MEMORANDUM OF UNDERSTANDING
BETWEEN
Click or tap here to enter text.
AND
THE KENTUCKY DEPARTMENT OF EDUCATION
TO AUTHORIZE THE RELEASE AND USE OF CONFIDENTIAL DATA
\*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\* \*\*\*

**THIS AGREEMENT** is made and entered into by and between the Kentucky Department of Education (“KDE”) and Click or tap here to enter text., (“Approved Data Recipient”) collectively the “parties,” and establishes the procedures relating to an exchange of information between the parties.

**WHEREAS**, various elements of the data maintained by KDE are protected by the Privacy Act of 1974, 5 U.S.C. 552a; and the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.;

**WHEREAS**, the parties agree that the data being provided will be treated as “confidential” as the term is used in this agreement.

**NOW THEREFORE**, the KDE and Click or tap here to enter text. (Approved Data Recipient) hereby mutually agree as follows:

# Section 1. Identification of the Approved Data Recipient as Organization to Receive Confidential Data.

1. The KDE and the Approved Data Recipient hereby agree that the Approved Data Recipient is an entity to whom the KDE can disclose, upon written request, data KDE compiled and maintains.
2. The KDE and the Approved Data Recipient hereby agree that no student data, including confidential data protected under the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. 1232g; the Individuals with Disabilities Act, 20 U.S.C. 1400 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; or the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq. will be disclosed to the Approved Data Recipient.
3. The KDE and the Approved Data Recipient agree that under no circumstances will any data be used, published or disseminated in a manner that could reasonably lead to the personal identification of an individual unless such disclosure is to an entity listed as Data Custodians in Exhibit E.

# Section 2. The Approved Data Recipient and the Authorized Users’ Obligations.

1. The Approved Data Recipient shall not share these confidential data with anyone, except those employees of the Approved Data Recipient and the Approved Data Recipient’s subcontractors listed on Exhibit E, or other Data Custodians as listed in Exhibit E (“Authorized Users").
2. The Approved Data Recipient shall require and maintain confidentiality agreements or the KDE’s Nondisclosure Statement(s) with each Authorized User of confidential data. If a confidentiality agreement with each Authorized User is used, which is different from the KDE Nondisclosure Statement(s), then the terms of the Approved Data Recipient’s confidentiality agreements shall contain, at a minimum, the terms and conditions of this agreement and a copy of the current Approved Data Recipient’s confidentiality agreement or the KDE’s Nondisclosure Statement(s), as appropriate, shall be attached to this agreement as Exhibit B.
3. An Approved Data Recipient that receives Personal Information as defined by and in accordance with Kentucky’s Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the “Act”), shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to “non-affiliated third parties” set forth in the Act.

“Personal Information” is defined in accordance with KRS 61.931(6) as “an individual’s first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

1. An account number, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
2. A Social Security number;
3. A taxpayer identification number that incorporates a Social Security number;
4. A driver’s license number, state identification card number or other individual identification number issued by an agency;
5. A passport number or other identification number issued by the United States government; or
6. Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Education Rights and Privacy Act, as amended 20 U.S.C. sec 1232g.”

As provided in KRS 61.931(5), a “non-affiliated third party” means any person that has a contract or agreement with KDE and receives (accesses, collects or maintains) personal information from KDE pursuant to the contract or agreement.

Approved Data Recipient shall not redisclose, without written consent of the KDE, any “personal information,” as defined in KRS 61.931(6), or any other personally identifiable information of a student or other persons, such as employees.

1. The Approved Data Recipient hereby agrees to cooperate with KDE in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.
2. The Approved Data Recipient shall notify as soon as possible, but not to exceed seventy-two (72) hours, KDE, the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Kentucky Attorney General, and the Commonwealth Office of Technology of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)2 applies and the Approved Data Recipient abides by the requirements set forth in that exception. If the agency is a unit of government listed in KRS 61.931(1)(b), the Approved Data Recipient shall notify the Commissioner of the Department of Local Government in the same manner as above. If the agency is a public school district listed in KRS 61.931(1)(d), the Approved Data Recipient shall notify the Commissioner of the Department of Education in the same manner as above. If the agency is an educational entity listed under KRS 61.931(1)(e), the Approved Data Recipient shall notify the Council on Postsecondary Education in the same manner as above. Notification shall be in writing on the form developed by the Commonwealth Office of Technology and incorporated by reference into Kentucky Regulation 200 KAR 1:016.
3. The Approved Data Recipient hereby agrees that KDE may withhold payment(s) owed to the Approved Data Recipient for any violation of the Identity Theft Prevention Reporting Requirements.
4. The Approved Data Recipient hereby agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.
5. Upon conclusion of an investigation of a security breach of Personal Information as required by KRS 61.933, the Approved Data Recipient hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach.
6. In accordance with KRS 61.932(2)(a) the Approved Data Recipient shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices established by the Commonwealth Office of Technology that are available here: [https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx](https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies%2CStandardsandProcedures.aspx).
7. If Approved Data Recipient is a cloud computing service provider (as defined in KRS 365.734(1)(b) as “any person or entity other than an educational institution that operates a cloud computing service”), Approved Data Recipient does further agree that:
	1. Approved Data Recipient shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services unless the provider receives express permission from the student’s parent. The Approved Data Recipient shall work with the student’s school and district to determine the best method of collecting parental permission. KRS 365.734 defines “process” and “student data.”
	2. With a written agreement for educational research, Approved Data Recipient may assist an educational institution in conducting educational research as permitted by the Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C. Sec.1232g.
	3. Pursuant to KRS 365.734, Approved Data Recipient shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
	4. Pursuant to KRS 365.734, Approved Data Recipient shall not sell, disclose, or otherwise process student data for any commercial purpose.
	5. Pursuant to KRS 365.734, Approved Data Recipient shall certify in writing, by its signature on this MOU, that it will comply with KRS 365.734(2).
8. The Approved Data Recipient shall protect confidential and otherwise personally identifiable data in a manner that does not permit personal identification of students, parents, educators, administrative staff and non-students by anyone except those bound by this agreement and the KDE. The Approved Data Recipient shall store all confidential data on secure data servers using current industry best practices. The Approved Data Recipient shall notify the KDE as soon as practicable if the Approved Data Recipient learns of any security breach to the server containing the confidential and otherwise personally identifiable data or of any disclosure of confidential and otherwise personally identifiable data to anyone other than the Approved Data Recipient’s Authorized Users or the KDE officials authorized to receive confidential and otherwise personally identifiable data. The Approved Data Recipient shall cooperate and take all reasonable means prescribed by the KDE to secure any breaches as soon as practicable.
9. The Approved Data Recipient shall not redisclose the KDE’s confidential and otherwise personally identifiable data to any other party without the prior consent of the parent, teacher, employee, eligible student, or non-student except as allowed by applicable federal and state law.
10. The Approved Data Recipient certifies that it has the capacity to restrict access to confidential and otherwise personally identifiable data solely to Authorized Users and to ensure that the confidential and otherwise personally identifiable data is accessed only for the purposes described in this agreement. A copy of the Approved Data Recipient’s data security policies and procedures is attached to this agreement as Exhibit C.
11. The Approved Data Recipient shall destroy all confidential and otherwise personally identifiable data within forty-five (45) days after it is no longer needed to perform the use and purpose described in this agreement, upon KDE’s request or upon termination of this agreement, whichever occurs first unless agreed otherwise in writing. The Approved Data Recipient’s description of the method(s) which will be used to destroy all confidential and otherwise personally identifiable data shall be attached to this agreement as Exhibit D. The Approved Data Recipient shall provide written verification of the data destruction to the KDE within forty-five (45) days after the data is destroyed by completing Exhibit F.
12. The Approved Data Recipient shall permit the KDE, at the KDE’s cost and upon written reasonable request, to audit the Approved Data Recipient to confirm that the Approved Data Recipient is complying with the data security policies and procedures in Exhibit C, maintaining and having on file confidentiality agreements or the KDE’s Nondisclosure Statement(s) for each Authorized User of confidential data, and/or that the Approved Data Recipient has destroyed the data as verified.
13. The Approved Data Recipient shall collect and use these confidential and otherwise personally identifiable data only for the purposes and related to the activities outlined in this agreement or in any overarching agreement between KDE and the Approved Data Recipient (“Master Agreement”).
14. The Approved Data Recipient shall obtain prior written approval from the KDE before accessing confidential and otherwise personally identifiable data for activities beyond the scope specified in this agreement or in a Master Agreement; and any access beyond the scope of this agreement or a Master Agreement shall be consistent with federal and Kentucky law requirements. If Approved Data Recipient requests written approval from KDE based on a Master Agreement, then Approved Data Recipient shall include a copy of the operative Master Agreement in their request. Any confidential and otherwise personally identifiable data collected by the Approved Data Recipient under activities approved by the KDE under this section, which are not regularly collected within the scope of this agreement but are consistent with the activities described in this agreement, shall be subject to the terms and conditions of this agreement.
15. If the Approved Data Recipient becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then the Approved Data Recipient shall use all reasonable efforts to provide the KDE with prior notice before disclosure so that the KDE may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure the KDE’s compliance with the confidentiality requirements of federal or Kentucky law; provided, however, that the Approved Data Recipient will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, the Approved Data Recipient will only disclose that portion of confidential and otherwise personally identifiable data that the Approved Data Recipient is legally required to disclose.

# Section 3. Disclosure of Data not an Endorsement of the Studies.

TheKDE is not required to agree with or endorse the conclusions or results of the studies. At least five days prior to Approved Data Recipient’s public disclosure of conclusions or results of the studies, the Approved Data Recipient shall provide a copy of conclusions, results, or product(s) resulting from the study (e.g., article, report, book, etc.) to the KDE Chief Data Officer via email to KDE Data Services (kdedatarequest@education.ky.gov). No later than 45 days following the end date of the studies, the Approved Data Recipient shall provide their conclusions, results, or product(s) of the studies.

# Section 4. Transfer Protocol.

The KDE and the Approved Data Recipient shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. The Approved Data Recipient shall confirm the transfer of confidential data and notify the KDE as soon as practicable of any discrepancies between the actual data transferred and the data described in this agreement. The same protocol shall apply to any transfer of confidential data from the Approved Data Recipient to the KDE.

# Section 5. Breach of Data Confidentiality.

The Approved Data Recipient acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to the KDE for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by the Approved Data Recipient, the KDE, in addition to any other rights and remedies available to the KDE at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach.

# Section 6. Amendment and Assignability.

The terms and conditions of this agreement may only be amended by mutual written consent of both the KDE and the Approved Data Recipient, and the Approved Data Recipient shall not assign its respective rights or obligations under this agreement without prior written consent of the KDE. The rights and obligations of each party under this agreement shall inure to the benefit of and shall be binding upon that party and its respective successors and assigns.

# Section 7. Choice of Law and Forum.

All questions as to the execution, validity, interpretation, construction, or performance of this agreement shall be governed by the laws of the Commonwealth of Kentucky. Any suit, action, or other proceeding regarding the execution, validity, interpretation, construction, or performance of this agreement shall be filed in the Franklin Circuit Court of the Commonwealth of Kentucky.

# Section 8. Waiver.

The failure by one party to require performance of any provision shall not affect that party's right to require performance at any time thereafter, nor shall a waiver of any breach or default of this agreement constitute a waiver of any subsequent breach or default or a waiver of the provision itself. No modification, amendment, waiver or release of any provision of this agreement or of any right, obligation, claim or cause of action arising from this agreement shall be valid or binding for any purpose unless in writing and duly executed by the party against whom they are asserted.

# Section 9. Severability.

Any provision of this agreement that is declared invalid by a court of competent jurisdiction or by operation of law, shall not affect the validity or enforceability of any other provision of this agreement.

# Section 10. Authority to Enter the Agreement.

The KDE and the Approved Data Recipient represent and warrant, by the signatures of their duly appointed representatives, that they are legally entitled to enter into this agreement.

# Section 11. Data Custodians.

The individuals who are the designated data custodians for the Approved Data Recipient with respect to this agreement are listed with their contact information in Exhibit E.

# Section 12. Term and Termination.

The term of this agreement shall be the latter of the duration set forth in Exhibit A or the date the requirements for destruction of all confidential and otherwise personally identifiable data are met which includes submittal of a completed Exhibit F to KDE. Agreement will be effective until KDE receives notification that data has been destroyed. The duration of this agreement shall not modify the term of the Master Agreement, if one exists, between the KDE and the Approved Data Recipient. Either party may cancel this agreement at any time for cause or may cancel without cause on thirty (30) days’ written notice.

# Section 13. Effective Date and Term of the Agreement.

This agreement will become effective once the KDE and the Approved Data Recipient have both signed.

# APPROVED:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signature/Date**

**Robin Kinney, Interim Commissioner
Kentucky Department of Education**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved Data Recipient’s Authorized Agent Signature/Date

Approved Data Recipient Authorized Agent’s Name: Click or tap here to enter text.

Approved Data Recipient Authorized Agent’s Title: Click or tap here to enter text.

Approved Data Recipient Entity Name: Click or tap here to enter text.

Memorandum of Understanding (MOU)

# Description of Exhibits

**To authorize the release and use of confidential data**

Exhibits referenced in the Memorandum of Understanding must be completed and incorporated into the final MOU. Exhibits include:

* Exhibit A - The initial data request that describes the study and data being requested
* Exhibit B - Approved Data Recipient Confidentiality Agreements (one for each data custodian)
* Exhibit C - Approved Data Recipient data security policy
* Exhibit D - Data destruction plan at completion of study
* Exhibit E - Identification of data custodians
* Exhibit F – Approved Data Recipient’s Certificate of Data Destruction

# Exhibit A: The approved KDE Data Request Form may be inserted for Exhibit A, Sections I and II.

### Section I – Required for all requestors:

#### Contact Information

Approved Data Recipient Legal Name: Click or tap here to enter text.

Primary Data Custodian Name: Click or tap here to enter text., Title:Click or tap here to enter text.

Phone:Click or tap here to enter text. Email:Click or tap here to enter text.

Secondary Data Custodian Name: Click or tap here to enter text., Title: Click or tap here to enter text.

Phone:Click or tap here to enter text. Email: Click or tap here to enter text.

#### Purpose, Scope and Duration

Use of data received under this MOU is limited to purpose and scope defined.

#### Completely describe the purpose and scope of the study:

Click or tap here to enter text.

#### Describe how the results will be used. Include the KDE strategic objectives and initiatives supported by the study:

Click or tap here to enter text.

##### Duration of Study

### **Start Date:** Click or tap to enter a date. **End Date:**  Click or tap to enter a date.

#### Data Being Requested

##### Provide specific data elements needed to complete study:

Click or tap here to enter text.

##### School Years Included in Study:

[ ] 2023-24 [ ] 2022-23 [ ] 2021-22 [ ] 2020-21 [ ] 2019-20 [ ] 2018-19 [ ] 2017-18 [ ] 2016-17 [ ] 2015-16 [ ] 2014-15 [ ]  2013-14 [ ] 2012-13 [ ]  2011-12 [ ] 2010-11 [ ] 2009-10 [ ] 2008-09 [ ]  Other: Click or tap here to enter text.

##### Level of detail/aggregation:

[ ]  Individual [ ]  School [ ]  District [ ]  State

# Exhibit B: Approved Data Recipients Employee or Contractor Nondisclosure Statement

[*Click here to download the Nondisclosure Statement form*](https://www.education.ky.gov/_layouts/download.aspx?SourceUrl=https://www.education.ky.gov/districts/tech/Documents/MOU_NonStudentData_ExhibitB.docx)*, which can be used for making multiple copies. After entering each data custodian’s information into the form fields, print and obtain the required signatures. Include the completed Nondisclosure Statements or confidentiality agreement with your proposed MOU.*

Approved Data Recipient’s Name: Click or tap here to enter text.

Approved Data Recipient’s employee or contractor name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Address: Click or tap here to enter text. Phone: Click or tap here to enter text.

I understand that the performance of my duties as an employee or contractor, of an Approved Data Recipient for the Kentucky Department of Education (KDE), may involve a need to access and review confidential information and, that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under the law as stated below. By signing this document, I agree to the following:

* I will not permit access to confidential information to persons not authorized by the KDE and its Approved Data Recipient.
* I will maintain the confidentiality of the data or information.
* I will not access data of persons related or known to me for personal reasons.
* I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in the KDE survey, project, or proposed research.
* I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
	+ to my immediate supervisor, Associate Commissioner, and
	+ to the Division of Human Resources if I am a KDE employee or
	+ to the KDE Office for whom I perform work under this agreement if I am an Approved Data Recipient or an employee of an Approved Data Recipient
* I understand that procedures must be in place for monitoring and protecting confidential information.
* I understand that KRS 61.931 defines “personal information” to include an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
	1. An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
	2. A Social Security number;
	3. A taxpayer identification number that incorporates a Social Security number;
	4. A driver's license number, state identification card number, or other individual identification number issued by any agency;
	5. A passport number or other identification number issued by the United States government; or
	6. Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
* I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
* I understand that any personal characteristics that could make the person’s identity traceable, including membership in a group such as ethnicity or program area, are protected.
* In addition, I understand that any data sets or output reports that I may generate using confidential data are to be protected. I will not distribute to any unauthorized person any data sets or reports that I have access to or may generate using confidential data. I understand that I am responsible for any computer transactions performed as a result of access authorized by use of sign on/password(s).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Approved Data Recipient’s employee or contractor signature/ Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Approved Data Recipient’s authorized agent signature/ Date

Approved Data Recipient’s authorized agent name (typed): Click or tap here to enter text.

# Exhibit C:

Please describe the measures you take to ensure the protection of the data released to you. If you have a policy, please attach or copy/paste here as Exhibit C. (If using a delivery method other than KDE’s managed file transfer service (MOVEit), include information on the requested delivery method. Please note that PII can only be shared using secure/encrypted methods.

Click or tap here to enter text.

# Exhibit D:

Please describe the methods Approved Data Recipient will use to irrevocably destroy, wipe or sanitize all personal or confidential data at the completion of the study. This includes all formats and media including but not limited to paper, electronic, magnetic as well as any internal hard drive of a printer or copier prior to its disposal, relocation or being sent to surplus. Please specify the planned date of destruction for each format and media that is applicable. If you have a policy that describes the methods you will use to destroy all confidential data, it can be attached as Exhibit D. Approved Data Recipient's Certificate of Destruction (Exhibit F) is required for certification that all forms of personal or confidential data have been irrevocably destroyed, wiped or sanitized.

Click or tap here to enter text.

# Exhibit E:

In alphabetical order by last name, provide information for those persons designated as data custodians. This should include anyone with access to confidential data. A designated primary and secondary data custodian are required and a minimum of four are requested. A signed Confidentiality Agreement or KDE’s Nondisclosure Statement labeled Exhibit B is required for each data custodian.

Prior to designating additional data custodians who are not listed on Exhibit E at the time the MOU is executed, Approved Data Recipient must submit a written request and an MOU amendment will be required.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Last Name** | **First Name** | **Email** | **Phone** | **Employer** |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |
| Last | First | Email | Phone | Employer |

# Exhibit F: Approved Data Recipient’s Certificate of Data Destruction

The Approved Data Recipient shall irreversibly destroy all copies of all confidential and otherwise personally identifiable data regardless of format (e.g., paper, electronic) within forty-five (45) days after it is no longer needed to perform the studies described in this agreement, upon KDE’s request or upon termination of this agreement, whichever occurs first unless agreed otherwise in writing. Using this form, the Approved Data Recipient shall provide written verification of the data destruction to the KDE within forty-five (45) days after the data is destroyed. Scan the signed Certificate of Data Destruction and return it to KDE Data Services (kdedatarequest@education.ky.gov).

If the Approved Data Recipient uses a contractor for data destruction services, a certificate of destruction from the contractor is also required. Please submit the contractor’s certificate of destruction with this signed Certificate of Data Destruction.

Approved Data Recipient Entity’s Name: Click here to enter text.

MOU Number: Click here to enter text. (If you do not know your MOU identification number, contact KDE by email at kdedatarequest@education.ky.gov.

In accordance with the provisions of the Memorandum of Understanding (MOU) between the Kentucky Department of Education and the (“Approved Data Recipient”), the confidential and otherwise personally identifiable data were destroyed as required in Section 2(N) according to the methods described in Exhibit D of the MOU.

Date submitted: Click here to enter a date.
Scheduled date of destruction (per MOU): Click here to enter a date.
Actual destruction date: Click here to enter a date.

##### Description of records disposed of:

| **Media type** | **Method of Destruction** | **Comments** |
| --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |

I hereby certify that all confidential and otherwise personally identifiable data described above have been destroyed in the manner indicated.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Approved Data Recipient’s Authorized Agent Signature / Date

Agent’s Name (Typed): Click here to enter text., Agent’s Title: Click here to enter text.