Kentucky Council on Postsecondary Education

# Data Access Policy

Unit/Department: Data & Information


CPE Contact

Lee Nimocks, Vice President

Email: lee.nimocks@ky.gov

## Table of Contents

## I. POLICY STATEMENT

The Kentucky Council on Postsecondary Education (CPE) collects and maintains data containing confidential personal information, including student education records, in accordance with federal and state laws and regulations. Data is utilized for federal and state reporting, funding calculations, and research. CPE does not permit access to, or the disclosure of, confidential personal information, student education records, or personally identifiable information contained therein except for purposes authorized under the Family Educational Rights and Privacy Act (FERPA) or other applicable law.

CPE also may maintain or gain access to other confidential data to which this policy will apply along with any contractual or legal requirements mandated as a result of having such access.

## II. PURPOSE

This policy establishes the procedures and protocols for collecting, maintaining, protecting, disclosing, and disposing of confidential data records, including data collections containing personally identifiable information about students and personnel. It is intended to be consistent with the disclosure provisions of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and KRS 164.283.

## III. SCOPE OF POLICY

These policies and procedures apply to all employees and contractors of CPE and are applicable to other entities requesting access to confidential, sensitive, or restricted information.

Related policies, laws, operating procedures, and other documents that contain directives applying to agency, confidential, sensitive, and restricted enterprise information include:

- Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99 located at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
- KRS 164.283.
- Memorandum of Understanding(s) between CPE and outside agencies or entities.

## IV. DEFINITIONS

**A.** Authorized Representative refers to any entity or individual designated by a state or local educational authority to conduct any audit or evaluation, or any compliance or enforcement activity, in connection with federal legal requirements that relate to these programs (FERPA 34 C.F.R. § 99.3).

**B.** Confidentiality refers to how personally identifiable information collected is protected and when an individual's consent is required to disclose.

**C.** Data Collection includes any collection of educational records, which may include data collected in an enterprise-level system (e.g., Student Information System) or through alternate collection means.

**D.** De-identification is a process that renders data safe to utilize and share by removing or obscuring all identifying fields such as name or identification numbers, thus making it very difficult to identify an individual based on a combination of variables. CPE will employ a set of data de-identification rules.

**E.** Disclosure or Disclose means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means (internally or externally).

**F.** Education Record describes any information or data recorded in any medium—including but not limited to handwriting, print, or system—which contains information directly related to a student, school, or district (including personnel records) and which are maintained by an educational agency or institution or a person acting for such agency or institution. See 20 U.S.C. 1232g(a)(4)(A); 34 C.F.R. 99.3.

**G.** Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law designed to protect the privacy of student education records and to allow students, their parents, and/or legal guardians access to the student's educational record.

**H.** Kentucky Adult Education Reporting System (KAERS) is the authoritative reporting system and database at CPE for student-level information collected from adult education providers located in each county of the state and approved by Kentucky Adult Education (KYAE).

**I.** Kentucky Longitudinal Data System is a shared data system created pursuant to KRS 151B.132 and managed by the Kentucky Center for Education and Workforce Statistics (KCEWS) with data provided by the Kentucky Department of Education (KDE), the Council on Postsecondary Education (CPE), the Education Professional Standards Board (EPSB), the Kentucky Higher Education Assistance Authority (KHEAA), and the Kentucky Education and Workforce Development Cabinet. This system links data from early childhood, K-12, postsecondary, the workforce and other sources to allow stakeholders to develop a broader understanding of the implications programs and policies have on our state.

**J.** Kentucky Postsecondary Education Data System (KPEDS) is the authoritative reporting system and database at CPE for student-level information collected from Kentucky colleges and universities.

**K.** Linkage consists of the ability to combine educational records through use of common identifiers for the purpose of research or re-identification.

**L.** Memorandum of Understanding (MOU) refers to the data disclosure and confidentiality agreement between CPE and the entity requesting data.

**M.** Personally Identifiable Information (PII) includes the name and address of the student and the student's family; a personal identifier, such as the student's Social Security Number, student number, or biometric record; other indirect information, such as the student's date and place of birth and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of relevant circumstances, to identify a student with reasonable certainty; and information based on a targeted request.

**N.** Privacy defines the right of individuals to have their personal information adequately protected to avoid the potential for harm, embarrassment, inconvenience, and/or unfairness.

**O.** Re-disclosure describes the sharing or use of data collection beyond the original, approved, intent.

**P.** Security means technical procedures that are implemented to ensure that records are not lost, stolen, vandalized, illegally accessed, or improperly disclosed.

**Q.** Student Identification (SID) Number is a unique number assigned by the Student Information System to track student and education records. It does not contain any series of numbers matching a Social Security number.

**R.** Student refers any person who is or has attended a public or accredited non-public school and for whom an educational agency or institution maintains education records. See 34 C.F.R. 99.3.

**S.** Suppression denotes withholding information from publication. Some information is withheld from publication to protect small counts that could lead to a disclosure. Other information is withheld from publication in a table to prevent the calculation of the data based on small counts from the published information; this is known as complementary suppression.

**T.** Vendor-Partner includes any CPE contract holders with access to education records.

## V. INFORMATION COLLECTED AND MAINTAINED

CPE collects, through enterprise data systems and other collection methods, records from postsecondary institutions and other education entities, including but not limited to:

A. Personally Identifiable Information that identify each student. These data may include name, identification number, address, race/ethnicity, gender, date of birth, place of birth, social security number, and eligibility status for federal and state student aid programs (i.e., Pell Grant, KEES, etc.);

B. Participatory data including attendance, student progress, degree completion, school attended, academic work completed, grade point average, entrance assessments, and date of graduation.

C. Employment data from postsecondary institutions.

D. Financial data from postsecondary institutions in the way of budgets and expenditures (annual submission).

Records may be maintained in one or more data systems. All systems and collections shall be subject to this policy. A detailed description of the data collected can be found in CPE's Data Reporting Guidelines and the KAERS Data Manual for Kentucky.

## VI. MEASURES TO MAINTAIN SECURITY OF CONFIDENTIAL DATA

CPE shall utilize various procedures and measures to ensure the security of confidential records. These procedures include assignment of a unique identifier to each student or employee, a system of restricted access to data, and statistical cut-off procedures.

A. A unique Student Identification number (SID) is assigned to each Kentucky student. The student ID is computer-generated and contains no embedded meaning. The student locator tool in both the KPEDS and KAERS systems assigns a unique SID.

B. Security protocols limit who has access to the data and for what purposes.

C. Statistical cut-off procedures (suppression rules) are utilized to prevent student identification in aggregate-level reports.

D. All CPE employees, contractors, and vendor-partners must abide by FERPA requirements and this Data Access and Security Policy.

E. CPE shall maintain a current listing of agency personnel who have access to personally identifiable student information through authentication and internal links.

F. Confidential or identifiable student-level data shall be communicated or transferred electronically to external entities through a secure site. Student-level data should be password protected prior to any exchange through e-mail or alternative transfer method. The password should not be included in the e-mail with the student-level data; it must be provided through a separate communication.

G. De-identification rules as established within this policy must be followed to ensure confidentiality of data shared for research purposes.

H. All CPE employees and contractors must receive and acknowledge CPE's adopted Internet and Electronic Mail Acceptable Use Policy (CI0-060).

I. Other safeguards -- All agency employees, agents of CPE, researchers, and other entities with direct access to confidential student information are responsible for protecting the data via the following procedures:
    - Prevent disclosure of data by protecting visibility of reports and computer monitors when displaying and working with confidential information.
    - Workstations must be locked or shut down when left unattended for any amount of time.
    - Data must be stored in a secure location. Electronic files should be password protected and/or stored in a location only accessible by the authorized entity. Confidential information will not be faxed.
    - When no longer needed, paper reports must be shredded and electronic files must be destroyed.
    - Reports, CDs, and/or any other media containing confidential information must be stamped or otherwise marked as confidential prior to being released outside the agency. The envelope containing the information also must indicate that the contents are confidential.

## VII. SECURITY INCIDENT NOTIFICATION

Users suspecting an unauthorized disclosure of personally identifiable or confidential information shall immediately notify CPE Technical Support at cpetech.support@ky.gov and cooperate with CPE Technical Support staff as part of any necessary investigation. CPE shall comply with the security breach and investigation procedures outlined in KRS 61.931 to 61.934 and CIO-090.

## VIII. DE-IDENTIFICATION OF DATA

De-identification involves the removal of personally identifying information in order to protect personal privacy. With the exception of disclosure of education records for audits and evaluations and studies as defined by FERPA, data is provided in a de-identified or aggregate form. Social Security numbers, names, date of birth, or other identifiable data are excluded. The State Student Identification (SSID) Number can be provided to allow for matching of data records or re-identification but must be excluded from any publically produced reports.

## XI. SUPPRESSION RULES

According to FERPA, confidential personally identifiable information includes "information that, alone or in combination, is linked to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances to identify the student with reasonable certainty." Consequently, it is CPE's policy that public reports containing aggregate student data must suppress results for small groups of students when associated with characteristics that would make it possible to identify a student. This policy applies to public reports whenever an identified group contains fewer than 10 students. Suppression of data in the form of percentages shall occur when the percentages are 0 or 100 for any student demographic categories. Exceptions may be made on a case-by-case basis when reporting of groups fewer than 10 will not result in the disclosure of personally identifiable information.

When an identified group is smaller than these thresholds, the report must display a placeholder (for example, -, *, NA) with a disclaimer explaining what the placeholder means. Internal and external report authors also should be aware of small group suppression rules. Report authors are responsible for ensuring that CPE's suppression policy is applied appropriately to any reports created.

## X. DATA ACCESS

This section describes the conditions under which CPE will release confidential information. Confidentiality refers to a person's obligation not to disclose or transmit information to unauthorized parties. The requesting entity or individual must sign and have an approved CPE Memorandum of Understanding (MOU) as appropriate before any data will be released. Authorization must be evaluated annually to ensure access to the data is still required. Use of data is only for purposes as defined in the signed MOU.

The entities to which information may be released and the conditions of the release are listed for each entity below:

1) **CPE Staff** –All CPE staff must sign Non-Disclosure agreements at the time of employment. CPE staff members who have a need to access confidential information are permitted access through system access protocols established and maintained by CPE system administrators. Supervisors must indicate that the staff person needs access to this information in the performance of his or her assigned duties and responsibilities. Supervisors will ensure that the appropriate safeguards are instituted to protect the confidentiality of student information and that the staff person has received appropriate training. CPE staff may not access agency information for personal purposes (for example, research for a dissertation). Employees must maintain the confidentiality of all education records. Data will be destroyed in accordance with the state's record retention policy.

2) **KYAE Provider Staff** – Staff members of approved adult education providers may request access to data in KAERS by signing and agreeing to the KAERS

Employee Confidentiality/Security Contract. Staff members who have a need to access confidential information are permitted access through system access protocols established and maintained by CPE system administrators. Supervisors must indicate that the staff person needs access to this information in the performance of his or her assigned duties and responsibilities. Supervisors will ensure that the appropriate safeguards are instituted to protect the confidentiality of student information and that the staff person has received appropriate training. Staff may not access agency information for personal purposes (for example, research for a dissertation). Staff must maintain the confidentiality of all education records. Data will be destroyed in accordance with the state's record retention policy.

3) **Public** - CPE may disclose, without student consent, student information in aggregate form that is not easily traceable to a student. Public access is limited to aggregate level reports. Suppression rules set forth in this policy are adhered to for all public reporting. Certain non-confidential Tier 1 and Tier 2 data are available to anyone through the CPE Data Portal website at http://cpe.ky.gov/info/.

4) **Parents and Students** shall be directed to the respective institution in order to obtain related records.

5) **Research** - CPE may disclose confidential, personally identifiable information of students to individuals and/or organizations for research and analysis purposes to improve instruction; develop, validate, or administer predictive tests; or improve instruction. Such disclosures also may be made to authorized representatives conducting audits or evaluations of education programs. Disclosures are authorized under the FERPA Studies or Audit/Evaluation Exceptions. Any such disclosure shall be made only if (1) the conditions in FERPA regulation 34 CFR 99.31(a)(6) or 99.35 are met; (2) the request for data sharing is approved by CPE with a signed Memorandum of Understanding (MOU) to ensure compliance with FERPA regulations and CPE policies; (3) requester agrees to return or destroy education records upon completion of research use; (4) researcher understands associated penalties for violation of data privacy, use, or re-disclosure.

6) **Kentucky Longitudinal Data System** - personally identifiable data is provided to the Kentucky Longitudinal Data System per agreement between agencies and in accordance with KRS 151B.132.

## XI. TRAINING NEEDS

All CPE staff shall be made aware of the Data Access and Security Policy and will receive subsequent information through newsletter articles, e-mail messages, and/or training classes.

## XII. RESPONSIBILITY FOR DATA REQUESTS

The CPE Director of Data and Information is primarily responsible for processing all data requests. Requests for Tier 1 and Tier 2 data will be filled if the information requested has already been published or collected and can easily be put into a distribution format that protects confidential information.

Request for Tier 3 data will be considered if the request is consistent with the statutory duties, responsibilities and mission of CPE.

## XIII. RECORD OF ACCESS

In compliance with FERPA guidelines, CPE shall maintain a record indicating the name of any individual or organization external to CPE that requests and is allowed access to educational records. The record of access shall indicate the interest such person or organization had in obtaining the information, as well as the date the requested data were disclosed. See 20 U.S.C. 1232g (b) (4); 20 U.S.C. 1232g (j) (4).

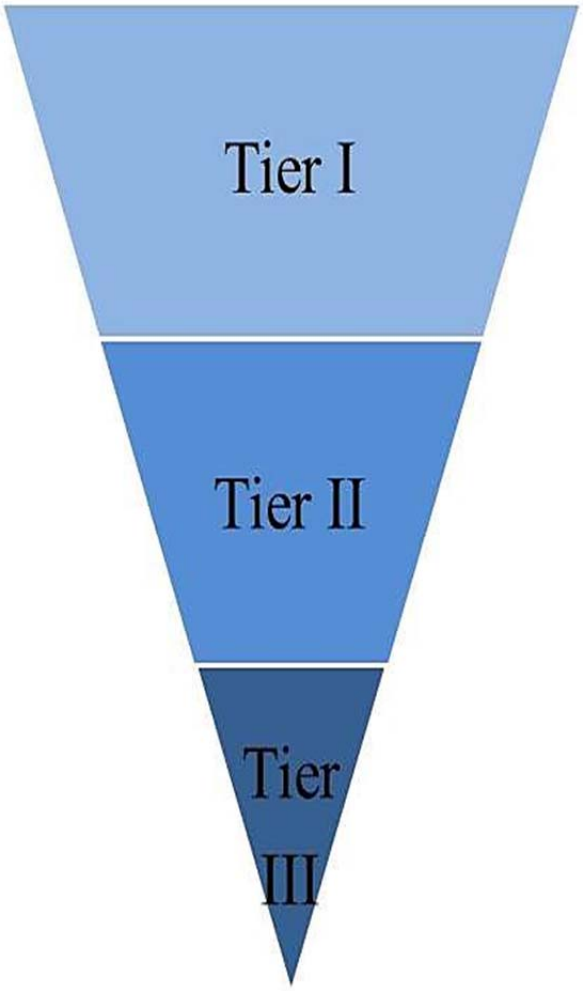
## XIV. DESTRUCTION OF DATA

Any entity receiving personally identifiable information must destroy such information when it is no longer needed for the purpose specified in the request for disclosure. The manner of destruction shall protect the confidentiality of the information and must be done at the conclusion of the intended purpose.

## XV. PENALTIES FOR VIOLATION OF DATA USE

Enforcement penalties for violation of data privacy security, unauthorized disclosure, or re-disclosure may include loss or denial of access to confidential information, revocation of network access privileges, and any other penalties as prescribed by federal or state law, including a fine not less than $25, nor more than $100, and/or imprisonment for up to 30 days for convictions of deliberate disclosures of confidential student academic records per KRS 164.991.

# Data Tiers Defined




**Non-Confidential Data:**

Data publically available. Counts are reportable down to one according to CPE policy.

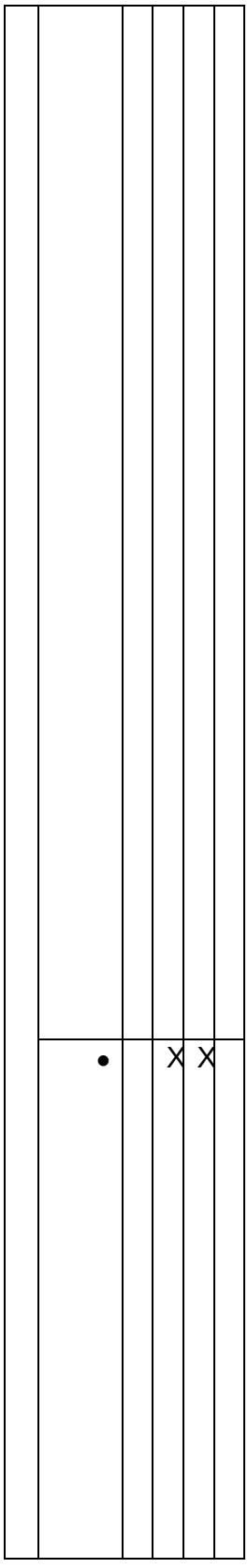
**Suppressed Data:**

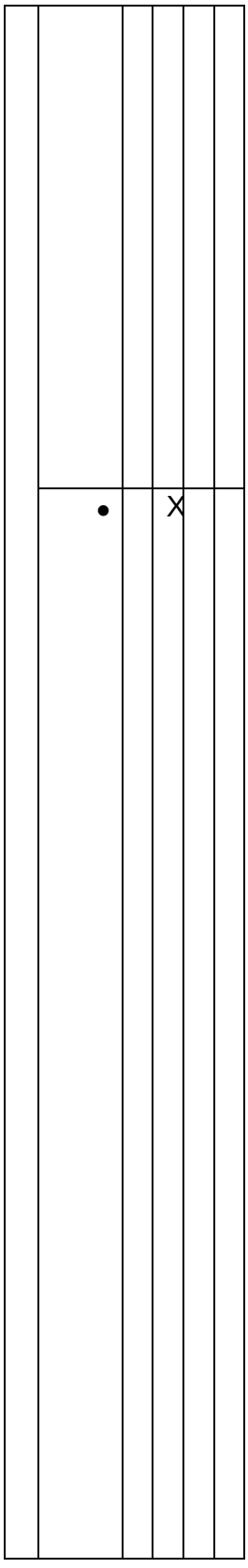
Data publically available. Counts less than 10 are suppressed according to CPE Data Access Policy

**Unsuppressed Data:**

Data only available with an approved data request proposal or MOU/nondisclosure agreement. Counts less than 10 are included. Must be use for the purpose of Audit, Evaluation and Studies.

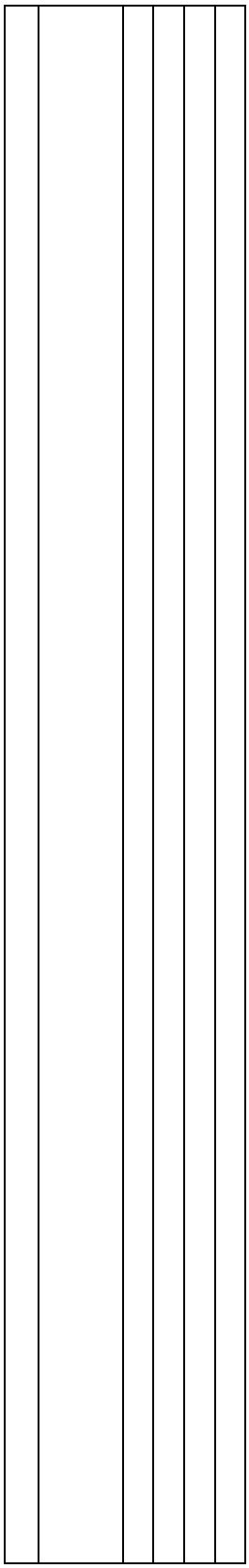
| DATA TIERS FOR EXTERNAL RELEASE OF DATA<br>CPE Student Records Confidentiality<br>Examples of Data Request<br>** These are examples and not meant to be all-inclusive. | Suppressed | Unsuppressed | Aggregate | Approved Research Proposal |
|---|---|---|---|---|
| Tier I | Aggregate-level counts by institution or region without identifiable attributes such as gender, race or other characteristics, such as: | | X | X |
| | • | | X | X |


•
X X



| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| **Tier II** | Tier I Data with additional break-out by gender, ethnicity, | X | | X | |

| | | | | | |
|---|---|---|---|---|---|
| | or other attribute that could lead to identification: | | | | |
| | • | X | | X | |
| | • | X | | X | |

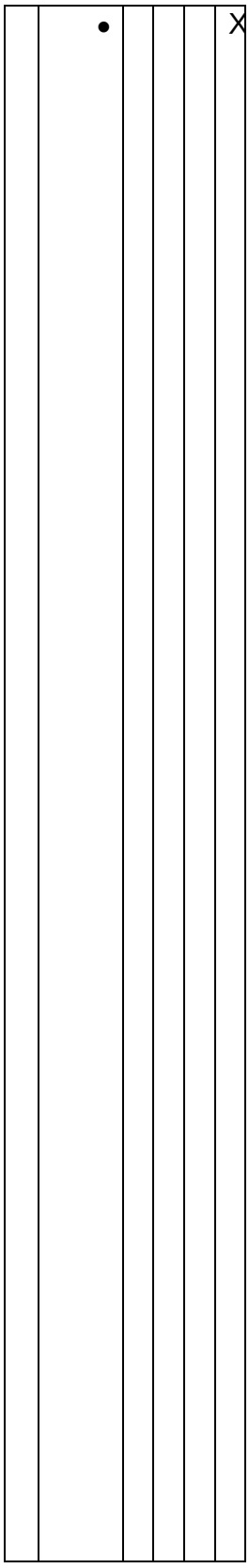


| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | • | X | | X | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | • | X | | X | |

| | | | | | |
|---|---|---|---|---|---|
| **Tier III** | Tier I or II Student-Level detail with personally identifiably characteristics for purposes of research or program accountability that is not de-identified or | | | | X |

| | | | | | |
|---|---|---|---|---|---|
| | suppressed | | | | |
| | • | | | | X |


X