OKLAHOMA STATE REGENTS FOR HIGHER EDUCATION
Improving our future by degrees

OK FDP
Oklahoma FAFSA Data Portal

PRIVACY CERTIFICATION

1. Confidential Information, Dissemination of Information, Ownership, Survival:

A. Confidential Information: In performance of this Agreement, both parties shall have access to or receive certain information that is not generally known to others ("Confidential Information"). Each party shall not use or disclose any Confidential Information or any finished or unfinished, documents, screens, reports, writings, procedural manuals, forms, source code, object code, work flow charts, methods, processes, data, data studies, drawings, maps, files, records, computer printouts, designs, equipment descriptions, or other materials prepared or generated as a result of this Agreement ("Work Product") without the prior written consent of the other party. Both parties shall use at least the same standard of care in the protection of the Confidential Information of the other party as each party uses to protect its own Confidential Information, but in any event such Confidential Information shall be protected in at least a commercially reasonable manner.

B. Highly Confidential Information: "Highly Confidential Information" means employee, volunteer, student, or teacher data including, but not limited to student identification number, social security number, phone number, email address, gender, ethnicity, race, foster care status, disabilities, school, grade, grade point average, standardized test scores, assessment data, after school activities, highest grade completed, discipline history, criminal history, free or reduced lunch qualifications, housing status, income, household income or payroll information. In performance of this Agreement, both parties shall have access to or receive Highly Confidential Information. Each party shall not use or disclose any Highly Confidential Information without the prior written consent of the other party.

C. Transmitting and Storing Highly Confidential Information: Both parties shall:

i. When mailing physical copies of Highly Confidential Information, send the Highly Confidential Information in a tamper-proof, labeled container, with a tracking number and a delivery confirmation receipt;

ii. Only mail Highly Confidential Information on electronic media, such as CDs, DVDs, electronic tape, etc., if the Highly Confidential Information is encrypted. Encryption must utilize the Advanced Encryption Standard ("AES") algorithm with a key of 256 bits or greater ("Encrypt"). The Highly Confidential Information shall only be mailed in accordance with the provisions of Section i, above;

iii. Encrypt all Highly Confidential Information prior to transmitting it electronically. OSRHE shall not transmit any unencrypted Highly Confidential Information via email, blackberry, blackjack, instant messages or any other unencrypted protocols;

iv. Not send any password or other information sufficient to allow decryption of Highly Confidential Information with the Encrypted Highly Confidential Information;

v. Keep all physical copies (paper or other physical representations) of Highly Confidential Information under lock and key, or otherwise have sufficient physical access control measures to prevent unauthorized access. Neither party shall leave Highly Confidential Information unsecured and unattended at any time;

vi. Encrypt any Highly Confidential Information stored on electronic media, such as CDs, DVDs, tape, flash drives, etc. Further, such electronic media shall be kept locked, or otherwise have sufficient physical access control measures to prevent unauthorized access. Neither party shall leave Highly Confidential Information in any electronic format, including computer databases, unsecured, meaning accessible without a password, and unattended at any time;

vii. Both parties shall take precautions to ensure that access through modems, networks, and the Internet is carefully monitored and limited to authorized users; and

viii. Only authorized users within either organization who have signed a notarized Affidavit of Nondisclosure shall have access to Highly Confidential Information, unless disclosure of Highly Confidential Information to a third party is authorized by the prior written consent of both parties pursuant to Section D below.

D. Dissemination of Information: Neither party shall disseminate any Confidential Information or Highly Confidential Information to a third party without the prior written consent of the other party. If either party is presented with a request for documents by any administrative agency or with a subpoena duces tecum regarding any Confidential Information, Highly Confidential Information or Work Product which may be in that party's possession, that party shall immediately give notice to the other party and its General Counsel with the understanding that the other party shall have the opportunity to contest such process by any means available to it prior to submission of any documents to a court or other third party. Neither party shall be obligated to withhold delivery of documents beyond the time ordered by a court of law or administrative agency, unless the request for production or subpoena is quashed or withdrawn, or the time to produce is otherwise extended. Each party shall cause its personnel, staff and

subcontractors, if any, to undertake the same obligations regarding confidentiality and dissemination of information as agreed to by both parties under this Agreement. Neither party shall make any disclosure or publication whereby a sample unit or survey respondent (including students and schools) could be identified or the data furnished by or related to any particular person or school under these sections could be identified.

E. Ownership: All original research results, data, information, records and work product generated under this Agreement, including all tangible or intangible property (collectively "Work Product") shall be jointly owned by Entity and OSRHE. Each party agrees that all Confidential Information, Highly Confidential Information and preexisting intellectual property shall at all times be and remain the property of the party that supplied it. Each party shall execute all documents and perform all acts that the other party may request in order to assist the other party in perfecting or protecting its rights in and to the Work Product and all intellectual property rights relating to the Work Product.

F. Use of Confidential Information, Highly Confidential Information, and Work Product: Each party warrants and represents that it shall not use the Confidential Information, Highly Confidential Information or Work Product, unless in the aggregate, for any purpose not specifically identified in this agreement, including, but not limited to any research project whether internal or external to that party. Any use of the Confidential Information, Highly Confidential Information, or any Work Product not specifically contemplated in this Agreement shall be considered a material breach of this Agreement.

G. Third Party Confidential Information and Proprietary Information: Each party agrees not to utilize, analyze, reverse engineer, or otherwise exploit any third party Confidential Information or proprietary information in performing the Services regardless of where that party obtained the third party Confidential Information or proprietary information (even if the third party Confidential Information or proprietary information was provided by the other party) unless that party has previously secured the appropriate authorization in writing from such third party. In accordance with the provisions of Section 12 of this Agreement, each party hereby agrees to indemnify and hold harmless the other party against any and all claims related to third party Confidential Information and proprietary information in connection with or arising out of the acts or omissions of the indemnifying party or its Staff under this Agreement.

H. Return or Destruction of Confidential Information and Highly Confidential Information: Each party shall, at the other party's option, destroy or return all Confidential Information and Highly Confidential Information to the other party upon demand within three (3) business days of demand. In addition, that party shall, at the other party's option, destroy or return all Confidential Information and Highly Confidential Information that belong to the other party within three (3) days of the expiration or termination of this Agreement. In the event the party to which the aforesaid information belongs elects to have the other party destroy the Confidential Information and Highly Confidential Information, that party shall provide an affidavit attesting to such destruction.

I. Staff and Subcontractors: Each party agrees to cause its personnel, staff and subcontractors, if any, to undertake the same obligations of confidentiality and ownership agreed to herein by that party.

J. Oklahoma Open Records Act: The parties acknowledge that this Agreement and all documents submitted to the Educational Entity related to this contract award are a matter of public record and are subject to the Oklahoma Open Records Act (Title 51 O.S. §§24A.1 – 24A.30 as amended) and any other comparable state and federal laws.

K. Information Security Procedures: It is critical that Highly Confidential Information be kept secure and protected from unauthorized disclosure. Therefore, all the Highly Confidential Information shared pursuant to this Agreement must be stored securely so that only authorized users within the organization have access to it. This means that computer data bases should be password protected; that precautions are taken to ensure that access through modems, networks, and the Internet is carefully monitored and limited to authorized users; and that data tapes, disks, paper files and other storage media are kept in secure locations.

L. Security Incidents: Each party shall report to the other all known or suspected Security Incidents. "Security Incident" means any unauthorized action by a known or unknown person which, if successfully completed, should reasonably be considered one of the following: a cyber-attack, denial of service (DoS/DDoS), disclosure of confidential customer or other sensitive information, misuse of system access, unauthorized access or intrusion (hacking), malware infection, unsolicited network reconnaissance, or any other activity that directly affects either of the party's Confidentiality, Integrity, and Availability of systems and/or data. "Security Incident" shall also include any contact by a law enforcement agency regarding any data. For purposes hereof, "the Parties" shall include any of their employees, agents, contractors or third parties including, without limitation, any vendors used by them that have access (either authorized or unauthorized) to the data.

M. Survival: The provisions of this Section shall survive the termination or expiration of this Agreement and only be ended with the complete and secure disposal of all confidential and / or highly confidential information and with the agreement of both parties

With my signature, I certify that I have read and understand that the data received by my eligible entity is confidential and shared data shall not be used for any purpose other than those described in the **FAFSA Data Portal Completion Agreement**, Part 6, A-M.

Signature	Name
Date	School/District/Entity Name