**DATA USE & SECURITY AGREEMENT**

**BETWEEN**

**DISTRICT NAME**
(hereinafter called ***{“Data Receiver”}*)
AND**

**THE RHODE ISLAND OFFICE OF THE POSTSECONDARY COMMISSIONER (OPC)**

(hereinafter called the ***{“Data Provider”}*) (**collectively the “Parties”).

**RECITALS**

**WHEREAS**, The U.S. Department of Education, under the FAFSA Completion Initiative, has authorized state grant agencies to provide limited FAFSA information to an LEA, secondary schools, and to certain “Designated Entities” regarding student progress in completing the Free Application for Federal Student Aid, hereby referred to as the “FAFSA”;

**WHEREAS**, on March 14, 2014 the U.S. Department of Education released a revised “Student Aid Internet Gateway Participation Agreement for State Grant Agencies” (hereinafter called the SAIG Participation Agreement) which includes a provision allowing a state grant agency to disclose defined “FAFSA Filing Status Information” to local educational agencies (LEAs), to secondary schools, and to certain other Designated Entities that have been determined by the Secretary to be eligible to receive this information;

**WHEREAS**, to receive FAFSA Filing Status Information for a student, the Designated Entity must have an “established relationship” with the student which exists when the student is enrolled in, has registered with, or is receiving services from the designated entity to assist the student in the pursuit of postsecondary education;

**WHEREAS**, FAFSA Filing Status Information provided to an LEA, secondary school, or Designated Entity may only be provided to Authorized Personnel of the LEA, secondary school, or Designated Entity and only for the authorized purpose (as provided in Section B (Purpose of the Agreement) of the SAIG Participation Agreement) of providing assistance to the student in completing the FAFSA. (The definition of Authorized Personnel as provided in Section C (Definitions) of the SAIG Participation Agreement is incorporated herein by reference);

**WHEREAS**, Designated Entities may receive FAFSA Filing Status Information from a state grant agency only if: (1) the state grant agency has submitted to the Department the completed SAIG Participation Agreement (Part Two of the SAIG Application); (2) the state grant agency has executed a written agreement with the designated entity as provided in Section G of the SAIG Participation Agreement; and (3) the designated entity has an established relationship with the student, as defined in Section C (Definitions) of the SAIG Participation Agreement;

**WHEREAS**, the federal Family Educational Rights and Privacy Act of 1974, as amended and its accompanying regulations (“FERPA”) provide that student “education records” and personally identifiable information (PII) from those education records may be released without student or parental consent to authorized representatives of state and local education authorities for the purposes of conducting an audit or evaluation of education programs or for the compliance with Federal legal requirements that relate to those programs (24 C.F.R. §99.31(a)(3)(iv) & §99.35);

**WHEREAS,** The *Data Receiver* desires *Data Provider* to provide such limited FASFA Filing Status Information so as to assist students in completing the FAFSA form;

**WHEREAS**, *Data Provider* is desirous of providing such services and limited FASFA Filing Status Information to the *Data Receiver;* and

**NOW, THEREFORE**, in consideration of the foregoing and the mutual covenants contained herein, *Data Provider* and *Data Receiver* hereby agree as follows:

1. **Incorporation of Recitals:** The matters recited above are hereby incorporated into and made part of this Agreement.
2. **Term of the Agreement:** This Agreement will be effective upon being signed by both parties and will remain effective through the end of Month, Year, unless terminated sooner by either party sending ninety (90) day prior written notice to the other pursuant to the notice provision below.
3. **Scope of Services:** The Parties desire to cooperate with each other in sharing FASFA Filing Status Information (as such specific information is identified and set out in Exhibit A attached hereto and incorporated herein) for the purposes of audit and evaluation and to assist approved Designated Entities in identifying students who have or will complete a Free Application for Federal Student Aid (FAFSA) as defined by the U.S. Department of Education. The approved uses of this information are identified and set out in Exhibit B attached hereto and incorporated herein. The Parties may, from time to time, request changes in the Scope of Services. Any such changes shall be documented by written amendment to this Agreement signed by both parties.

The *Data Receiver,* for the purposes of the FERPA audit or evaluation requirements identified herein, will serve as an authorized representative of the *Data Provider.*

All data exchanges will be conducted via the OPC FAFSA website at: http://fafsaweb.riopc.edu. The Data Receiver will be supplied with a login and password to access the portal and download agreed upon data files. Additionally, the files are downloadable in Excel file format through the portal.

1. **Compensation.**

This agreement is a non-financial understanding between the *Data Provider* and the *Data Receiver.* No financial obligation by or on behalf of either of the parties is implied by a party’s signature at the end of this agreement.

1. **Confidential Information, Dissemination of Information, Ownership, Survival.**
2. **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 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 the 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.
3. **Highly Confidential Information:** “Highly Confidential Information” means personally identifiable student information and data (“PII”) including, but not limited to name, address, student date of birth, and including, but not limited to the limited ISIR/FASFA Filing Status Information being shared pursuant to this Agreement. 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, and only to the extent allowable pursuant to the disclosure provisions in the FAFSA, all provisions of the Higher Education Act, as amended (HEA), 20 U.S.C. 1001 et seq., including but not limited to HEA section 483(a)(3)(E), 20 U.S.C.1090(a)(3)(E) and the Family Educational Rights and Privacy Act (FERPA) and their accompanying regulations.
4. **Transmitting and Storing Highly Confidential Information:** Both parties shall:
5. 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 Encryptions 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 C(i) above;

iii. Encrypt all Highly Confidential Information prior to transmitting it electronically. *Data Provider* 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 password protect any laptop or computer that contains Confidential Information or Highly Confidential Information. Additionally, any laptop or computer that contains Highly Confidential Information shall have its full hard drive encrypted. Neither party shall leave any laptop or computer unattended without enabling a screen-lock or otherwise blocking access to the laptop or computer. Both parties shall ensure that no password or other information sufficient to access a laptop or computer containing Highly Confidential Information is attached or located near the laptop or computer at any time;

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

ix. Only “authorized personnel”[[1]](#footnote-1)within either organization who have signed a Nondisclosure Agreement 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.

x. The *Data Receiver* shall assign at least one employee and/or staff member to be responsible for the security of the data and information provided hereunder (“Data Custodian”), including but not limited to the Confidential Information and Highly Confidential Information provided pursuant to this Agreement, and shall provide the Data Provided with the name(s) and contact information for the individual(s) assigned as such Data Custodian. If more than five (5) Data Custodians are assigned by the *Data Receiver*, then the Data receiver shall assign one such Data Custodian (a “Local Access Manager”) to oversee and be responsible for the security of the data and information, including but not limited to the Confidential Information and Highly Confidential Information, provided to the other Data Custodians pursuant to this Agreement.

1. **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, and only to the extent such disclosure or re-disclosure is allowed under all applicable state and federal privacy laws and regulations, including but not limited to, the privacy provisions of Section 483(a)(3)(E) of the HEA, 20 U.S.C. 1090 (a)(3)(E), and applicable sections of FERPA. Neither party shall issue publicity news releases or grant press interviews related to the Agreement, except as may be required by law or with the prior written consent of the other party. If either party is presented with a request for documents by any administrative agency, or pursuant to a public records request under applicable law, 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 (and/or to the student(s) whose education records and/or PII from his/her education records are the subject to the subpoena in compliance with the requirements of FERPA) 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 agents, 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.**

 The *Data Receiver* further specifically agrees that it will not re-disclose or share the FAFSA Filing Status Information obtained pursuant to this Agreement in personally identifiable form other than (1) to the FAFSA applicant and to the FAFSA applicant’s parents if the applicant is under age 18, to the applicant if the applicant is age 18 or older or enrolled in a post-secondary institution, or (2) if required to do so by law and if such use is consistent with all applicable privacy laws, including the privacy provisions of section 483(a)(3)(E) of the HEA, 20 U.S.C. 1090(a)(3)(E) and the Family Educational Rights and Privacy Act (20 U.S.C. 1232g).

 All data sharing measures will be performed in accordance with the requirements of the federal “Family Education Rights and Privacy Act of 1974 as amended, (20 U.S.C. §1232g) (FERPA). FERPA §1232g(b)(1)(C) provides that education records and personally identifiable information (PII) from education records may be released without student or parental consent to authorized representatives of state educational authorities for use in “connection with the audit and evaluation of Federally [or state] supported education programs, or in connection with the enforcement of, the Federal legal requirements that relate to such programs: *Provided*, That except when collection of personally identifiable information is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements” (FERPA §1232g(b)(3) & 34CFR. §99.35). Additionally, FERPA regulation 34 CFR §99.31(a) (3) allows disclosure of PII without consent to authorized representatives of a state education authority.

**E. Ownership:** All original data, information, and records, generated under this Agreement, including all tangible or intangible property (collectively called “Work Product”) as well as Confidential Information and Highly Confidential Information shall be owned by the *Data Provider*. Each party agrees that all preexisting intellectual property shall and 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 and Highly Confidential Information:** Each party warrants and represents that it shall not use the Confidential Information, Highly Confidential Information or Work Product for any purpose not specifically identified in this Agreement. 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. The use of Highly Confidential information obtained hereunder by the *Data Receiver* shall comply with and be only for the purposes consistent with section 483(a)(3)(E) of the HEA, 20 U.S.C. 1090(a)(3)(E), as well as the requirements of FERPA.

**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 provided hereunder 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 7 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 or 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) business 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 to destroy the Confidential Information and Highly Confidential Information, that party shall provide an affidavit attesting to such destruction.

 In general, proper disposal methods may include, but are not
 limited to:

* 1. For Highly Confidential Information and PII in paper records, shredding, burning, pulping, or pulverizing the records so that the Highly Confidential Information and PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
	2. For Highly Confidential Information and PII on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).
	3. Other methods of disposal also may be appropriate, depending on the circumstances. Organizations are encouraged to consider the steps that other data professionals are taking to protect student privacy in connection with record disposal.

**I. Staff and Agents:** Each party agrees to cause its personnel, staff, and agents, if any, to undertake the same obligations of confidentiality and ownership agreed to herein by that party, and that only those authorized individuals who are relevant to the use of the FASFA Filing Status Information provided pursuant to this Agreement shall have access to such information.

**J. Access to Public Records Act:** The parties acknowledge that this Agreement and all documents submitted to the *Data Provider* related to this contract are a matter of public record and are subject to the Rhode Island Access to Public Records Act (R.I.G.L. section 38-2-1 et. seq.) and any other comparable state and federal laws, and shall be made available to the U.S. Department of Education upon request.

1. **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 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.
2. **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: an attack, penetration, denial of service, disclosure of Confidential Information, Highly Confidential Information, or other sensitive information, misuse of system access, unauthorized access or intrusion (hacking), virus intrusion, scan of systems or networks, or any other activity that could affect either of the party’s systems or data, or the security, confidentiality or integrity of the data received, stored, processed, or maintained. “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. *Data Receiver* shall report to *Data Provider*within 48 hours of *Data Receiver* becoming aware of any use or disclosure of the Confidential and/or Highly Confidential Information in violation of this agreement or applicable law.

*Data Receiver* shall also be responsible for contacting any parties, including students and parents (if applicable) who may have been affected by the Security Incident.

1. **Survival:** The provisions of this Section shall survive the termination or expiration of the Agreement.

6. **Representations and Warranties of the Parties:** Both parties represent and warrant that the following shall be true and correct as of the Effective Date of this Agreement and shall continue to be true and correct during the Term of the Agreement:

 Compliance with Laws**:** The parties are and shall remain in compliance with all applicable federal, state, county, and municipal statutes, laws, ordinances, and regulations relating to this Agreement, as amended from time to time, including but not limited to FERPA, the HEA, the Privacy Act of 1974, as amended, any others relating to privacy, confidentiality of student education records, and non-discrimination.

 Authorization**:** Each party has taken all action necessary for the approval and execution of the Agreement, and execution by the persons signing on behalf of both parties is duly authorized and has been made with complete and full authority to commit both parties to all terms and conditions of this Agreement which shall constitute valid, binding obligations of each party.

7. **Indemnification:** Each party agrees to indemnify and hold harmless the other party and its governing boards, and their members, directors, officers, staff, employees and agents, from and against all claims, judgements and liabilities (including reasonable attorney’s fees and expenses incurred in the defense thereof) arising out of the negligent acts or omissions of the indemnifying party, its employees, agents or contractors, or relating to their breach of this Agreement including those provisions relating to confidentiality, to the extent that such claims, judgements and liabilities are not caused by the negligent acts of omissions of the indemnified party’s employees, agents or contractors. Each party agrees that it shall give the other party prompt notice of any claim, threatened or made, or suit instituted against it, which could result in a claim for indemnification pursuant to the terms hereof. Each party shall have the right but not the obligation, at its own expense, to participate in the defense of any suit, without relieving the other party of any of its obligations hereunder. The indemnification provisions set forth herein shall survive the expiration or termination of this Agreement.

8. **Audit and Oversight:** The *Data Receiver*  agrees to provide *Data Provider* access to *Data Receiver’s* facilities, records, processes, procedures, and electronic systems to ensure that all of its authorized users of the data and information provided pursuant to this Agreement are aware of and are in compliance with all of the requirements to protect and secure any Confidential Information, including Highly Confidential Information, and to ensure Data Receiver’s compliance with all of such requirements. The *Data Receiver* hereby consents to *Data Provider’s*  monitoring, recording and auditing of policies and procedures of data management, and the *Data Receiver* further agrees to provide the *Data Provider* with written evidence of its performance and compliance upon written request.

9. **Contacts:** For the purposes of providing the services described herein, the parties shall set forth below or by attachment if necessary, the primary contact information for authorized recipients/Data Custodians of any Confidential and Highly Confidential Information.

* 1. **Primary Data Receiver Point of Contact/ Primary Data Custodian.**

(Individual becomes Local Access Manager with 5 or more total users; See next page to add additional data custodians):

**Printed Name**: Primary Data Receiver First and Last Name

**Title:** Title

**School District:** District Name / District Code

**Phone Number:** Phone Number

**Physical Address:** Physical Address

**Email Address:** Email Address

* 1. **Primary Data Provider Point of Contact:**

**Printed Name:** John Knight

**Title:** ­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­ FAFSA Completion Project Administrator

**Institution/Agency:** Rhode Island Office of the Postsecondary Commissioner

**Phone Number:** 401-736-1168

**Email Address:** FAFSA@RIOPC.EDU

**Physical Address:** 560 Jefferson Boulevard Suite 100, Warwick, RI 02886

**====================================================================**

10. **Notices:** All legal notices required under this Agreement shall be in writing and sent to addresses and persons set forth below, or to such other addresses as may be designated by a party in writing. All notices shall be deemed received when (i) delivered personally, or (ii) sent by email (followed by the actual document), or (iii) one day after deposit with a commercial express courier specifying next day delivery, with written verification of receipt. Refusal to accept delivery has the same effect as receipt.

 If to *Data Provider*: If to *Data Receiver:*

 OPC, General Counsel Addressee

 560 Jefferson Blvd., Suite 100 Street Address, Room Number

 Warwick, RI 02886 City, State, Zip

**IN WITNESS WHEREOF**, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date below.

**Signed by Data Receiver Designated Signatory:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Date:MM/DD/YYYY

**Printed Name**: Authorized Signatory for District **Title:** Title

**Designated Entity:** District Name / District Code

**Phone Number:** Phone Number

**Physical Address:** Physical Address

**Email Address:** Email Address

**Signed by OPC / Data Provider Designated Signatory: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 Date:MM/DD/YYYY

**Printed Name:** Ronald Cavallaro, Esq.

**Title:** ­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­ Acting Commissioner on Postsecondary Education

**Institution/Agency:** Rhode Island Office of the Postsecondary Commissioner

**Phone Number:** 401-736-1100

**Physical Address:** 560 Jefferson Boulevard Suite 100, Warwick, RI 02886

Please add the contact information for any additional data custodians on the next page. Please note that each district may have **up to five contacts** (**district level and high school level**) before a Local Access Manager is required.

**Additional District Level Data Custodians** (able to access students from the entire district):

Name: First and Last Name

Title: Title Phone: Phone Number

Email: Email Address

Name: First and Last Name

Title: Title Phone: Phone Number

Email: Email Address

**High School Data Custodians** (only able to access students from one high school):

**Contact 1: Name**: First and Last Name High School: High School Name

Title: Title Email:Email Address

 **Contact 2: Name**:First and Last Name High School: High School Name

Title: Title Email:Email Address

 **Contact 3: Name**: First and Last Name High School:High School Name

Title: Title Email: Email Address

 **Contact 4: Name:** First and Last Name High School: High School Name

Title: Title Email:Email Address

**Exhibit A**

**To**

**Data Use & Security Agreement**

**Between**

**DISTRICT NAME
And**

**THE RHODE ISLAND OFFICE OF THE POSTSECONDARY COMMISSIONER**

**DATE MM/DD/YYYY**

Information to be Provided per this Agreement.

FAFSA Filing Status Information, per the SAIG Participation Agreement, is information from an ISIR that the Agency may disclose to LEAs, secondary schools, and Designated Entities on the completion status of a student’s FAFSA. FAFSA Filing Status Information includes: Student’s first name; Student’s last name; Student’s date of birth; Student’s ZIP Code; FAFSA submitted date (the date the FAFSA was submitted to the Department); FAFSA processed date (the date the Department processed the FAFSA); a Selected for Verification flag; and a FAFSA completion flag, as determined by the Agency (e.g., FAFSA not submitted, FAFSA complete, or FAFSA incomplete).

The following specific FAFSA Filing Status Information shall be provided by Data Provider to Data Receiver pursuant to this Agreement:

Student’s first name;
Student’s last name;
Student’s date of birth;
FAFSA submitted date (the date the FAFSA was submitted to the Department);
and a FAFSA completion flag, as determined by the Agency

**Exhibit B**

**To**

**Data Use & Security Agreement**

**Between**

**DISTRICT NAME
And**

**THE RHODE ISLAND OFFICE OF THE POSTSECONDARY COMMISSIONER**

**DATE MM/DD/YYYY**

**Approved Uses of the FASFA Filing Status Information.**

The FASFA Filing Status Information provided by Data Provider to Data Receiver pursuant to this Agreement shall only be used by that local education agency (“LEA”), secondary school, or other entity designated by the U.S. Secretary of Education (“Designated Entity”) to determine the completion status of a student’s Free Application for Federal Student Aid (FAFSA) and facilitate providing assistance to such students in completing the FAFSA.

1. “Authorized personnel” include employees, staff, and authorized agents who are under the “direct control” of the *Data Receiver* with respect to the use and maintenance of the information, and who are permitted access to the information under all applicable statutes and regulations. [↑](#footnote-ref-1)