   1. No release of a sample unique for which only one record in the Confidential Data obtained through sampling (e.g., not a census) provides a certain combination of values from key variables. For example, in no table should all cases in any row or column be found in a single cell.

---

[4] For more information, see the U.S. Bureau of the Census checklist. *Supporting Document*

Checklist on Disclosure Potential of Data, at www.census.gov/srd/sdc/S14-1_v1.3_Checklist.doc; NCHS Disclosure Potential Checklist at http://www.cdc.gov/nchs/data/NCHS%20Micro-Data%20Release%20Policy%204-02A.pdf; and *FCSM Statistical Policy Working Paper 22 (Second Version, 2005)* at http://www.fcsm.gov/working-papers/SPWP22_rev.pdf.

2. No release of a sample rare for which only a small number of records (e.g., 3, 5, or 10 depending on sample characteristics) in the Confidential Data provide a certain combination of values from key variables. For example, in no instance should the cell frequency of a cross-tabulation, a total for a row or column of a cross-tabulation, or a quantity figure be fewer than the appropriate threshold as determined from the sample characteristics. In general, assess empty cells and full cells for disclosure risk stemming from sampled records of a defined group reporting the same characteristics.

3. No release of a population unique for which only one record in the Confidential Data that represents the entire population (e.g., from a census) provides a certain combination of values from key variables. For example, in no table should all cases in any row or column be found in a single cell.

4. No release of the statistic if the total, mean, or average is based on fewer cases than the appropriate threshold as determined from the sample characteristics.

5. No release of the statistic if the contribution of a few observations dominates the estimate of a particular cell. For example, in no instance should the quantity figures be released if one case contributes more than 60 percent of the quantity amount.

6. No release of data that permits disclosure when used in combination with other known data. For example, unique values or counts below the appropriate threshold for key variables in the Confidential Data that are continuous and link to other data from ICPSR or elsewhere.

7. No release of minimum and maximum values of identifiable characteristics (e.g., income, age, household size, etc.) or reporting of values in the "tails," e.g., the 5th or 95th percentile, from a variable(s) representing highly skewed populations.

8. Release only weighted results if specified in the data documentation.

9. No release of ANOVAs and regression equations when the analytic model that includes categorical covariates is saturated or nearly saturated. In general, variables in analytic models should conform to disclosure rules for descriptive statistics (e.g., see #7 above) and appropriate weights should be applied.

10. In no instance should data on an identifiable case, or any of the kinds of data listed in preceding items 1-9, be derivable through subtraction or other calculation from the combination of tables released.

11. No release of sample population information or characteristics in greater detail than released or published by the researchers who collected the Confidential Data. This includes but is not limited to publication of maps.

12. No release of anecdotal information about a specific private person(s) or case study without prior approval.

13. The above guidelines also apply to charts as they are graphical representations of cross-tabulations. In addition, graphical outputs (e.g., scatterplots, box plots, plots of residuals) should adhere to the above guidelines.

I. To mitigate the risk of disclosing identities or private information derived from the Confidential Information by following practices that include, but are not limited to the following:

1. No streaming video from the Confidential Data may be captured on any computer or other medium.

2. No excerpts, images or other derivatives from the Confidential Data may be published or disseminated in any way.

3. No descriptions of individuals, activities, environments, or other aspects of the Confidential Data may be released in a way that would lead to identification of individuals. Information about objects in the Confidential Data (such as school, grade, subject) may not be included in presentations or publications if they may increase the risk of disclosure.   Special care should be used in describing attributes of individuals that in combination might uniquely identify an individual, such as school, grade, age, race, gender, "gifted," "special education," "English language learner," or physical attributes (height, weight, hair color, etc.).

4. No anecdotal descriptions or verbatim transcripts may be released if they can be linked to information that increases the risk of identification of individuals.

5. No information from quantitative and video objects in the Confidential Data may be linked for the purpose of identifying individuals.

6. No identifying information revealed by individuals depicted in the Confidential Data may be recorded in any way. For example, names of persons, places, or events written on blackboards or spoken by an individual may not be written on paper or typed into a computer document. This type of information may never be released in public presentations or publications. If there is any doubt about whether a research note may pose a disclosure risk, it should be created within the Virtual Data Enclave.

J. That if the identity of any private person should be discovered, then:

1. No use will be made of this knowledge;

2. ICPSR will be advised of the incident within five (5) business days of discovery of the incident;

3. The information that would identify the private person will be safeguarded or destroyed as requested by ICPSR; and

4. No one else will be informed of the discovered identity..

K. Unless other provisions have been made with ICPSR, all access to the Confidential Data will be terminated on or before completion of this Agreement or within five (5) days of written notice from ICPSR. Investigators requiring access to the Confidential Data beyond completion of this Agreement should submit a request for continuation three months prior to the end date of the Agreement.

L. To ensure that the Confidential Data are managed and used in compliance with the terms and conditions of this Agreement and with all applicable statutes and regulations. Noncompliance with this Agreement by any Research Staff or Participant hereto shall be

deemed noncompliance and a breach by Investigator and Institution for purposes of section VII below.

M. To notify ICPSR of a change in institutional affiliation of the Investigator. Notification must be in writing and must be received by ICPSR at least six (6) weeks prior to Investigator's last day of employment with Institution. Investigator's separation from Institution terminates this Agreement. Investigator may reapply for access to Confidential Data as an employee of the new institution. Re-application requires:

    1. Execution of a new Agreement for the Use of Confidential Data by both the Investigator and the proposed new institution;

    2. Execution of any Supplemental Agreement(s) with Research Staff and Pledges of Confidentiality by Research Staff and Participants at the proposed new institution;

    3. Preparation and approval of a new Data Security Plan; and

    4. Evidence of approval or exemption by the proposed new institution's IRB.

These materials must be approved by ICPSR before Confidential Data or any derivatives or analyses may be accessed at the new institution.

N. That if the Investigator who is changing institutions does not have the new agreement executed by the time they leave their institution, ICPSR will temporarily deactivate the Investigator's account but will maintain the Investigator's profile to save their work during the transition.   Upon approval of the new RDCS online application, ICPSR will reactivate the Investigator's account. If a new agreement is not executed within three (3) month, the Investigator's account will be deleted.

O. That any books, articles, conference papers, theses, dissertations, reports, or other publications that employed the Confidential Data or other resources provided by ICPSR reference the bibliographic citation provided by ICPSR in the study description.

P. That use of the Confidential Data will be consistent with the Institution's policies regarding scientific integrity and human subjects research.

Q. To respond fully and in writing within ten (10) working days after receipt of any written inquiry from ICPSR regarding compliance with this Agreement.

VII. VIOLATIONS OF THIS AGREEMENT

A. The Institution will treat allegations by ICPSR or other parties of violations of this Agreement as allegations of violations of its policies and procedures on scientific integrity and misconduct. If the allegations are confirmed, the Institution will treat the violations as it would violations of the explicit terms of its policies on scientific integrity and misconduct.

B. In the event Investigator or Institution breaches any provision of this Agreement, they shall be jointly and severally responsible to promptly cure the breach and mitigate any damages. Investigator and Institution hereby acknowledge that any breach of the confidentiality provisions herein may result in irreparable harm to ICPSR not adequately compensable by money

damages. Investigator and Institution hereby acknowledge the possibility of injunctive relief in the event of breach, in addition to money damages. In addition, ICPSR may:

       1. Terminate this Agreement upon notice and terminate access to the Confidential Data and any derivatives thereof;

       2. Deny Investigator future access to Confidential Data; and/or

       3. Report the inappropriate use or disclosure to the appropriate federal and private agencies or foundations that fund scientific and public policy research.

C. Institution agrees, to the extent permitted under the law, to indemnify, defend, and hold harmless The University of Michigan, ICPSR, RAND Corporation, Bill & Melinda Gates Foundation, and the sources of Confidential Data from any or all claims and losses accruing to any person, organization, or other legal entity as a result of Investigator's, Research Staff's, Participant's, and/or Institution's acts, omissions, or breaches of this Agreement.

VIII. CONFIDENTIALITY

The Institution is considered to be a contractor or cooperating agency of ICPSR; as such, the Institution, the Investigator, and Research Staff are authorized to protect the privacy of the individuals who are the subjects of the Confidential Data by withholding their identifying characteristics from all persons not connected with the conduct of the Investigator's research project. Identifying characteristics are considered to include those data defined as confidential under the terms of this Agreement.

IX. INCORPORATION BY REFERENCE

All parties agree that the following documents are incorporated into this Agreement by reference:

A. The Application for Obtaining Confidential Data

B. A copy of the Institution's IRB approval or exemption of the Research Project

C. The Data Security Plan proposed by the Investigator and approved by ICPSR

X. MISCELLANEOUS

A. All notices, contractual correspondence, and return of data under this Agreement on behalf of the Investigator shall be made in writing and delivered to the address below:

MET Longitudinal Database Restricted Data Manager
ICPSR
P.O. Box 1248
Ann Arbor, MI 48106-1248

B. This agreement shall be effective for 24 months from execution.

C. The respective rights and obligations of ICPSR and Investigator, Research Staff, and Institution pursuant to this Agreement shall survive termination of the Agreement.

D. This Agreement may be amended or modified only by the mutual written consent of the authorized representatives of ICPSR and Investigator and Institution. Investigator's research project, Data Security Plan, Research Staff, or Participants may be amended or modified only by submitting such amendments or modifications to the RDCS and receiving approval from the authorized representatives of ICPSR. This Agreement may be extended only by submitting an extension request to the RDCS and receiving approval from the authorized representatives of ICPSR. Investigator and Institution agree to amend this Agreement to the extent necessary for ICPSR to comply with the requirements of any applicable regulatory authority.

E. The persons signing this Agreement have the right and authority to execute this Agreement, and no further approvals are necessary to create a binding agreement.

F. The obligations of Investigator, Research Staff, Participants, and Institution set forth within this Agreement may not be assigned or otherwise transferred without the express written consent of ICPSR.

Investigator and Institutional Signatures

Investigator   Institutional Representative

_____   _____
SIGNATURE   DATE   SIGNATURE   DATE

_____   _____
NAME TYPED OR PRINTED   NAME TYPED OR PRINTED

_____   _____
TITLE   TITLE

_____   _____
INSTITUTION   INSTITUTION

_____   _____
BUILDING ADDRESS   BUILDING ADDRESS

_____   _____
STREET ADDRESS   STREET ADDRESS

_____   _____
CITY, STATE, ZIP   CITY, STATE, ZIP

Representative of ICPSR Archive   Representative of University of Michigan

_____   _____
SIGNATURE   DATE   SIGNATURE   DATE

_____   _____
PRINTED NAME AND ARCHIVE   PRINTED NAME AND TITLE

Attachment A: Data Security Plan

All of the following computer and data security requirements and procedures are required to be implemented as part of this Agreement:

- You must password protect the computer that is used to access the MET Longitudinal Database.
- Under no circumstances may you share or give your MET Longitudinal Database username and password to anyone, and this includes not sharing them with other members of your project team or your organization's IT staff. Passwords must not be stored on a computer in electronic or written form. Software password storage programs may not be used.
- Since the MET Longitudinal Database is administered by ICPSR, University of Michigan you should not contact the IT staff at your organization with questions about the MET Longitudinal Database. (You may contact your organization's IT staff if you need help installing the VM client software to access the MET Longitudinal Database. Your organization's IT staff should never be allowed to access the MET Longitudinal Database or any Confidential Data.)
- Under no circumstances can any unauthorized person be allowed to access or view Confidential Data within the MET Longitudinal Database.
- The MET Longitudinal Database may only be accessed within the designated Project Office (as listed in the Application) using only the approved computer and assigned IP address.
- Unauthorized persons will not be allowed inside the designated Project Office when an authorized project team member is logged into the MET Longitudinal Database. While logged into the MET Longitudinal Database, the security protocol specified in the Application will be followed.
- You must not allow the computer monitor to display MET Longitudinal Database content to any unauthorized person. The computer monitor display screen must not be visible from open doors or through windows.
- You must set the computer to activate a password protected screen saver after three minutes of inactivity.
- If you are logged into the MET Longitudinal Database and you leave your computer, you must "disconnect" or "logoff" from the MET Longitudinal Database. (Disconnecting from the MET Longitudinal Database will leave any open programs running, but closes the connection to the MET Longitudinal Database. Logging off of the MET Longitudinal Database closes the connection and terminates all programs that are running.)
- All Confidential Data must be kept within the MET Longitudinal Database:
  - You must not duplicate or copy the data (e.g., you must not retype and/or use non-technical ways of copying the data, such as handwritten notes).
  - You must not take screenshots, photographs, or videos of the displayed Confidential Data or statistical outputs.
  - You must not type or record the Confidential Data or results from the data onto your PC or onto some other device or media.
- You must protect all hardcopy documents related to the Confidential Data such as research notes. Such hardcopy documents must be kept in locked drawers or cabinets when not in use.
- Prior to a disclosure review and approval by ICPSR, neither you nor any project team member may talk about or discuss any Confidential Data or results from the MET

Longitudinal Database in non-secure or public locations. These discussions cannot occur where an unauthorized person could eavesdrop.
- You must submit all statistical outputs/results from the MET Longitudinal Database to ICPSR for a disclosure review prior to sharing or giving such outputs to unauthorized persons. You also agree to revise or alter such outputs as required by ICPSR in order to minimize disclosure risk prior to ICPSR approving these outputs for dissemination to unauthorized persons.
- You may only disseminate aggregated information from the Confidential Data to unauthorized persons after you obtain clearance to do so through the ICPSR disclosure review process.

Attachment B

Supplemental Agreement with Research Staff

1. The undersigned Research Staff, in consideration of their use of these Confidential Data, agree:
    a. That they have read the associated Agreement for the Use of Confidential Data.
    b. That they are "Research Staff" within the meaning of the Agreement.
    c. To comply fully with the terms of the Agreement, including the Data Security Plan.

2. The undersigned Investigator agrees that the persons designated herein are Research Staff within the meaning of the associated Agreement for the Use of Confidential Data.

3. Investigator ensures that all Research Staff sign a Supplemental Agreement and an individual Pledge of Confidentiality.

Research Staff Name:

Research Staff Electronic Signature:

Date Signed:

Investigator Name:

Investigator Electronic Signature:

Date Signed:

Attachment C. Research Staff Pledge of Confidentiality

Pledge of Confidentiality

By virtue of my affiliation with this research project I have access to Confidential Data identified in this Agreement. I understand that access to this Confidential Data carries with it a responsibility to guard against unauthorized use and to abide by the Data Security Plan. To treat information as confidential means to not divulge it to anyone who is not a party to the Agreement for the Use of Confidential Data, or cause it to be accessible to anyone who is not a party to that Agreement.

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

1. I agree not to permit Confidential Data access to anyone not a party to the Agreement for the Use of Confidential Data.
2. I agree to not attempt to identify private persons as defined in the Agreement for the Use of Confidential Data.
3. I agree that in the event an identity of any private person is discovered inadvertently, I will (a) make no use of this knowledge, (b) advise the Investigator of the incident who will report it to ICPSR, (c) safeguard or destroy the information as directed by the Investigator after consultation with ICPSR, and (d) not inform any other person of the discovered identity.

Investigator or Research Staff Name:

Investigator or Research Staff Electronic Signature:

Data Signed:

Attachment D. Participant Pledge of Confidentiality

Pledge of Confidentiality

As a Participant in this research project I have access to Confidential Information, which may be videos, images, documents, or other in other formats.   I understand that participation in this research project carries with it a responsibility to protect the privacy of the individuals who provided Confidential Information.

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

1. I agree not to permit access to Confidential Information to anyone.

2. I agree not to discuss any aspect of Confidential Information with anyone except the Investigator and Research Staff of this project.

3. I agree to view videos, documents, and other Confidential Information only under secure conditions approved by the Investigator or Research Staff. For example, I will not view videos in a public location where someone might be able to see my computer screen.

4. I agree not to attempt to identify any persons depicted or described in Confidential Information.

5. I agree that if I recognize or discover the identity of a person in Confidential Data, I will (a) make no use of this knowledge, (b) advise the Research Staff of the incident, (c) safeguard or destroy the information as directed by the Research Staff, and (d) not inform any other person of the discovered identity.

6. I agree to immediately report any incident involving Confidential Information to

      [Investigator's name and contact information]

Name:

Signature:

Data Signed:

Attachment E

Confidential Data Order Summary

Investigators may request one or all of the following three collections from the MET Longitudinal Database. Investigators will be provided access to the data collections required to accomplish their research plan.

1. MET Sample Analytical files
   a. Teacher level files: Teacher characteristics, surveys, knowledge assessments, video scores
   b. Section level files: Value added measures, summary measures from supplemental student assessments (BAM, ACT, SAT-9), summary measures from observation session scores (PLATO, MQI, CLASS, FFT, QST, UTOP)
   c. Student level files: supplemental student assessments (BAM, ACT, SAT-9), student perception surveys
   d. Observation session files: observation session scores (PLATO, MQI, CLASS, FFT, QST, UTOP)
   e. Teacher working conditions survey
   f. Survey of Enacted Curriculum
   g. Principal survey

2. Student assessment scores and characteristics supplied by school districts

3. Classroom observation videos