CPE DATA GOVERNANCE POLICY

Data Access and Security Policy

This Policy at a Glance

- CPE releases data in three tiers. The tier decides what a requester must sign.
- Every external request for data that is not already published starts with Form DG-1, External Data Request.
- Student-level data leaves CPE only under a signed Form DG-2, Data Sharing Agreement. Each agreement names one purpose and one legal basis.
- Every person who handles confidential data signs a confidentiality agreement. Outside staff sign Form DG-3. CPE staff sign Form DG-4.
- Every agreement closes with Form DG-5, Certificate of Data Destruction.

I. Policy Statement

The Kentucky Council on Postsecondary Education (CPE) collects and maintains data that include confidential personal information and student education records. CPE uses these data for state and federal reporting, funding calculations, accountability, research, and policy analysis. CPE does not disclose confidential information or personally identifiable information from education records except as permitted by the Family Educational Rights and Privacy Act (FERPA), Kentucky law, and this policy.

CPE also holds confidential data that it receives from other agencies and partners. This policy applies to those data as well. Any added requirements in the agreements under which CPE received the data also apply.

II. Purpose

This policy sets the rules for how CPE collects, protects, shares, and disposes of confidential data. It also creates one process for handling every external data request. The goal is straightforward. Researchers, partners, and the public should know what data they can get, what they must sign to get it, and how long it will take.

III. Scope

This policy applies to all CPE employees, interns, contractors, and vendors. It also applies to any outside organization or individual that requests or receives CPE data. It covers data in any form, including database extracts, files, reports, dashboards, and printed materials.

This policy does not govern requests made under the Kentucky Open Records Act (KRS 61.870 to 61.884). CPE's records custodian handles those requests under that law. Education records protected by FERPA remain confidential under either process.

IV. Legal Authority

This policy carries out the requirements of the following laws. Where a law or an agreement sets a stricter standard than this policy, the stricter standard applies.

- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and its regulations at 34 C.F.R. Part 99.
- KRS 164.283, which makes student academic records at Kentucky public postsecondary institutions confidential and permits CPE access for professional academic research.
- KRS 164.991, which sets penalties for violations of KRS 164.283.
- KRS 61.931 to 61.934, which set security and breach notification requirements for personal information held by state agencies and their contractors.
- KRS 151B.132, which establishes the Kentucky Longitudinal Data System.

V. Definitions

Key Terms

Term	Meaning in this policy
Aggregate data	Counts, rates, averages, or other summary statistics about groups of students.
Authorized representative	An individual or organization that CPE designates in writing to conduct an audit or evaluation of a federal- or state-supported education program, or a related compliance or enforcement activity (34 C.F.R. 99.3 and 99.35).
Data custodian	Any person who has access to CPE confidential data under an agreement with CPE.
Data Sharing Agreement	The written agreement (Form DG-2) that governs any release of Tier 3 data. It replaces the general "Memorandum of Understanding" used in earlier versions of this policy.
De-identified data	Student-level data from which personally identifiable information has been removed or obscured so that a reasonable person could not identify a student with reasonable certainty (34 C.F.R. 99.31(b)).
Disclosure	Permitting access to, or releasing, transferring, or communicating, personally identifiable information from education records by any means.
Education record	A record directly related to a student and maintained by an educational agency or institution, or by a party acting for it (20 U.S.C. 1232g(a)(4)(A); 34 C.F.R. 99.3).
KPEDS	The Kentucky Postsecondary Education Data System. It is CPE's authoritative collection of student-level data submitted by Kentucky colleges and universities.
Kentucky Longitudinal Data System	The statewide education and workforce data system established under KRS 151B.132 and managed by the Kentucky Center for Statistics (KYSTATS).
Personally identifiable information (PII)	Information that identifies a student directly, such as a name or student ID number, or indirectly, such as a date of birth or a combination of traits. It includes any information that, alone or in combination, would allow a reasonable person in the school community to identify a student with reasonable certainty (34 C.F.R. 99.3).
Redisclosure	Sharing data received from CPE with any person or organization not authorized in the agreement under which the data were released.
Student-level data	Data in which each record represents one student.
Suppression	Withholding or masking values in a table to prevent disclosure about small groups. Complementary suppression masks additional values so that suppressed values cannot be calculated from totals.

VI. Data CPE Collects and Maintains

CPE collects records from Kentucky postsecondary institutions and receives data from partner agencies. These collections include the following kinds of information.

- Student identifying and demographic information, such as name, student ID, Social Security number, date of birth, sex, race and ethnicity, and residency.
- Enrollment, course, and academic progress data, including credit hours, grade point average, and degrees and credentials earned.
- Financial aid and eligibility data, such as Pell Grant and KEES status.
- Institutional data on employees, finances, facilities, and academic programs.
- Data received from partner agencies under interagency agreements.

CPE's data reporting guidelines and the KPEDS data dictionary describe each collection in detail. All CPE data systems and collections are subject to this policy.

VII. Data Tiers

CPE sorts every data release into one of three tiers. The tier depends on how much risk the release carries for student privacy. The tier also decides what the requester must complete before CPE releases the data.

CPE Data Tiers for External Release

Tier	What it includes	Examples	What the requester needs
Tier 1 *Public*	Aggregate data that CPE has already published. Small cells were suppressed before publication.	Enrollment and degrees by institution and sector; Progress Report and accountability metrics; CPE dashboards and data portal.	Nothing. CPE staff point the requester to the published source.
Tier 2 *Restricted aggregate*	Custom aggregate tables that CPE has not published, including breakouts by demographic group, institution, or program.	Retention by race and ethnicity at one institution; custom transfer or college-going tables.	Form DG-1. CPE applies suppression rules before release. No agreement is needed.
Tier 3 *Confidential*	Student-level records, whether identified or de-identified, and any aggregate tables with unsuppressed small cells.	Research studies, program evaluations, and linkage projects with partner data.	Form DG-1, an approved Form DG-2 agreement, and a Form DG-3 for each data custodian. Form DG-5 at close-out.

VIII. Who May Access CPE Data

CPE Staff, Interns, and Contractors

CPE staff receive access to confidential data only as needed for their assigned duties. A supervisor must approve each request for system access. Every staff member with access signs Form DG-4 at onboarding and again each year. Staff may not use CPE data for personal purposes that are not educational. Educational uses, such as dissertation research, require an approved Form DG-1, like any other external request.

Vendors and Service Contractors

A vendor may receive confidential data when it performs a service that CPE would otherwise perform with its own staff and when CPE directly controls its use of the data (34 C.F.R. 99.31(a)(1)(i)(B)). The vendor's contract must include the security and breach terms that KRS 61.932 requires. Each vendor employee with access signs Form DG-3.

State Agency Partners

CPE shares data with the Kentucky Longitudinal Data System under KRS 151B.132 and its interagency agreement with KYSTATS. CPE shares data with other state agencies only under a statute-specific interagency agreement. CPE's Office of General Counsel negotiates these agreements.

Researchers and Evaluators

Researchers and evaluators may receive Tier 2 data through Form DG-1. They may receive Tier 3 data only through a Form DG-2 agreement under one of the three purposes described in Section X.

Kentucky Colleges and Universities

Institutions may request comparative or statewide data through Form DG-1. Institutions should obtain records about their own students from their own systems. Any request that involves student-level data from other institutions is a Tier 3 request.

Students and Parents

CPE is not the official record holder for individual students. Students and parents seeking education records should contact the institution the student attended.

The Public, Media, and Policymakers

Anyone may use Tier 1 data. Members of the public, the media, and policymakers may also request Tier 2 data through Form DG-1.

IX. External Data Request Process

Every external request follows the same steps. Tier 1 requests usually end at Step 1. Tier 2 requests skip the agreement steps. The target times below begin when CPE receives a complete request.

External Data Request Process at a Glance

Step	What happens	Who	Form	Target time
1. Check published data	CPE staff point the requester to published reports and dashboards that may already answer the question.	Requester and DAA	None	2 business days
2. Submit request	The requester submits Form DG-1 online or e-mails a completed copy to CPE Data and Advanced Analytics (DAA).	Requester	DG-1	Not applicable
3. Initial review	DAA assigns the tier, confirms the purpose and legal basis, and narrows the request to the minimum necessary data.	DAA	DG-1	10 business days
4. Tier 2 release	DAA prepares the tables, applies suppression, completes a second-person check, and releases them.	DAA	DG-1	15 business days after review
5. Agreement	For Tier 3, DAA drafts the agreement with the requester. General Counsel reviews it. Both parties sign.	DAA, General Counsel, requester	DG-2, DG-3	60 to 90 days
6. Secure release	DAA prepares the approved file, transfers it securely, and logs the disclosure.	DAA	None	15 business days after signature
7. Monitoring	The recipient submits planned publications for disclosure review and confirms compliance each year.	Recipient and DAA	Annual attestation	30 days before publication
8. Close-out	The recipient destroys the data and returns a signed destruction certificate.	Recipient	DG-5	30 days after the agreement ends

How CPE Decides on Tier 3 Requests

CPE approves a Tier 3 request only when it meets all of the following conditions.

1. The request fits one of the three agreement purposes in Section X and a valid legal basis under FERPA.
2. The work is consistent with CPE's statutory duties and is likely to benefit Kentucky postsecondary education. Requests that align with CPE's research agenda receive priority.
3. The data requested are the minimum necessary for the stated purpose.
4. The requester has an adequate plan to secure, use, and destroy the data.
5. CPE has the staff capacity to prepare the data within a reasonable time.
6. The requester and its staff have not violated a prior CPE agreement or been barred from access under FERPA.

CPE may deny, narrow, or delay any request. When it does, DAA will explain why in writing. Requesters submit Form DG-1 online at https://cpe.ky.gov/data/request.html. Requesters who prefer e-mail may send a completed copy of Form DG-1 to CPEDataRequest@ky.gov.

X. Data Sharing Agreements

Each Data Sharing Agreement states one purpose. The purpose determines the legal basis, the data CPE can release, and the terms the recipient must follow. A project that has more than one purpose needs more than one agreement or a written amendment. Form DG-2 covers Purposes A, B, and C. Interagency data sharing and vendor services use the separate instruments shown in the table.

Data Sharing Agreement Types

Agreement type	Use it when	Legal basis	Data allowed	Instrument
Purpose A *Research Study*	An outside organization conducts a study for, or on behalf of, CPE or Kentucky institutions. The study must aim to develop or validate tests, administer student aid programs, or improve instruction.	FERPA studies exception, 34 C.F.R. 99.31(a)(6)	Identified student-level data, minimum necessary	Form DG-2
Purpose B *Audit or Evaluation*	CPE designates an outside party to audit or evaluate a federal- or state-supported education program, or to support related compliance work.	FERPA audit or evaluation exception, 34 C.F.R. 99.31(a)(3) and 99.35	Identified student-level data, minimum necessary	Form DG-2
Purpose C *De-identified Data Use*	The project does not need to know who students are. CPE removes identifiers before release and may attach a random research code.	De-identification, 34 C.F.R. 99.31(b)	De-identified student-level data	Form DG-2
Interagency *State Partners*	A state agency receives data under a specific statute, such as the Kentucky Longitudinal Data System.	Governing statute and FERPA	As set in statute and agreement	Interagency agreement
Vendor *Service Contract*	A contractor performs a service for CPE under CPE's direct control.	FERPA school official exception and KRS 61.932	Only what the service needs	Contract with data terms

What Every Agreement Must Include

- The single purpose of the project and the legal basis for disclosure.
- A description of the work detailed enough to show how the data serve that purpose.
- A list of the data elements, populations, and years to be released.
- The names of every person who will access the data. Each must sign Form DG-3.
- Security requirements for storage, transfer, and access.
- A ban on redisclosure and on any attempt to identify individual students.
- Publication review and suppression requirements.
- Breach notification requirements.
- A term that ends on a set date and a deadline for destroying the data.

Term, Changes, and Renewal

An agreement lasts only as long as the project needs. It may not exceed three years. Any change to the purpose, data, or term requires a written amendment signed by both parties. The recipient may add data custodians by written notice to DAA and a signed Form DG-3. CPE will not release data until the new custodian's form is on file. Recipients confirm compliance with their agreement each year.

XI. Safeguards for Confidential Data

Everyone who handles CPE confidential data must follow these safeguards. They apply to CPE staff and to every outside recipient.

- **Access.** Grant access only to people who need it for an approved purpose. DAA keeps a current list of staff with access to PII and reviews it each year and whenever staff change roles or leave.
- **Encryption.** Encrypt confidential data in transit and at rest.
- **Transfer.** Move student-level data only through a CPE-approved secure file transfer service. Never send it as an ordinary e-mail attachment. If a password-protected file is used, send the password through a separate channel.
- **Storage.** Store confidential data only on CPE-managed systems or on systems approved in the agreement. Do not store it on personal devices, personal cloud accounts, or unencrypted removable media.
- **Online tools.** Do not enter confidential data into public generative AI tools or any online service that CPE has not approved for confidential data.
- **Workspace.** Lock screens when away. Keep printed confidential material secured. Shred it when it is no longer needed. Do not send confidential data by fax.
- **Labeling.** Mark any media or printed report that contains confidential data as confidential before it leaves CPE.

CPE staff must also follow the enterprise security and acceptable use policies of the Commonwealth Office of Technology.

XII. De-identification and Suppression Standards

De-identification

CPE releases data in de-identified or aggregate form unless an agreement under Purpose A or B allows identified data. De-identified files exclude names, Social Security numbers, student ID numbers, addresses, e-mail addresses, phone numbers, and full dates of birth. CPE also reviews indirect identifiers. When a combination of traits could single out a student, CPE will group categories, use ranges instead of exact values, or remove fields.

For education research, CPE may attach a random record code to each de-identified record so that files can be matched over time (34 C.F.R. 99.31(b)(2)). The code is never based on a Social Security number or other PII. CPE does not share the method used to create it.

Suppression

Any table released outside CPE must follow the standards below. Report authors are responsible for applying them, whether they work inside CPE or outside it.

CPE Suppression Standards

Rule	Standard
Small cells	Suppress any value based on fewer than 10 students.
Complementary suppression	Suppress additional values when a suppressed value could be calculated from totals or from other cells.
Extreme percentages	Suppress percentages of 0 or 100 for any demographic group.
Placeholder	Show suppressed values with an asterisk (*) and include a note explaining it.
Exceptions	The Executive Director of DAA may approve an exception in writing when the release would not disclose PII, such as a count of institutions rather than students.

XIII. Record of Disclosures

FERPA requires CPE to keep a record of each disclosure of PII from education records (34 C.F.R. 99.32). DAA maintains this record. Each entry lists the requester and organization, the date of disclosure, the data disclosed, the purpose and legal basis, the agreement number, and the date CPE received the destruction certificate.

XIV. Retention and Destruction

CPE keeps its own records according to the records retention schedules approved for state agencies. Outside recipients must destroy CPE data when it is no longer needed for the approved purpose or when the agreement ends, whichever comes first. Destruction must happen within 30 days and must cover all copies, extracts, and backups. Electronic data must be

destroyed using methods consistent with NIST Special Publication 800-88. The recipient confirms destruction by returning Form DG-5 to DAA.

XV. Security Incidents

Anyone who suspects that CPE confidential data has been lost, stolen, or accessed or disclosed without authorization must report it right away. CPE staff report to their supervisor and to DAA at CPEDataRequest@ky.gov. Outside recipients must notify DAA within 24 hours of discovery. That is sooner than the 72-hour outer limit that KRS 61.932 sets for contractors. All parties must cooperate with any investigation. CPE will meet the notice requirements of KRS 61.931 to 61.934.

XVI. Training and Annual Acknowledgment

All CPE staff with access to confidential data complete data privacy and security training at onboarding and each year after that. Each staff member signs Form DG-4 at the same times. New staff also sign the policy acknowledgment in Appendix B before receiving access. DAA keeps a record of completed training and signed forms.

XVII. Penalties

A violation of this policy or of a CPE agreement may result in loss of access to CPE data, termination of the agreement, and the required return or destruction of all data. CPE staff may also face disciplinary action, up to and including dismissal. Contractors may face termination of their contract.

Kentucky law sets a fine of $25 to $100, up to 30 days in jail, or both for violations of KRS 164.283 (KRS 164.991). Under FERPA, if an outside party improperly rediscloses PII, CPE may bar that party from receiving PII for at least five years (34 C.F.R. 99.33(e)). Other state and federal penalties may also apply.

XVIII. Policy Review

DAA reviews this policy and its forms at least every two years. DAA also reviews them whenever relevant laws change. The CPE President or designee approves revisions.

Appendix A. Forms Used Under This Policy

Data Governance Forms

Form	Who completes it	When
DG-1 *External Data Request*	Any outside requester	At the start of every Tier 2 or Tier 3 request
DG-2 *Data Sharing Agreement*	The requesting organization and CPE	Before any Tier 3 release
DG-3 *External Data Custodian Confidentiality Agreement*	Each person at the recipient organization or vendor who will access Tier 3 data	With the agreement, and whenever a custodian is added
DG-4 *CPE Staff Data User Agreement*	CPE employees, interns, and contractors with access to CPE data systems	At onboarding and each year
DG-5 *Certificate of Data Destruction*	The recipient's requesters and authorized official	Within 30 days after the agreement ends

Appendix B. Policy Acknowledgment and Signatures

Every person who receives access to CPE confidential data signs this page before access is granted. This includes new CPE employees, interns, and contractors at onboarding. Human Resources signs for CPE staff. General Counsel signs for external users who are not CPE staff and receive Tier 3 data. A Data and Advanced Analytics authorized staff member signs for every user. DAA keeps the signed page on file.

> **Data user acknowledgment.** By signing below, I confirm that I have received and read the CPE Data Access and Security Policy. I understand my responsibilities under this policy, and I agree to follow it. I understand that a violation may result in loss of access, disciplinary action, and penalties under state and federal law.

> **CPE verification.** By signing below, each CPE signer confirms that each data user listed below has received this policy and needs access to CPE data for an approved purpose.

Signatures

Each data user signs on a separate row and lists a unit or organization with his or her title. Leave unused rows blank.

Signer	Printed name and title	Signature	Date
Data Users			
Data User			
Data User			
Data User			
Kentucky Council on Postsecondary Education			
Human Resources *CPE staff only*			
Data and Advanced Analytics Authorized Staff			
General Counsel *External, non-staff users with Tier 3 access only*			

Kentucky Council on Postsecondary Education
Data and Advanced Analytics | Data Governance
Rev. October 2026

FORM DG-1 | CPE DATA GOVERNANCE

External Data Request

Before You Begin

- Check published data first. Many questions can be answered with CPE's published reports and interactive dashboards at cpe.ky.gov. If those do not meet your needs, complete this form.
- Complete every part that applies. Parts 1 to 3 and Part 7 apply to every request. Parts 4 to 6 apply only to requests for student-level data (Tier 3). Submit the form online at https://cpe.ky.gov/data/request.html, or e-mail this completed copy to CPEDataRequest@ky.gov.
- Know what comes next. CPE reviews complete requests within 10 business days. Aggregate (Tier 2) requests do not need an agreement. Student-level (Tier 3) requests require a signed Data Sharing Agreement (Form DG-2) and a confidentiality agreement (Form DG-3) for each person who will handle the data.
- Do not include student data in this form. Describe the data you need. Do not attach records.

Part 1. Requester Information			
Name		**Title**	
Organization		**Department**	
Mailing address			
E-mail		**Phone**	
Organization type	☐ Kentucky public university ☐ KCTCS college ☐ Kentucky independent college or university ☐ State agency ☐ Federal agency	☐ Out-of-state college or university ☐ Research organization or nonprofit ☐ Legislator or legislative staff ☐ News media ☐ Other: _____	
Principal investigator (if different)		**PI e-mail**	
Student project?	☐ No ☐ Yes. This request supports a thesis, dissertation, or class project. My faculty advisor will sign Part 7.		
Faculty advisor (if student)		**Advisor e-mail**	

Part 2. About the Project		
Project title		
Describe the purpose of the project and the questions you want to answer.		
How will the results be used, and who will see them?		
Planned products	☐ Report or policy brief ☐ Journal article ☐ Presentation ☐ Thesis or dissertation	☐ Dashboard or website ☐ Internal use only ☐ Grant application or report ☐ Other: _____
Funding source or grant (if any)		
Date data needed		**Project end date**
IRB status	☐ Approved (attach approval) ☐ Pending	☐ Exempt (attach determination) ☐ Not applicable

Part 3. Data Requested	
Level of data	☐ **Aggregate tables** with small cells suppressed (Tier 2). No agreement is needed. ☐ **De-identified student-level records** (Tier 3, Purpose C). ☐ **Identified student-level records** (Tier 3, Purpose A or B).
Student population	
Academic years or terms	
Institutions or sectors	
Examples: "First-time, full-time undergraduates at Kentucky public universities, fall 2019 through fall 2024." Or: "Associate degree earners at KCTCS colleges, academic years 2020-21 through 2024-25."	

Data Elements Requested

Data element or table description	Why the project needs it

Linking to other data	☐ No. CPE data will not be linked to any other data. ☐ Yes. Describe the other data sources and how records will be matched below.
If linking, describe the other data sources and the matching method.	
Tier 3 only. Explain why aggregate or published data will not meet your needs.	

Part 4. Purpose and Legal Basis (Tier 3 only)

Check the one purpose that fits your project. A project with more than one purpose needs more than one agreement. Section X of the CPE Data Access and Security Policy explains each purpose.

Purpose A. Research Study	☐ The study is for, or on behalf of, CPE or Kentucky institutions. It will (check one): ☐ Develop, validate, or administer predictive tests ☐ Administer student aid programs ☐ Improve instruction
Purpose B. Audit or Evaluation	☐ The project evaluates a federal- or state-supported education program, or supports related compliance work. Name the program below.
Program evaluated (Purpose B)	
Purpose C. De-identified Data Use	☐ The project does not need to know who students are.

Explain how the project fits the purpose you checked.

Part 5. Data Security Plan (Tier 3 only)	
Where data will be stored	
Encryption	☐ Data will be encrypted at rest ☐ Data will be encrypted in transit
How will access be limited to the people listed in Part 6? Include logins, permissions, and multi-factor authentication.	
How and when will the data, including all copies and backups, be destroyed?	
Prior incidents	☐ Our organization has not had a breach involving education records in the past five years. ☐ Our organization has had such a breach. Explain in an attachment.

Part 6. Data Custodians (Tier 3 only)

Name	Title and project role	Organization	E-mail

Every person listed above must sign Form DG-3 before CPE releases any data. List only people who will access student-level data.

Part 7. Certification

By signing below, I certify the following.

- The information in this request is accurate and complete.
- I will use any data CPE provides only for the purpose described in this request and in any agreement CPE approves.
- I will follow the CPE Data Access and Security Policy, including its suppression standards, in every product that uses CPE data.
- I understand that CPE may deny, narrow, or delay this request, and that submitting it does not guarantee a release of data.

Signatures

Each requester signs, including any faculty advisor (student projects) and each principal investigator. Leave unused rows blank. CPE signatures confirm review and approval of this request.

Signer	Printed name and title	Signature	Date
Requesters			
Requester			
Requester			
Requester			
Requester			
Kentucky Council on Postsecondary Education			
Data and Advanced Analytics Authorized Staff			
General Counsel *Tier 3 requests only*			

For CPE Use Only			
Request number		**Date received**	
Date complete		**Assigned to**	
Tier assigned	☐ Tier 1. Referred to published data ☐ Tier 2. Aggregate release	☐ Tier 3. Agreement required	
Agreement type	☐ Purpose A. Research Study ☐ Purpose B. Audit or Evaluation ☐ Purpose C. De-identified Data Use	☐ Interagency agreement ☐ Vendor contract ☐ None needed	
Decision	☐ Approved ☐ Approved with changes	☐ Denied (reason sent in writing) ☐ Withdrawn	
Review date		**Agreement number**	
Release date			

FORM DG-2 | CPE DATA GOVERNANCE

Data Sharing Agreement

How to Use This Template

- One agreement, one purpose. Check one purpose in Section 2. Only the purpose-specific terms in Section 14 that match it apply.
- Fill in the blank fields. DAA completes this template with the recipient after approving Form DG-1.
- Attach everything listed in Section 16. CPE will not release data until all signatures and every custodian's Form DG-3 are on file.
- Do not edit the standard terms in Sections 5 through 15 without review by CPE's Office of General Counsel.

1. Parties and Agreement Summary

This Data Sharing Agreement ("Agreement") is between the Kentucky Council on Postsecondary Education ("CPE") and _____ ("Recipient"). CPE and Recipient are each a "Party."

Agreement Summary			
Agreement number		**DG-1 request number**	
Recipient			
Project title			
Lead requester		**Lead requester e-mail**	
CPE contact		**CPE contact e-mail**	
Start date		**End date (3 years or less)**	

2. Purpose and Legal Basis

Recipient may use the data released under this Agreement only for the one purpose checked below. A different purpose requires a new agreement.

Purpose A. Research Study	☐ Recipient will conduct a study for, or on behalf of, CPE or Kentucky postsecondary institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. Legal basis: FERPA studies exception, 34 C.F.R. 99.31(a)(6).
Purpose B. Audit or Evaluation	☐ CPE designates Recipient as its authorized representative to audit or evaluate the federal- or state-supported education program named in Section 3, or to support related compliance work. Legal basis: FERPA audit or evaluation exception, 34 C.F.R. 99.31(a)(3) and 99.35.
Purpose C. De-identified Data Use	☐ CPE will release only de-identified student-level data. Recipient does not need to know the identity of any student. Legal basis: 34 C.F.R. 99.31(b).

3. Project Description

Recipient's approved Form DG-1 is attached as Attachment 1 and describes the project in full. A brief summary of the project, including the questions it will answer and, for Purpose B, the program being evaluated, follows.

4. Data to Be Released

Attachment 2 lists the data elements, student population, institutions, and years CPE will release. CPE will release only the minimum data necessary for the purpose. CPE will not release Social Security numbers unless Attachment 2 lists them and DAA and General Counsel approve them in writing. CPE will deliver the data through a CPE-approved secure file transfer service.

5. Term

This Agreement takes effect on the date of the last signature. It ends on the end date in Section 1 or when the project is complete, whichever comes first. The term may not exceed three years. The Parties may extend the term only by a written amendment signed before the Agreement ends.

6. Authorized Data Custodians

Only the people listed in Attachment 3 may access the data. Each of them must sign Form DG-3 before receiving access. Recipient may add a custodian by giving DAA written notice and a signed Form DG-3. The new custodian may not access the data until DAA confirms receipt. Recipient must end a custodian's access right away when that person leaves the project. Recipient must notify DAA within five business days.

7. Use of the Data

Recipient agrees to the following limits on its use of the data.

a. Recipient will use the data only for the purpose in Section 2 and the project in Section 3.
b. Recipient will not disclose the data, or any file that contains student-level data derived from it, to anyone other than the custodians in Attachment 3.
c. Recipient will not attempt to identify any individual student, except as Purpose A or B requires to carry out the approved work.
d. Recipient will not contact any student or family based on the data.
e. Recipient will not link the data to any other data except as Attachment 1 describes.
f. Recipient will not use the data for any commercial purpose or to make decisions about individual students.

8. Data Security

Recipient will protect the data with security procedures suited to its sensitivity, as KRS 61.932 requires. At a minimum, Recipient will meet the following standards.

- Encrypt the data at rest and in transit.
- Store the data only on the systems described in Recipient's data security plan and only within the United States.
- Give each custodian a unique login. Use multi-factor authentication where the system supports it.
- Keep the data off personal devices, personal cloud accounts, and unencrypted removable media.
- Keep the data out of public generative AI tools and any online service not named in the security plan.
- Secure printed material and destroy it by cross-cut shredding when it is no longer needed.

9. Publication and Disclosure Review

Recipient will apply the CPE suppression standards to every table, chart, and report that uses the data. Recipient will send DAA a copy of each planned publication or presentation at least 30 days before release. DAA reviews these products only to confirm that they do not disclose personally identifiable information. CPE does not approve or edit Recipient's findings. Recipient will give CPE a copy of each final product.

Each product must include this statement: *"This work used data provided by the Kentucky Council on Postsecondary Education. The views expressed are those of the authors and do not necessarily reflect the views of CPE."*

10. Security Incidents

Recipient will notify DAA within 24 hours after discovering any actual or suspected loss, theft, or unauthorized access, use, or disclosure of the data. Recipient will send a written report within five business days. The report will describe what happened, the data involved, and the steps taken in response. Recipient will cooperate with any investigation. Recipient will pay the costs of notification and investigation that result from its own breach, consistent with KRS 61.931 to 61.934.

11. Monitoring

Recipient will confirm its compliance with this Agreement in writing each year on the anniversary of its start date. CPE may review Recipient's compliance, including its security practices, with reasonable notice.

12. Return or Destruction of Data

Within 30 days after this Agreement ends or the data are no longer needed, Recipient will destroy all data released under it. This includes all copies, extracts, backups, and derived files that contain student-level data. Electronic data must be destroyed using methods consistent with NIST Special Publication 800-88. Recipient will return a signed Form DG-5 to DAA. Recipient may keep aggregate results that meet the CPE suppression standards.

13. Termination

Either Party may end this Agreement with 30 days' written notice. CPE may end it at once if Recipient violates its terms. When the Agreement ends for any reason, Section 12 applies. If Recipient improperly rediscloses personally identifiable information, CPE may deny Recipient access to such information for at least five years (34 C.F.R. 99.33(e)).

14. Purpose-Specific Terms

Only the terms below that match the purpose checked in Section 2 apply.

Purpose A. Research Study

a. Recipient will conduct the study so that no one other than its representatives with legitimate interests in the information can personally identify any student or parent.
b. Recipient will destroy the data when it is no longer needed for the study, and no later than the deadline in Section 12.
c. Recipient will share the study's results with CPE.

Purpose B. Audit or Evaluation

a. By this Agreement, CPE designates Recipient in writing as its authorized representative for the audit or evaluation described in Section 3.
b. Recipient will use personally identifiable information only to carry out that audit or evaluation.
c. Recipient will protect the information from further disclosure and from any use not authorized by this Agreement.
d. Recipient will destroy the information when it is no longer needed for the audit or evaluation, and no later than the deadline in Section 12.

Purpose C. De-identified Data Use

a. Recipient will not attempt to re-identify any student, alone or by combining the data with other information.
b. Recipient will not attempt to learn how CPE created any record code attached to the data.
c. Recipient will notify DAA within 24 hours if it believes any student could be identified from the data.

15. General Terms

- Kentucky law governs this Agreement.
- This Agreement and its attachments are the entire agreement between the Parties about the data. Any change must be in writing and signed by both Parties.
- Recipient may not assign this Agreement or delegate its duties without CPE's written consent.
- Each Party is responsible for its own acts and those of its employees and agents.
- Nothing in this Agreement waives the sovereign immunity of CPE or the Commonwealth of Kentucky.
- Sections 7, 8, 10, 12, and 13 survive the end of this Agreement for as long as Recipient holds any of the data.

16. Attachments

- Attachment 1. Recipient's approved Form DG-1, External Data Request, including its data security plan.
- Attachment 2. Data to Be Released.
- Attachment 3. Authorized Data Custodians, with a signed Form DG-3 for each person.

17. Signatures

Signatures			
Each person signing for a Party has authority to bind that Party. Leave unused Requester rows blank.			
Signer	**Printed name and title**	**Signature**	**Date**
Recipient			
Recipient Authorized Official			
Requester			
Requester			
Requester			
Kentucky Council on Postsecondary Education			
Data and Advanced Analytics Authorized Staff			
General Counsel			

Attachment 2. Data to Be Released

Student population	
Institutions or sectors	
Academic years or terms	
Data level	☐ Identified student-level data (Purpose A or B) ☐ De-identified student-level data with a random record code (Purpose C) ☐ De-identified student-level data without a record code (Purpose C)

Data Elements

#	Data element	Source table or collection	Purpose served
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

Attachment 3. Authorized Data Custodians

List every person who will access the data. Each person must sign Form DG-3 before receiving access. Attach the signed forms to this Agreement.

Authorized Data Custodians

Name	Title and project role	E-mail	DG-3 on file (date)

FORM DG-3 | CPE DATA GOVERNANCE

External Data Custodian Confidentiality Agreement

About This Form

- Who signs. Every person at a recipient organization or vendor who will access CPE Tier 3 data. This includes students, research assistants, and contractors.
- When. With the Data Sharing Agreement (Form DG-2) or vendor contract, and before the person receives any access. Send a new form whenever a custodian is added.
- Where to send it. Return the signed form to CPEDataRequest@ky.gov. Keep a copy for your records.

Agreement Information			
Organization		**Agreement number**	
Project title			

My Commitments

I understand that my work on this project gives me access to confidential information about students. By signing this form, I agree to the following.

1. I have read the CPE Data Access and Security Policy and the agreement or contract under which I will access CPE data. I will follow both.
2. I will use CPE data only for the purpose stated in that agreement.
3. I will not share CPE data, or any file derived from it that contains student-level data, with anyone who is not an authorized custodian under the agreement.
4. I will not try to identify any student except as the agreement requires. I will not contact any student or family based on CPE data.
5. I will not look up records of people I know or use the data for any personal reason.
6. I will not link CPE data to other data except as the agreement allows.
7. I will store and transfer the data only in the secure ways the agreement requires. I will not place CPE data on personal devices, personal cloud accounts, public AI tools, or other unapproved online services.
8. I will keep my login credentials private. I am responsible for all activity under my credentials.

9. I will apply CPE suppression standards to any table, chart, or report before it is shared outside the project team.
10. I will report any known or suspected loss, theft, or improper disclosure of CPE data to my supervisor and to CPE Data and Advanced Analytics within 24 hours of discovery.
11. I will destroy or return CPE data when my work on the project ends or when the agreement ends, whichever comes first.
12. My duties under this form continue after my work on the project ends.

Information the Law Protects

FERPA protects personally identifiable information from student education records. This includes a student's name, student ID number, date of birth, and any other information that, alone or in combination, would allow a reasonable person to identify the student. KRS 61.931 also protects personal information such as a name combined with a Social Security number, a driver's license number, or a financial account number. Other state and federal privacy laws may also apply. I understand that traits that could make a person identifiable, such as membership in a small group, are protected as well.

Consequences of a Violation

A violation may result in loss of my access to CPE data, termination of the agreement for my entire organization, and discipline by my employer. Under FERPA, CPE may bar an organization that improperly rediscloses student information from receiving such information for at least five years (34 C.F.R. 99.33(e)). Penalties under state and federal law, including KRS 164.991, may also apply.

Signatures

Each data custodian signs on a separate row. Leave unused rows blank. Use another copy of this form for more custodians.

Signer	Printed name and title	Signature	Date
Recipient Organization			
Data Custodian			
Data Custodian			
Data Custodian			
Supervisor or Authorized Official			
Kentucky Council on Postsecondary Education			
Data and Advanced Analytics Authorized Staff			
General Counsel *Tier 3 data sharing agreements only*			

FORM DG-4 | CPE DATA GOVERNANCE

CPE Staff Data User Agreement

About This Form

- Who signs. Every CPE employee, intern, and contractor who needs access to confidential data or to CPE data systems.
- When. At onboarding, before access is granted, and again each year with annual data privacy and security training.
- Routing. The staff member signs, the supervisor confirms the access is needed, Human Resources confirms employment, and DAA grants access and files the form.

Staff Information			
Name		**Title**	
Unit		**Supervisor**	
Role	☐ Employee ☐ Intern	☐ Contractor or temporary staff	
Agreement type	☐ Initial (onboarding) ☐ Annual renewal	☐ Change in access	
Access requested	☐ KPEDS data warehouse ☐ Restricted network folders with student-level data ☐ Restricted dashboards or reporting tools ☐ Partner agency data (name): _____ ☐ Other: _____		

My Commitments

I understand that CPE holds confidential information about students and other individuals. I share responsibility for protecting it. By signing this form, I agree to the following.

1. I have read the CPE Data Access and Security Policy and will follow it.
2. I will access CPE data only as needed for my assigned duties.

3. I will not use CPE data for personal purposes that are not educational. I will use CPE data for educational purposes, such as coursework or dissertation research, only after CPE approves that use through Form DG-1.
4. I will not look up records about myself, my family, my friends, or anyone else I know for personal reasons.
5. My user ID and password are issued to me alone. I will not share them. I am responsible for all activity under my credentials. CPE may revoke my access at any time.
6. I will not send student-level data by ordinary e-mail. I will use CPE-approved secure transfer methods.
7. I will not store confidential data on personal devices, personal cloud accounts, or unencrypted removable media.
8. I will not enter confidential data into public generative AI tools or any online service that CPE has not approved for confidential data.
9. I will apply CPE suppression standards to anything I prepare for release outside CPE. I will have it checked by a second staff member when the policy requires.
10. I will release data outside CPE only through the process in the CPE Data Access and Security Policy.
11. I will report any known or suspected incident right away to my supervisor and DAA at CPEDataRequest@ky.gov.
12. When I change roles or leave CPE, I will return or delete any CPE data in my possession. I understand that my access will end.
13. I will complete data privacy and security training at onboarding and each year after that.

Consequences of a Violation

A violation of this agreement or the policy may result in loss of access and disciplinary action, up to and including dismissal. Contractors may also face termination of their contract. Kentucky law sets a fine of $25 to $100, up to 30 days in jail, or both for violations of KRS 164.283 (KRS 164.991). Other state and federal penalties may also apply.

Signatures			
Signer	**Printed name and title**	**Signature**	**Date**
Staff Member			
Supervisor *Confirms access is needed for assigned duties*			
Human Resources			
Data and Advanced Analytics Authorized Staff			

For DAA Use Only			
Access granted on		**Training completed on**	
Next renewal due			

FORM DG-5 | CPE DATA GOVERNANCE

Certificate of Data Destruction

About This Form

- When. Within 30 days after the agreement ends or the data are no longer needed, whichever comes first.
- Scope. Covers every copy held by every custodian, including extracts, backups, and derived files that contain student-level data.
- Where to send it. Return the signed form to CPEDataRequest@ky.gov. DAA will close the agreement and update the Record of Disclosures.

Agreement Information			
Agreement number		**Organization**	
Project title			
Lead requester		**Lead requester e-mail**	
Agreement end date		**Date of destruction**	

Data Files Destroyed

File name or description	Date received from CPE	Locations and copies destroyed

Destruction Method	
Method used (check all that apply)	☐ Secure deletion or overwriting consistent with NIST Special Publication 800-88 ☐ Physical destruction of storage media ☐ Cross-cut shredding of printed records ☐ Return of all copies to CPE ☐ Other: _____

Certification

We certify the following on behalf of the organization named above.

1. All data CPE released under the agreement have been destroyed. This includes every copy, extract, and backup held by every custodian named in the agreement.
2. All derived files that contain student-level data have been destroyed.
3. We have kept only aggregate results that meet the CPE suppression standards.
4. We have not disclosed the data to anyone outside the agreement, except as described in an attachment to this form.

Signatures			
Each requester who received CPE data signs. Leave unused rows blank.			
Signer	**Printed name and title**	**Signature**	**Date**
Recipient Organization			
Requester			
Requester			
Requester			
Authorized Official			
Kentucky Council on Postsecondary Education			
Data and Advanced Analytics Authorized Staff			
General Counsel *Tier 3 data sharing agreements only*			