NATIONAL CENTER FOR EDUCATION STATISTICS

Institute for Education Sciences (IES)

Data Security Application

OMB# 1850-NEW

April 2023

IES RESTRICTED USE DATA APPLICATION

Contents

Directions and Tips

- Your application for access to IES data is approved in SAP but requires a security plan and documents before the data will be sent for researcher use.
- Your application will be considered incomplete until all documents here are completed and returned to IES Data Security at the following address below:

  IES Data Security, National Center for Education Statistics,
  Potomac Center Plaza,
  550 12th Street, SW, Room 4165,
  Washington, DC 20202

- Please mail in the following:
  1. License application
  2. Security Plan form
  3. Affidavits of nondisclosure for the PPO, SSO, and all additional data users
  4. Training certificates for the PPO, SSO, and all additional data users

For more information and more detailed instructions, please see https://nces.ed.gov/statprog/instruct.asp

LICENSE FOR THE USE OF INDIVIDUALLY IDENTIFIABLE INFORMATION PROTECTED UNDER THE EDUCATION SCIENCES REFORM ACT OF 2002 AND PROTECTED, AS APPLICABLE, UNDER THE FOUNDATIONS OF EVIDENCE-BASED POLICYMAKING ACT OF 2018 44 U.S.C., CHAPTER 35, SUBCHAPTER III, Part B, Section 3572 CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY ACT, THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT, AND THE PRIVACY ACT OF 1974

WHEREAS, the Institute of Education Sciences (IES) of the United States Department of Education has collected and maintains individually identifiable information, the confidentiality of which is protected by section 183 of the Education Sciences Reform Act of 2002 (ESRA) (PL 107-279) (20 U.S.C. 9573), and, as applicable, by the Privacy Act of 1974 (5 U.S.C. 552a); the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g); and Confidential Information Protection and Statistical Efficiency Act (CIPSEA), Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); and

WHEREAS, IES wishes to make the data available for statistical, research, or evaluation purposes to requestors qualified and capable of research and analysis consistent with the statistical, research, or evaluation purposes for which the data were provided or are maintained, but only if the data are used and protected in accordance with the terms and conditions stated in this license (License), upon receipt of such assurance of qualification and capability, it is hereby agreed between

_____,
(Insert the name of the agency or organization to be licensed)

hereinafter referred to as the "Licensee", and IES that:

I. INFORMATION SUBJECT TO THIS AGREEMENT

A. All data containing individually identifiable information about students, their families, and their schools maintained by IES under section 183 of the Education Sciences Reform Act of 2002, that are provided to the Licensee and all information derived from those data, and all data resulting from merges, matches, or other uses of the data provided by IES with other data are subject to this License and are referred to in this License as subject data.

B. Subject data under this License may be in the form of CD-ROMs, electronic data, hard copy, etc. The Licensee may only use the subject data in a manner and to a purpose consistent with:

1. The statistical, research, or evaluation purpose for which the data are

maintained. All subject data that include individually identifiable information are protected under the Privacy Act, ESRA, and/or CIPSEA and may be used only for statistical, research, or evaluation purposes consistent with purposes for which the data were collected and /or are maintained (Licensee's description of the research and analysis which is planned is attached and made a part of this License - Attachment No. 1.);

2. Subject data that includes personally identifiable information from students' education records are protected under FERPA and may only be used for the evaluation of Federally-supported education programs or for conducting studies, for, or on behalf of, educational agencies or institutions to improve instruction. (Licensee's description of the evaluation or study which is planned is attached and made a part of this License - Attachment No. 1.);

3. The limitations imposed under the provisions of this License; and

4. Section 183 of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573); and, as applicable, CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Privacy Act of 1974 (5 U.S.C. 552a); and the Family Educational Rights Protection Act (20 U.S.C. 1232g) which are attached to and made a part of this License (Attachment No. 2.)

II. INDIVIDUALS WHO MAY HAVE ACCESS TO SUBJECT DATA

A. There are four categories of individuals that the Licensee may authorize to have access to subject data. The four categories of individuals are as follows:

1. The Principal Project Officer (PPO) is the most senior officer in charge of the day-to-day operations involving the use of subject data and is responsible for liaison with IES.

2. Professional/Technical staff (P/T) conduct the research for which this License was issued.

3. Support staff includes secretaries, typists, computer technicians, messengers, etc. Licensee may disclose subject data to support staff who come in contact with the subject data in course of their duties only to the extent necessary to support the research under this License.

4. The System Security Officer (SSO) is responsible for maintaining the day-to-day security of the licensed data, including the implementation, maintenance, and periodic update of the Security Plan to protect the data in strict compliance with statutory and regulatory requirements.

B. Licensee may disclose subject data to only to only seven (7) staff, including the PPO, SSO, P/TS, and support staff, unless IES provides written authorization for a larger number of P/TS.

III. LIMITATIONS ON DISCLOSURE

A. Licensee shall not use or disclose subject data for any administrative purposes nor may the subject data be applied in any manner to change the status, condition, or public perception of any individual regarding whom subject data is maintained. (Note: Federal Law pre-empts any State law that might require the reporting or dissemination of these data for any purpose other than the statistical, research, and evaluation purposes for which they were collected and/or are maintained.)

B. Licensee shall not disclose subject data or other information containing, or derived from, subject data at fine levels of geography, such as school district, institution, or school, to anyone other than IES employees working in the course of their employment or individuals for whom access is authorized under this License agreement. Licensee may make disclosures of subject data to individuals other than those specified in this License only if those individuals have executed an Affidavit of Nondisclosure and the Licensee has obtained advance written approval from the IES Data Security Office.

C. Licensee shall not make any publication or other release of subject data listing information regarding individuals or specific educational institutions even if the individual respondent identifiers have been removed.

D. Licensee may publish the results, analysis, or other information developed as a result of any research based on subject data made available under this License only in summary or statistical form so that the identity of individuals or specific educational institutions contained in the subject data is not revealed.

IV. ADMINISTRATIVE REQUIREMENTS

A. The research conducted under this License and the disclosure of subject data needed for that research must be consistent with the statistical, research, or evaluation purpose for which the data were supplied. The subject data may not be used to identify individuals or specific educational institutions for recontacting unless Licensee has obtained advance written approval from the IES Data Security Office.

B. Execution of Affidavits of Nondisclosure.

1. Licensee shall provide a copy of this agreement, together with the Security Plan (Attachment No. 3) to the SSO and to each P/T and support staff person of the Licensee who will have access to subject data and shall require each of those individuals to execute an Affidavit of Nondisclosure (Attachment No. 4).

2. The Licensee must ensure that each individual who executes an Affidavit of Nondisclosure reads and understands the materials provided to her or him before executing the Affidavit.

3. Licensee shall ensure that each Affidavit of Nondisclosure is notarized upon execution.

4. Licensee may not permit any individual specified in paragraph II.A. to have access to subject data until the procedures in paragraphs IV.B.1. through 3 of this License are fulfilled for that individual.

5. Licensee shall promptly, after the execution of each Affidavit, send the original Affidavit to the IES Data Security Office and shall maintain a copy of each Affidavit at the Licensee's secured facility protected under this License.

C. Notification regarding authorized individuals to IES.

1. Licensee shall promptly notify the IES Data Security Office when the SSO, or any P/T or support staff who has been authorized to have access to subject data no longer has access to those data.

D. Publications made available to IES.

1. Licensee shall provide the IES Data security Office a copy of each publication containing information based on subject data or other data product based on subject data before they are made available to individuals who have not executed an Affidavit of Nondisclosure.

2. Because the publication or other release of research results could raise reasonable questions regarding disclosure of individually identifiable information contained in subject data, copies of the proposed publication or release must be provided to the IES Data Security Office before that disclosure is made so that IES may advise whether the disclosure is authorized under this License and the provisions of section 183 of the Education Sciences Reform Act of 2002; CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Privacy Act of 1974; and the Family Educational Rights and Privacy Act. Licensee agrees not to publish or otherwise release research results provided to IES if IES advises that such disclosure is not authorized.

E. Licensee shall notify the IES Data Security Office immediately upon receipt of any legal, investigatory, or other demand for disclosure of subject data.

F. Licensee shall notify the IES Data Security Office immediately upon discovering any breach or suspected breach of security or any disclosure of subject data to unauthorized parties or agencies.

G. Licensee agrees that representatives of IES have the right to make unannounced and unscheduled inspections of the Licensee's facilities, including any associated computer center, to evaluate compliance with the terms of this License and the requirements of section 183 of the Education Sciences Reform Act of 2002; CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.); the Privacy Act of 1974; and the Family Educational Rights and Privacy Act.

V. SECURITY REQUIREMENTS

A. Maintenance of, and access to, subject data.

1. Licensee shall retain the original version of the subject data at a single location and may make no copy or extract of the subject data available to anyone except the SSO or a P/T staff member as necessary for the purpose of the statistical research for which the subject data were made available to the Licensee.

2. Licensee shall maintain subject data (whether maintained on a personal computer or on printed or other material) in a space that is limited to access by the PPO, SSO, and authorized P/T staff.

3. Licensee shall ensure that access to subject data maintained in computer memory is controlled by password protection. Licensee shall maintain all print-outs, CD-ROMS, personal computers with subject data on hard disks, or other physical products containing individually identifiable information derived from subject data in locked cabinets, file drawers, or other secure locations when not in use.

4. Licensee shall ensure that all printouts, tabulations, and reports are edited for any possible disclosures of subject data.

5. Licensee shall establish security procedures to ensure that subject data cannot be used or taken by unauthorized individuals.

6. Licensee shall not permit removal of any subject data from the limited access space protected under the provisions of this License as required in the attached Security Plan (Attachment No. 3.), without first notifying, and obtaining written approval from, IES.

B. Retention of subject data.

Licensee shall return to the IES Data Security Office all subject data, or destroy those data under IES supervision or by approved IES procedures when the statistical analysis, research, or evaluation that is the subject of this agreement has been completed or this License terminates, whichever occurs first. Licensee, as part of its responsibilities discussed herein, agrees to submit a completed Close-out Certification Form to the IES Data Security Office.

C. Compliance with established security procedures.

Licensee shall comply with the security procedures described in the Security Plan (Attachment No. 3 to this License).

VI. PENALTIES

A. Any violation of the terms and conditions of this License may subject the Licensee to immediate revocation of the License by IES.

1. The IES official responsible for liaison with the Licensee shall initiate revocation of this License by written notice to Licensee indicating the factual basis and grounds for revocation.

2. Upon receipt of the notice specified in paragraph VI.A.1 of this License, the Licensee has thirty (30) days to submit written argument and evidence to the Director of IES indicating why the License should not be revoked.

3. The Director of IES shall decide whether to revoke the License based solely on the information contained in the notice to the Licensee and the Licensee's response and shall provide written notice of the decision to the Licensee within forty-five (45) days after receipt of Licensee's response. The Director of IES may extend this time period for good cause.

B. Any violation of this License may also be a violation of Federal criminal law under the Privacy Act of 1974 (5 U.S.C. 552a(i)); section 183 of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573(d)(2); and/or CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.). Alleged violations under section 183 of the Education Sciences Reform Act of 2002 and CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.) are subject to prosecution by the Offices of the United States Attorney. The penalty for violation of section 183 of the Education Sciences Reform Act of 2002 and CIPSEA, Subchapter III, Part B, Section 3572 of the Foundations of Evidence-Based Policymaking Act of 2018 (44 U.S.C.), is a fine of not more than $250,000 and imprisonment for a period of not more than five years.

VII. PROCESSING OF THIS LICENSE

A. The term of this License shall be for_____years. If, before the expiration of this License, the Director of IES establishes regulatory standards for the issuance and content of Licenses, the Licensee agrees to comply with the regulatory standards.

B. This License may be amended, extended, or terminated by mutual written agreement between the Licensee and the Director of IES. Any amendment must be signed by a Senior Official specified in paragraph VII.C. of this License, PPO, and the Director of IES and is effective on the date that all required parties have signed the amendment.

C. The Senior Official (SO), who cannot be the same individual designated as the PPO, having the legal authority to bind the organization to the terms of the License, shall sign this License below. The SO certifies, by his/her signature, that -

1. The organization has the authority to undertake the commitments in this License;

2. The SO has the legal authority to bind the organization to the provisions of this License; and

3. The PPO is the most senior subject matter officer for the Licensee who has the authority to manage the day-to-day statistical, research, or evaluation operations of the Licensee.

_____ _____
Signature of the Senior Official Date

_____
Type/Print Name of Senior Official

Title:_____Telephone: (____)_____

D. The individual described in paragraph II.A1. as the PPO shall sign this License below. If the SO also acts as the chief statistical officer for the Licensee; viz. as the PPO, the SO shall likewise sign under this paragraph as well as having signed under paragraph VII.C.

_____ _____
Signature of the Principal Project Officer Date

_____
Type/Print Name of the Principal Project Officer

Title:_____Telephone: (____)_____

Memorandum of Understanding
THE INSTITUTE OF EDUCATION SCIENCES
U.S. DEPARTMENT OF EDUCATION
and

THE _____

SUBJECT: Access by the _____ to individually identifiable information acquired by the Institute of Education Sciences (IES) of the United States Department of Education.

IES has collected and maintains individually identifiable information, the confidentiality of which is protected by Section 183 of the Education Sciences Reform Act of 2002 (ESRA) (PL 107-279) (20 U.S.C. 9573), and, as applicable, by the Privacy Act of 1974 (5 U.S.C. 552a); the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g); and Title V, subtitle A of the E-Government Act of 2002 (CIPSEA) (PL 107-347) (44 U.S.C. 3501 note); and wishes to make the data available for statistical, research or evaluation purposes to requestors qualified and capable of research and analysis consistent with the statistical, research or evaluation purposes for which the data were provided or are maintained, but only if the data are used and protected in accordance with the terms and conditions stated in this Memorandum of Understanding (MOU), upon receipt of such assurance of qualification and capability.

The _____ (hereinafter referred to as the "Agency") and the Institute of Education Sciences (IES) agree that:

I. INFORMATION SUBJECT TO THIS MOU

A. All data containing individually identifiable information about students, their families and their schools maintained by IES under Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279) and Title V, subtitle A of the E-Government Act of 2002 (P.L. 107-347) that are provided to the Agency and all information derived from those data, and all data resulting from merges, matches, or other uses of the data provided by IES with other data, are subject to this MOU and are referred to in this MOU as "subject data."

B. Subject data under this MOU may be in the form of CD-ROMs, electronic data or hard copy, etc. The Agency may only use the subject data in a manner and for a purpose consistent with:

1. The statistical, research or evaluation purpose for which the data are maintained. All subject data that include individually identifiable information are protected under the Privacy Act, ESRA, and/or CIPSEA and may be used only for statistical, research, or evaluation purposes consistent with purposes for which the data were collected and /or are maintained. The Agency's description of the research and analysis which is planned is attached and made a part of this MOU (Attachment No. 1),
2. Subject data that includes personally identifiable information from students' education records are protected under FERPA and may only be used for the evaluation of Federally-supported education programs or for conducting studies, for, or on behalf of, educational agencies or institutions to improve instruction. (Agency's description of the evaluation or study which is planned is attached and made a part of this MOU - Attachment No. 1.);
3. The limitations imposed under the provisions of this MOU, and
4. Section 183 of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573); and, as applicable, Title V, subtitle A of the E-Government Act of 2002 (44 U.S.C. 3501 note); the Privacy Act of 1974 (5 U.S.C. 552a), and

the Family Educational Rights Protection Act (20 U.S.C. 1232g) which are attached to and made a part of this MOU (Attachment No. 2.)

II. INDIVIDUALS WHO MAY HAVE ACCESS TO SUBJECT DATA

A. There are four categories of individuals that the Agency may authorize to have access to subject data. The four categories of individuals are as follows:

1. The Principal Project Officer (PPO) is the most senior officer in charge of the day-to-day operations involving the use of subject data and is responsible for liaison with IES.
2. Professional/Technical staff (P/T) conduct the research for which this MOU was issued.
3. Support staff includes secretaries, typists, computer technicians, messengers, etc. The Agency may disclose subject data to support staff who come in contact with the subject data in course of their duties only to the extent necessary to support the research under this MOU.
4. The System Security Officer (SSO) is responsible for maintaining the day-to-day security of the licensed data, including the implementation, maintenance, and periodic update of security procedures to protect the data in strict compliance with statutory and regulatory requirements.

B. The Agency may disclose subject data to only to only seven (7) staff, including the PPO, SSO, P/TS, and support staff, unless IES provides written authorization for a larger number of P/TS.

III. LIMITATIONS ON DISCLOSURE

A. The Agency shall not use or disclose subject data for any administrative purposes nor may the subject data be applied in any manner to change the status, condition, or public perception of any individual regarding whom subject data is maintained. (Note: Federal Law pre-empts any State law that might require the reporting or dissemination of these data for any purpose other than

the statistical, research, and evaluation purposes for which they were collected and/or are maintained.)

B. The Agency shall not disclose subject data or other information containing, or derived from, subject data at fine levels of geography, such as school district, institution, or school, to anyone other than IES employees working in the course of their employment or individuals for whom access is authorized under this MOU agreement. The Agency may make disclosures of subject data to individuals other than those specified in this MOU only if those individuals have executed an Affidavit of Nondisclosure and the Agency has obtained advance written approval from the IES Data Security Office.

C. The Agency shall not make any publication or other release of subject data listing information regarding individuals or specific educational institutions even if the individual respondent identifiers have been removed.

D. The Agency may publish the results, analysis, or other information developed as a result of any research based on subject data made available under this MOU only in summary or statistical form so that the identity of individuals or specific educational institutions contained in the subject data is not revealed.

IV. ADMINISTRATIVE REQUIREMENTS

A. The research conducted under this MOU and the disclosure of subject data needed for that research must be consistent with the statistical, research, or evaluation purpose for which the data were supplied. The subject data may not be used to identify individuals or specific educational institutions for recontacting unless the Agency has obtained advance written approval from the IES Data Security Office.

B. Execution of Affidavits of Nondisclosure.

1. The Agency shall provide a copy of this agreement to the SSO and to each P/T and support staff person of the Agency who will have access to

subject data and shall require each of those individuals to execute an Affidavit of Nondisclosure (Attachment No. 4).

2. The Agency must ensure that each individual who executes an Affidavit of Nondisclosure reads and understands the materials provided to her or him before executing the Affidavit.
3. The Agency shall ensure that each Affidavit of Nondisclosure is notarized upon execution.
4. The Agency may not permit any individual specified in paragraph II.A. to have access to subject data until the procedures in paragraphs IV.B.1. through 3 of this MOU are fulfilled for that individual.
5. The Agency shall promptly, after the execution of each Affidavit, send the original Affidavit to the IES Data Security Office and shall maintain a copy of each Affidavit at the Agency's secured facility protected under this MOU.

C. Notification regarding authorized individuals to IES.

1. The Agency shall promptly notify the IES Data Security Office when the SSO, or any P/T or support staff who has been authorized to have access to subject data no longer has access to those data.

D. Publications made available to IES.

1. The Agency shall provide the IES Data Security Office a copy of each publication containing information based on subject data or other data product based on subject data before they are made available to individuals who have not executed an Affidavit of Nondisclosure.
2. Because the publication or other release of research results could raise reasonable questions regarding disclosure of individually identifiable information contained in subject data, copies of the proposed publication or release must be provided to the IES Data Security Office before that disclosure is made so that IES may advise whether the disclosure is authorized under this MOU and the provisions of Section 183 of the

Education Sciences Reform Act of 2002; Title V, subtitle A of the E-Government Act of 2002; the Privacy Act of 1974; and the Family Educational Rights and Privacy Act. The Agency agrees not to publish or otherwise release research results provided to IES if IES advises that such disclosure is not authorized.

E. The Agency shall notify the IES Data Security Office immediately upon receipt of any legal, investigatory, or other demand for disclosure of subject data.

F. The Agency shall notify the IES Data Security Office immediately upon discovering any breach or suspected breach of security or any disclosure of subject data to unauthorized parties or agencies.

G. The Agency agrees that representatives of IES have the right to make unannounced and unscheduled inspections of the Agency's facilities, including any associated computer center, to evaluate compliance with the terms of this MOU and the requirements of Section 183 of the Education Sciences Reform Act of 2002; Title V, subtitle A of the E-Government Act of 2002; the Privacy Act of 1974; and the Family Educational Rights and Privacy Act.

V. SECURITY REQUIREMENTS

A. Maintenance of, and access to, subject data.

1. The Agency shall retain the original version of the subject data at a single location and may make no copy or extract of the subject data available to anyone except the SSO or a P/T staff member as necessary for the purpose of the statistical research for which the subject data were made available to the Agency.
2. The Agency shall maintain subject data (whether maintained on a personal computer or on printed or other material) in a space that is limited to access by the PPO, SSO, and authorized P/T staff.

3. The Agency shall ensure that access to subject data maintained in computer memory is controlled by password protection. The Agency shall maintain all print-outs, CD-ROMS, personal computers with subject data on hard disks, or other physical products containing individually identifiable information derived from subject data in locked cabinets, file drawers, or other secure locations when not in use.
4. The Agency shall ensure that all printouts, tabulations, and reports are edited for any possible disclosures of subject data.
5. The Agency shall establish security procedures to ensure that subject data cannot be used or taken by unauthorized individuals.
6. The Agency shall not permit removal of any subject data from the limited access space protected under the provisions of this MOU, without first notifying, and obtaining written approval from, IES.

B. Retention of subject data.

1. The Agency shall return to the IES Data Security Office all subject data, or destroy those data under IES supervision or by approved IES procedures when the statistical analysis, research, or evaluation that is the subject of this agreement has been completed or this MOU terminates, whichever occurs first. The Agency, as part of its responsibilities discussed herein, agrees to submit a completed Close-out Certification Form to the IES Data Security Office.

C. Compliance with established security procedures.

1. The Agency shall comply with the security procedures described in this MOU.

VI. PENALTIES

A. Any violation of the terms and conditions of this MOU may subject the Agency to immediate revocation of the MOU by IES.

1. The IES official responsible for liaison with the Agency shall initiate revocation of this MOU by written notice to the Agency indicating the factual basis and grounds for revocation.
2. Upon receipt of the notice specified in paragraph VI.A.1 of this MOU, the Agency has thirty (30) days to submit written argument and evidence to the Director of IES indicating why the MOU should not be revoked.
3. The Director of IES shall decide whether to revoke the MOU based solely on the information contained in the notice to the Agency and the Agency's response and shall provide written notice of the decision to the Agency within forty-five (45) days after receipt of Agency's response. The Director of IES may extend this time period for good cause.

B. Any violation of this MOU may also be a violation of Federal criminal law under the Privacy Act of 1974 (5 U.S.C. 552a(i)); Section 183 of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573(d)(2); and/or Title V, subtitle A of the E-Government Act of 2002. Alleged violations under Section 183 of the Education Sciences Reform Act of 2002 and Title V, subtitle A of the E-Government Act of 2002 are subject to prosecution by the Offices of the United States Attorney. The penalty for violation of Section 183 of the Education Sciences Reform Act of 2002 and Title V, subtitle A of the E-Government Act of 2002, is a fine of not more than $250,000 and imprisonment for a period of not more than five years.

VII. PROCESSING OF THIS MOU

A. The term of this MOU shall be for ____ years. If, before the expiration of this MOU, the Director of IES establishes regulatory standards for the issuance and content of MOUs, the Agency agrees to comply with the regulatory standards.

B. This MOU may be amended, extended, or terminated by mutual written agreement between the Agency and the Director of IES. Any amendment must be signed by a Senior Official specified in paragraph VII.C. of this MOU, PPO, and the Director of IES and is effective on the date that all required parties have signed the amendment.

C. The Senior Official (SO), who cannot be the same individual designated as the PPO, having the legal authority to bind the organization to the terms of the MOU, shall sign this MOU below. The SO certifies, by his/her signature, that -

1. The organization has the authority to undertake the commitments in this MOU;
2. The SO has the legal authority to bind the organization to the provisions of this MOU; and

3. The PPO is the most senior subject matter officer for the Agency who has the authority to manage the day-to-day statistical, research, or evaluation operations of the Agency.

_____ _____

Signature of the Senior Official Date

_____

Type/Print Name of Senior Official

Title:_____ Telephone: (____)_____

D. The individual described in paragraph II.A1. as the PPO shall sign this MOU below. If the SO also acts as the chief statistical officer for the Agency; viz. as the PPO, the SO shall likewise sign under this paragraph as well as having signed under paragraph VII.C.

_____ _____

Signature of the Principal Project Officer Date

_____

Type/Print Name of the Principal Project Officer

Title:_____ Telephone: (____)_____

E. The Director of the Institute of Education Sciences or Designee concurs in this MOU and authorizes the access of the Agency to the subject data. This is effective as of the date of the IES Director or Designee's signature below.

_____

Signature of Director or Designee, Institute of Education Sciences

_____, _____

Name (Print) Title

_____

Date

MOU Control Number: _____ (Assigned by IES)

Security Plan Form

Institute of Education Sciences (IES)
Restricted-use Data

Name of Institution / Organization: _____

PPO Name: _____

PPO Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

PPO Phone Number: _____

Type of Security Plan: New ☐ Renewal ☐ Modification ☐

License Number: _____

Physical Location of Data

Project Office Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

Project Office Phone Number: _____

Note: *The restricted-use data and computer must be secured and used **only** at this location. When the data are not being used, the data must be stored under lock and key at this location. Only authorized users of the data, as listed on the License, may have key access to this secure project office/room.*

Physical Security of Data

Describe Building Security:
(Describe building security arrangements where project office is located.)

Describe Project Office Security:
(Describe project office security arrangements for the room where the computer and data will be located.)

Computer Security Requirements

Describe Computer System:
(*Please read the **Note** below. Computer security must follow the requirements listed below.)*

Computer Operating System: _____

Anti-Virus Software Installed on Computer: _____

Note: *The restricted-use data must be copied to and run on a standalone, desktop computer.* ***Use of a laptop computer, external hard drive, or USB memory stick is strictly prohibited.*** *Absolutely no restricted-use data may be copied onto a server or computer that is attached to a modem or network (LAN) connection. Prior to attaching the computer to a modem or LAN connection, the restricted-use data must be purged and overwritten on the computer.*

The following physical location and computer security procedures must be implemented when in possession of restricted-use data. By checking the box next to each security procedure, you signify that these security procedures will be implemented for the duration of the project and License period:

- Only authorized users listed on the License will have access to the secure room. Access will be limited to the secure room/project office by locking the office when away from the office. ☐
- Data will only be secured, accessed and used within the secure project office/room (as specified on page 1 of this plan). ☐
- A password will be required as part of the computer login process. ☐
- The password for computer access will be unique and contain 6 to 8 characters with at least one non-alphanumeric character. ☐

- The computer password will change at least every 3 months or when project staff leave. ☐
- Read-only access will be initiated for the original data. ☐
- An automatic password protected screensaver will enable after 5 minutes of inactivity. ☐
- No routine backups of the restricted-use data will be made. ☐
- Project office room keys will be returned and computer login will be disable within 24 hours after any user leaves the project. The PPO will notify IES of staff changes. ☐
- Restricted-use data will **not** be placed on a server (network), laptop computer, USB memory stick, or external hard drive. ☐
- The data will be removed from the project computer and overwritten, whether at the end of the project or when reattaching a modem or LAN connection. ☐
- Post Warning notification: During the computer log-in process, a warning statement (shown below) will appear on the computer screen before access is granted. If it is not possible to have the warning appear on the screen, it must be typed and attached to the computer monitor in a prominent location. ☐

W A R N I N G

U.S. Government Restricted-use Data

Unauthorized Access to Data (Individually Identifiable Information) on this Computer is a Violation of Federal Law and will Result in Prosecution.

Do You Wish to Continue? (Y)es or (N)o

N O T I C E

Proposed Publications Using Restricted-use Data

Sample Surveys and Evaluations

Licensees are required to round all unweighted sample size numbers to the nearest ten (nearest 50 for the Early Childhood Longitudinal Study Birth Cohort) in all information products (i.e., proposals, presentations, papers or other documents that are based on or use restricted-use data). Licensees are required to provide a draft copy of each information product that is based on or uses restricted-use data to the IES Data Security Office for a disclosure review. In the case of information products that are based on or use FERPA-protected restricted use data, the IES Data Security Office will also review the product to determine if, consistent with the approved project proposal, the Licensee used the data to conduct a study to improve instruction or as an "authorized representative of the Secretary" to evaluate a Federally supported education program. The Licensee must not release the information product to any person not authorized to access the data you are using until formally notified by IES that no potential disclosures were found and, if applicable, that no FERPA issues were identified. This review process usually takes 3 to 5 business days.

The PPO shall also forward a final copy of any public presentations or reports published or released that are based on or use restricted-use to the IES Data Security Office to provide feedback on uses of ESRA data.

Administrative Record/Universe Data

Licensees are required to follow the disclosure avoidance procedures transmitted with the restricted-use data in all information products (i.e., proposals, presentations, papers or other documents that are based on or use restricted-use data). Licensees are required to provide a draft copy of each information product that is based on or uses restricted-use data to the IES Data Security Office for a disclosure review. In the case of information products that are based on or use FERPA-protected restricted-use data, the IES Data Security Office will also review the product to determine if, consistent with the approved project proposal, the Licensee used the data to conduct a study to improve instruction or as an "authorized representative of the Secretary" to evaluate a Federally supported education program. The Licensee must not release the information product to any person not authorized to access the data you are using until formally notified by IES that no potential disclosures were found and, if applicable, that no FERPA issues were identified. This review process usually takes 3 to 5 business days.

The PPO shall also forward a final copy of any public presentations or reports published or released that are based on, or use FERPA-protected restricted-use data to the IES Data Security Office.

Signature Page – Management Review and Approval

I have reviewed the requirements of the License agreement and the security procedures in this plan that describe the required protection procedures for securing, accessing and using the restricted-use data.

I hereby certify that the computer system, physical location security procedures, and access procedures meet all of the License requirements and will be implemented for the duration of the project and License period.

Senior Official Signature	Date
Senior Official Name & Title (print)	Phone Number
Principal Project Officer Signature	Date
Principal Project Officer Name & Title (print)	Phone Number
System Security Officer Signature	Date
System Security Officer Name & Title (print)	Phone Number

Note: The National Center for Education Statistics (NCES) processes licenses and disseminates restricted-use data for all centers in the Institute of Education Sciences (IES) including the National Center for Education Research (NCER), the National Center for Education Statistics (NCES), the National Center for Education Evaluation (NCEE), and the National Center for Special Education Research (NCSER).

Security Plan Form:

Remote Access Only

Institute of Education Sciences (IES)
Restricted-use Data

Name of Institution / Organization: _____

PPO Name: _____

PPO Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

PPO Phone Number: _____

Type of Security Plan: New ☐ Renewal ☐ Modification ☐

License Number: _____

Physical Location of Data

Project Office Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

Project Office Phone Number: _____

Note: *The restricted-use data and computer must be secured and used **only** at this location. When the data are not being used, the data must be stored under lock and key at this location. Only authorized users of the data, as listed on the License, may have key access to this secure project office/room.*

Physical Security of Data

Describe Building Security:
(Describe building security arrangements where project office is located.)

Describe Project Office Security:
(Describe project office security arrangements for the room where the computer and data will be located.)

Computer Security Requirements

Describe Computer System:
(*Please read the **Note** below. Computer security must follow the requirements listed below.)*

Computer Operating System: _____

Anti-Virus Software Installed on Computer: _____

Note: *The restricted-use data must be copied to and run on a standalone, desktop computer.* ***Use of a laptop computer, external hard drive, or USB memory stick is strictly prohibited.*** *Absolutely no restricted-use data may be copied onto a server or computer that is attached to a modem or network (LAN) connection. Prior to attaching the computer to a modem or LAN connection, the restricted-use data must be purged and overwritten on the computer.*

The following computer security procedures must be implemented when in possession of restricted-use data. By checking the box next to each security procedure, you signify that these security procedures will be implemented for the duration of the project and License period:

- A password will be required as part of the computer login process. ☐
- The password for computer access will be unique and contain 6 to 8 characters with at least one non-alphanumeric character. ☐

- The computer password will change at least every 3 months or when project staff leave. ☐
- Read-only access will be initiated for the original data. ☐
- An automatic password protected screensaver will enable after 5 minutes of inactivity. ☐
- Restricted-use data will **not** be placed on a server (network), laptop computer, USB memory stick, or external hard drive. ☐
- Post Warning notification: During the computer log-in process, a warning statement (shown below) will appear on the computer screen before access is granted. If it is not possible to have the warning appear on the screen, it must be typed and attached to the computer monitor in a prominent location. ☐

W A R N I N G

U.S. Government Restricted-use Data

Unauthorized Access to Data (Individually Identifiable Information) on this Computer is a Violation of Federal Law and will Result in Prosecution.

Do You Wish to Continue? (Y)es or (N)o

N O T I C E

Proposed Publications Using Restricted-use Data

Sample Surveys and Evaluations

Licensees are required to round all unweighted sample size numbers to the nearest ten (nearest 50 for the Early Childhood Longitudinal Study Birth Cohort) in all information products (i.e., proposals, presentations, papers or other documents that are based on or use restricted-use data). Licensees are required to provide a draft copy of each information product that is based on or uses restricted-use data to the IES Data Security Office for a disclosure review. In the case of information products that are based on or use FERPA-protected restricted use data, the IES Data Security Office will also review the product to determine if, consistent with the approved project proposal, the Licensee used the data to conduct a study to improve instruction or as an "authorized representative of the Secretary" to evaluate a Federally supported education program. The Licensee must not release the information product to any person not authorized to access the data you are using until formally notified by IES that no potential disclosures were found and, if applicable, that no FERPA issues were identified. This review process usually takes 3 to 5 business days.

The PPO shall also forward a final copy of any public presentations or reports published or released that are based on or use restricted-use to the IES Data Security Office to provide feedback on uses of ESRA data.

Administrative Record/Universe Data

Licensees are required to follow the disclosure avoidance procedures transmitted with the restricted-use data in all information products (i.e., proposals, presentations, papers or other documents that are based on or use restricted-use data). Licensees are required to provide a draft copy of each information product that is based on or uses restricted-use data to the IES Data Security Office for a disclosure review. In the case of information products that are based on or use FERPA-protected restricted-use data, the IES Data Security Office will also review the product to determine if, consistent with the approved project proposal, the Licensee used the data to conduct a study to improve instruction or as an "authorized representative of the Secretary" to evaluate a Federally supported education program. The Licensee must not release the information product to any person not authorized to access the data you are using until formally notified by IES that no potential disclosures were found and, if applicable, that no FERPA issues were identified. This review process usually takes 3 to 5 business days.

The PPO shall also forward a final copy of any public presentations or reports published or released that are based on, or use FERPA-protected restricted-use data to the IES Data Security Office.

Signature Page – Management Review and Approval

I have reviewed the requirements of the License agreement and the security procedures in this plan that describe the required protection procedures for securing, accessing and using the restricted-use data.

I hereby certify that the computer system, physical location security procedures, and access procedures meet all of the License requirements and will be implemented for the duration of the project and License period.

Senior Official Signature	Date
Senior Official Name & Title (print)	Phone Number
Principal Project Officer Signature	Date
Principal Project Officer Name & Title (print)	Phone Number
System Security Officer Signature	Date
System Security Officer Name & Title (print)	Phone Number

Note: The National Center for Education Statistics (NCES) processes licenses and disseminates restricted-use data for all centers in the Institute of Education Sciences (IES) including the National Center for Education Research (NCER), the National Center for Education Statistics (NCES), the National Center for Education Evaluation (NCEE), and the National Center for Special Education Research (NCSER).

License #_____

Affidavit of Nondisclosure

_____ (Job Title)

_____ (Date Assigned to Work with IES Data)

_____ (Organization, State or Local Agency Name)

_____ (Organization or Agency Address)

(NCES Database or File Containing Individually Identifiable Information*)

I, _____ , do solemnly swear (or affirm) that when given access to the subject IES database or file, I will not -

(i) use or reveal any individually identifiable information furnished, acquired, retrieved or assembled by me or others, under the provisions of Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279) for any purpose other than statistical, research, or evaluation purposes specified in the IES survey, project or contract;

(ii) make any disclosure or publication whereby a sample unit or survey respondent (including students and schools) could be identified or the data furnished by or related to any particular person or school under these sections could be identified; or

(iii) permit anyone other than the individuals authorized by the Director of the Institute of Education Sciences to examine the individual reports.

_____
(Signature)

[The penalty for unlawful disclosure is a fine of not more than $250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both. The word "swear" should be stricken out when a person elects to affirm the affidavit rather than to swear to it.]

City/County of _____ Commonwealth/State of _____ .
Sworn to and subscribed before me this _____ day of
_____, 20_____ . Witness my hand and official Seal.

_____
(Notary Public/Seal)

My commission expires_____ .

* Request all subsequent follow-up data that may be needed. This form cannot be amended by NCES, so access to databases not listed will require submitting additional notarized Affidavits.

Form last revised 08/06/19