U.S. Department of Education's
Federal Student Aid (FSA) Partner Connect System and User Access Management

Responsibilities of FSA Partner Connect Users (OMB No. 1845-XXXX)

The Student Aid Internet Gateway (SAIG) was established to allow authorized entities, including postsecondary educational institutions, institutional third-party servicers, Federal Family Education Loan Program (FFELP) guaranty agencies and guaranty agency (GA) servicers, FFELP lenders and lender servicers, federal loan servicers, and State Higher Education Agencies to exchange data electronically with the U.S. Department of Education (Department). To participate in the SAIG, each entity must enroll for SAIG access through Federal Student Aid (FSA) Partner Connect. The enrollment process enables the organization enrolling to select services to receive, submit, view, and/or update student financial aid data online and by batch using Department provided software.

There are five categories of users who may obtain data from the Department's systems for the purposes of administering the Higher Education Act (HEA) programs. Additionally, FSA Partner Connect facilitates system access for the U.S. Department of Homeland Security's Systematic Alien Verification Entitlements (SAVE) system (referred to as "*other Federal agencies' systems*" throughout the document). These user types are defined below and referenced throughout the Responsibilities of FSA Partner Connect Users.

- **Primary Administrator:** A Primary Administrator is defined as an individual appointed by an organization who is the primary responsible party to manage the organization's user access.
- **Secondary Administrator:** A Secondary Administrator is defined as an additional backup administrator that shall assist with managing the organization's user access.
- **SAIG Mailbox Owner:** An SAIG Mailbox Owner is defined as a user who owns a Primary SAIG Mailbox, Batch SAIG Mailbox, Individual SAIG Mailbox, Test SAIG Mailbox, or Federal Tax Information (FT) Mailbox.
- **SAIG Mailbox User:** An SAIG Mailbox User is defined as an individual chosen by the Primary or Secondary Administrator to manage the password associated with a Primary SAIG Mailbox, Batch SAIG Mailbox, Individual SAIG Mailbox, Test SAIG Mailbox, or FT Mailbox.
- **Partner User:** A Partner User is defined as an individual within an organization who does not have administrative privileges and can have EDconnect access to an SAIG or FT Mailbox.

Each user must read, acknowledge, and electronically sign.

1. **Responsibilities of the Primary Administrator, Secondary Administrator, SAIG Mailbox Owner, and SAIG Mailbox User:**

   - Must ensure that SAIG computing resources are used only for official organization business.
   - Must ensure that a substantially Established Relationship with the applicant is in place (e.g., the applicant has applied for admission to the institution, the applicant has included the institution on the *Free Application for Federal Student Aid* (FAFSA®), or the Lender holds a loan for the borrower) before accessing Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the Higher Education Act (HEA) programs and to obtain privacy protected information about the student.
   - Only the owner of the SAIG Mailbox enrolled for the National Student Loan Data System (NSLDS) Online Service is permitted to use the NSLDS.
   - Must use software provided by the Department to monitor SAIG Mailbox activity. This software will keep track of who is using the SAIG Mailbox, what information is being accessed, the date and time of access, and the batch number (if applicable).
   - By applying for access to Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the HEA programs, users must comply with the acceptable use of Department systems, including compliance with the Terms of Service, Code of Conduct, Rules of Behavior, and Information Security Standards which includes, among other things, monitoring, recording, and auditing of the information gained in this manner from FSA systems.
   - Must ensure that all Federal Student Aid applicant information (including Federal tax information) is protected from access by or disclosure to unauthorized personnel. In the event of an unauthorized disclosure or breach of student applicant information or other sensitive information (such as personally identifiable information), the Administrator must notify Federal Student Aid by completing the Cybersecurity Breach Intake Form on FSA Partner Connect as soon as possible but no later than 24 hours after identification of the unauthorized disclosure or breach. Organizations must also report any breaches that occur at their third-party providers that maintain, store, or otherwise utilize the data. Any information that is provided to third parties by the organization is also covered by these same provisions. Organizations must cooperate with the Department and assist in responding to an unauthorized disclosure or breach by providing any documentation or information requested by the Department.
   - Must ensure that all Federal Student Aid applicant information (including federal tax information) is used only for the application, award, and administration of financial aid to the applicant; and consistent with the requirements of 20 U.S.C.

§1090 and 26 U.S.C. §6103(l)(13).

- Must adhere to the strict confidentiality and integrity requirements of the Gramm – Leach – Bliley Act (GLBA) and, when accessing FTI, the requirements of 26 U.S.C. §6103.
- Must ensure that password sharing, the sharing of system access, and the use of any tools that allow access to the SAIG are strictly prohibited. (These tools are called "authenticators.")
- Must ensure that access is provided only to systems, networks, data, control information, and software for which the Administrator is authorized.
- Must ensure that procedures for sanitizing stored information are followed (e.g., overwriting electronic media that contain sensitive information before reuse).
- The SAIG Mailbox Owner and User must inform the organization's Primary Administrator when access to a Federal Student Aid system or other Federal agencies' systems for the purposes of administering the HEA programs, is no longer required (i.e., the individual is leaving a position or their job responsibilities have changed).
- The information provided to the Administrator and SAIG Mailbox Owner and User by the Department is protected by the Privacy Act of 1974, as amended (Privacy Act), 5 U.S.C. §552a. Protecting this information, once it is entrusted to the Administrator and SAIG Mailbox Owner and User, becomes their responsibility. Therefore, the Administrator and SAIG Mailbox Owner and User must protect the privacy of all information that has been provided by the Department. The Administrator and SAIG Mailbox Owner and User understand that any person, including themself, who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and is subject to a fine of up to $5,000 (5 U.S.C. §552a(i)(3)).
- The federal tax information (FTI) provided to the Administrator and SAIG Mailbox Owner and User by the Department is protected by the Internal Revenue Code of 1986, as amended. Protecting FTI, once it is entrusted to the Administrator and SAIG Mailbox Owner and User, becomes their responsibility. The Administrator and SAIG Mailbox Owner and User understand that any person, including themself, who knowingly and willfully conduct:
  - ***unauthorized disclosure of a tax return or return information*** is punishable as a felony by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution (26 U.S.C. §7213).
  - ***unauthorized inspection of a tax return or return information*** is punishable by a fine of up to $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution (26 U.S.C. §7213A).
- The Administrator and SAIG Mailbox Owner and User understand that, pursuant to 26 U.S.C. §7431 a taxpayer may bring civil action for damages against an officer or employee who has inspected or disclosed, knowingly or by reason of negligence, such taxpayer's tax return or return information in violation of any provision of IRC §6103.
- The Administrator and SAIG Mailbox Owner and User understand that any person, including themself, who knowingly and willfully use an access device (18 U.S.C. §1029(e)(1)) issued to another person or obtained by fraud or false statement to access the Department information technology systems for fraud, commercial advantage, or private financial gain shall be guilty of a felony and is subject to a fine of up to $20,000, imprisonment for up to five years, or both, under provisions of the United States Code (20 U.S.C. §1097(e)).

2. Additional Requirements of the Primary Administrator:

- Must ensure that all users are aware of and comply with all the requirements to protect and secure data from Departmental or other Federal agencies' systems for the purposes of administering the HEA programs.
- At least on an annual basis or sooner as may be required by applicable law, must validate all Administrator and user access rights for the organization.
- At least on an annual basis or sooner as may be required by applicable law, must monitor the organization's NSLDS user access.
- Must ensure that the organization has a process to inform the Administrator of any changes in a user's need for access to FSA systems or other Federal agencies' systems for the purposes of administering the HEA programs, because of changes to job responsibilities or termination of employment. The Administrator must immediately deactivate or delete user access rights for organization employees who no longer require access.

3. Responsibilities of the Partner User:

Any individual who is not an Administrator and who accesses Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the HEA programs, and/or uses resources that access Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the HEA programs, whether by batch or online, must read this statement.

The user understands that intentional submission of false or misleading information to the Department is subject to a fine up to $10,000, imprisonment for up to five years, or both, under provisions of the United States Criminal Code (including 18 U.S.C. §1001). The user also agrees to comply with all provisions of Section 483 of the Higher Education Act of 1965, as amended.

The user understands that the intentional use of an access device (18 U.S.C. §1029(e)(1)) issued to another person or obtained by fraud or false statement to access the Department information technology systems for fraud, commercial advantage, or private financial gain shall be guilty of a felony and is subject to a fine of up to $20,000, imprisonment for up to five years, or both, under provisions of the United States Code (20 U.S.C. §1097(e)).

The user understands that the information provided by the Department is protected by the Privacy Act. Protecting this information, once it is entrusted to the user, becomes their responsibility. Therefore, the user agrees to protect the privacy of all information provided to them by the Department. The user understands that any person, including themself, who knowingly and willfully requests or obtains any record concerning an individual from an organization under false pretenses, shall be guilty of a misdemeanor and is subject to a fine of up to $5,000 (5 U.S.C. §552a(i)(3)).

Appropriate uses of Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the HEA programs, by a Partner User:

- Must use FSA systems and services only for official organization business.
- Must ensure that a substantially Established Relationship with the applicant is in place (e.g., the applicant has applied for admission to the institution, the applicant has included the institution on the FAFSA®, or the lender holds a loan for the borrower) before accessing Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the HEA programs, to obtain privacy protected information about the student.
- Must ensure that all Federal Student Aid applicant information (including federal tax information) is used for the application, award, and administration of financial aid to an applicant consistent with 20 U.S.C. §1090 and redisclosure requirements of FTI under 26 U.S.C. §6103(l)(13).
- Must adhere to the strict confidentiality and integrity requirements of the GLBA and, when accessing FTI, the requirements of 26 U.S.C. §6103.
- Must know the name of the Primary Administrator and how to contact that individual.
- Must protect all Federal Student Aid systems or other Federal agencies' systems for the purposes of administering the HEA programs from access by or disclosure to unauthorized personnel.
- Must report immediately to the Primary Administrator any security incidents, potential threats, or vulnerabilities that involve FSA systems and services.
- Must report to the Primary Administrator any compromise, suspected compromises, or incidents of sharing of a password or any other authenticator.
- Must access only those systems, networks, data, control information, and software for which he or she is authorized.
- Must ensure that all FSA systems and services information is marked according to its sensitivity and is properly controlled and stored.
- Must inform the organization's Primary Administrator that the Partner User no longer needs access to a Federal Student Aid system (i.e., the individual is leaving their position or their job responsibilities have changed).
- Must not add code that might be harmful to the SAIG or FSA systems and services and other Federal agencies' systems.

4. Agreements

- The Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and/or Partner User agree(s) and understand(s) that intentional submission of false or misleading information to the Department is subject to a fine of up to $10,000, imprisonment for up to five years, or both, under provisions of the United States Code (including 18 U.S.C. §1001). The Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and/or Partner User also agree(s) to comply with all provisions of Section 483 of the Higher Education Act of 1965, as amended.
- The Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and/or Partner User agree(s) and understand(s) that the unauthorized inspection (viewing) and disclosure of federal tax information (FTI) may lead to criminal and/or civil penalties pursuant to 26 U.S.C. §§7213, 7213A, and 7431. Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and/or Partner User further agree(s) and understand(s) that a taxpayer may bring civil action for damages against an officer or employee who has inspected or disclosed, knowingly or by reason of negligence, such taxpayer's tax return or return information in violation of any provision of IRC §6103.
- The Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and/or Partner User agree(s) to adhere to and understand(s) the strict confidentiality and integrity requirements of the GLBA and, when accessing FTI, the requirements of 26 U.S.C. §6103 and ensure that all Federal Student Aid applicant information (including federal tax information) is used for the application, award, and administration of financial aid to an applicant consistent with 20 U.S.C. §1090 and

redisclosure requirements of FTI under 26 U.S.C. §6103(l)(13).

- Section 490 of the Higher Education Act of 1965 provides for criminal penalties for any person, who knowingly and willfully uses an access device (18 U.S.C. §1029(e)(1)) issued to another person or obtained by fraud or false statement to access the Department information technology systems for fraud, commercial advantage, or private financial gain. As such, the Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and/or Partner User agree(s) and understand(s) that intentional use an access device (18 U.S.C. §1029(e)(1)) issued to another person or obtained by fraud or false statement to access the Department information technology systems for fraud, commercial advantage, or private financial gain shall be guilty of a felony and is subject to a fine of up to $20,000, imprisonment for up to five years, or both, under provisions of the United States Code (20 U.S.C. §1097(e)).

5. Privacy Act Statement

AUTHORITY:

The Department is authorized to collect the SAIG enrollment information that you provide pursuant to Title IV of the Higher Education Act of 1965, as amended (HEA), 20 U.S.C. §1070 *et seq.*, and, with respect to Social Security numbers, pursuant to 31 U.S.C. §7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

PURPOSE(S):

The Department collects the aforementioned information for the purposes of: (1) processing stored data from the SAIG, Participation Management System Enrollment Forms (web and paper versions); (2) maintaining the SAIG, Participation Management System Enrollment website (titled https://FSAWebEnroll.ed.gov); (3) managing the assignment of individual electronic SAIG, Participation Management System mailbox numbers, known as "TG numbers"; and (4) authorizing users of the Department's Federal Student Aid systems, including Central Processing System (CPS), electronic Campus Based (eCB) System, National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD) System, Financial Management System (FMS), Enterprise Complaint System (ECS), and Access and Identity Management System (AIMS), and the system of the U.S. Department of Homeland Security (DHS), for the purposes of administering or assisting in administering programs authorized under title IV of the HEA.

NON-CONSENSUAL DISCLOSURES:

The Department may disclose the aforementioned information pursuant to the following routine uses listed in the Department's system of records notice, entitled "Student Aid Internet Gateway (SAIG), Participation Management System" (18–11–10), 83 FR 8855-8859 (March 1, 2018), without the consent of the individual if the disclosure is compatible with the purposes for which the information was collected:

(1) **Program Disclosures**. The Department may disclose records maintained in the SAIG, Participation Management System, to DHS for the purpose of allowing authorized users who are eligible to participate in the electronic exchange of data with the Department to transmit files to and from the following databases and access the Department's websites online for the purposes of administering or assisting in administering programs authorized under title IV of the HEA:

(a) COD System;
(b) CPS;
(c) eCB System;
(d) NSLDS;
(e) FMS;
(f) ECS;
(g) AIMS; and,
(h) the DHS system.

The Department will only disclose records from this system to DHS for purposes of administering or assisting in administering programs authorized under title IV of the HEA and only after the Department has approved in writing a request from DHS to access these records.

(2) **Freedom of Information Act (FOIA) or Privacy Act Advice Disclosure.** The Department may disclose records to the U.S. Department of Justice (DOJ) or the Office of Management and Budget (OMB) if the Department seeks advice regarding whether records maintained in this system of records are required to be disclosed under the FOIA or the Privacy Act.

(3) **Disclosure to the DOJ.** The Department may disclose records to the DOJ to the extent necessary for obtaining DOJ advice on any matter relevant to an audit, inspection, or other inquiry related to the programs covered by this system.

(4) **Contract Disclosure.** If the Department contracts with an entity to perform any function that requires disclosing records to the contractor's employees, the Department may disclose the records to those employees. As part of such a contract,

the Department shall require the contractor to agree to establish and maintain safeguards to protect the security and confidentiality of the records in the system.

(5) **Litigation and Alternative Dispute Resolution (ADR) Disclosures**.

(a) *Introduction.* In the event that one of the following parties is involved in judicial or administrative litigation or ADR, or has an interest in judicial or administrative litigation or ADR, the Department may disclose certain records to the parties described in paragraphs (b), (c), and (d) of this routine use under the conditions specified in those paragraphs:

i. The Department, or any of its components;
ii. Any Department employee in their official capacity;
iii. Any Department employee in their individual capacity where the DOJ agrees to or has been requested to provide or arrange for representation of the employee;
iv. Any Department employee in their individual capacity where the Department has agreed to represent the employee;
v. The United States where the Department determines that the litigation is likely to affect the Department or any of its components.

(b) *Disclosure to DOJ.* If the Department determines that disclosure of certain records to the DOJ is relevant and necessary to judicial or administrative litigation or ADR, and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to the DOJ.

(c) *Adjudicative Disclosures.* If the Department determines that disclosure of certain records to an adjudicative body before which the Department is authorized to appear or to a person or entity designated by the Department or otherwise empowered to resolve or mediate disputes, is relevant and necessary to the judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to the adjudicative body, person, or entity.

(d) *Parties, Counsel, Representatives, and Witnesses.* If the Department determines that disclosure of certain records to a party, counsel, representative, or witness is relevant and necessary to the judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to the party, counsel, representative, or witness.

(6) **Research Disclosure.** The Department may disclose records to a researcher if the official serving or acting as the Chief Operating Officer of Federal Student Aid determines that the individual or organization to which the disclosure would be made is qualified to carry out specific research related to functions or purposes of this system of records. The official may disclose records from this system of records to that researcher solely for the purpose of carrying out that research related to the functions or purposes of this system of records. The researcher shall be required to agree to maintain safeguards to protect the security and confidentiality of the disclosed records.

(7) **Congressional Member Disclosure.** The Department may disclose records to a Member of Congress in response to an inquiry from the Member made at the written request of the individual whose records are being disclosed. The Member's right to the information is no greater than the right of the individual who requested it.

(8) **Enforcement Disclosure.** In the event that information in this system of records indicates, either on its face or in connection with other information, a violation or potential violation of any applicable statute, regulation, or order of a competent authority, the Department may disclose the relevant records to the appropriate agency, whether foreign, Federal, State, Tribal or local, charged with the responsibility of investigating or prosecuting that violation or charged with enforcing or implementing the statute, Executive Order, rule, regulation, or order issued pursuant thereto.

(9) **Employment, Benefit, and Contracting Disclosure.**

(a) *For Decisions by the Department.* The Department may disclose a record to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to a Department decision concerning the hiring or retention of an employee or other personnel action, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

(b) *For Decisions by Other Public Agencies and Professional Organizations.* The Department may disclose a record to a Federal, State, local, or foreign agency or other public authority or professional organization, in connection with the hiring or retention of an employee or other personnel action, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit, to the extent that the record is relevant and necessary to the receiving entity's decision on the matter.

(10) **Employee Grievance, Complaint, or Conduct Disclosure.** If a record is relevant and necessary to an employee grievance, complaint, or disciplinary action involving a present or former employee of the Department, the Department may disclose a record from this system of records in the course of investigation, fact-finding, mediation, or adjudication, to any party to the grievance, complaint, or action; to the party's counsel or representative; to a witness; or to a designated fact-finder, mediator, or other person designated to resolve issues or decide the matter.

(11) **Labor Organization Disclosure.** The Department may disclose records from this system of records to an arbitrator to resolve disputes under a negotiated grievance process or to officials of a labor organization recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation.

(12) **Disclosure in the Course of Responding to a Breach of Data.** The Department may disclose records from this system to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that there has been a breach of the system of records; (b) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operation), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(13) **Disclosure in Assisting another Agency in Responding to a Breach of Data.** The Department may disclose records from this system to another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

CONSEQUENCES OF FAILING TO PROVIDE INFORMATION:

Without the information provided through SAIG Enrollment/Participation Management System, an Administrator or the participating entity would be denied access to electronically transmit reports and data and would be denied access to all systems/websites affiliated with the *Responsibilities of FSA Partner Connect Users* as appropriate.

ADMINISTRATOR, SAIG MAILBOX OWNER, SAIG MAILBOX USER, AND PARTNER USER RESPONSIBILITIES:

The information provided to the Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and Partner User by the Department is protected by GLBA, the Internal Revenue Code of 1986, as amended, and the Privacy Act. Protecting this information, once it is entrusted to the Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and Partner User, becomes their responsibility. Therefore, the Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and Partner User agree to protect the privacy of all information that has been provided by the Department. The Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and Partner User understand that any person, including themself, who knowingly and willfully requests or obtains any record concerning an individual from an organization under false pretenses shall be guilty of a misdemeanor and is subject to a fine of up to $5,000 (5 U.S.C. §552a(i)(3)). The Administrator, SAIG Mailbox Owner, SAIG Mailbox User, and Partner User further agree and understand that any person, including themself, who knowingly and willfully use an access device (18 U.S.C. §1029(e)(1)) issued to another person or obtained by fraud or false statement to access the Department information technology systems for fraud, commercial advantage, or private financial gain shall be guilty of a felony and is subject to a fine of up to $20,000, imprisonment for up to five years, or both, under provisions of the United States Code (20 U.S.C. §1097(e)).

I certify that I have read these responsibilities, understand them, and will protect all data obtained through or provided to Department systems. My electronic acknowledgement affirms that I have read these *Responsibilities of FSA Partner Connect Users* and agree to abide by them.

U.S. Department of Education's
Federal Student Aid (FSA) Partner Connect System and User Access Management

Paperwork Burden Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. The valid OMB control number for this information collection is 1845-NEW. Public reporting burden for this collection of information is estimated to average 10-20 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The obligation to respond to this collection is required to obtain or retain a benefit (20 U.S.C. 1070 *et seq.*). If you have comments or concerns regarding the status of your individual submission of this application, please contact the **FSA Partner and School Relations Center** via the Contact Customer Support form on FSA Partner Connect (https://fsapartners.ed.gov/help-center/contact-customer-support) or phone at 1-800-848-0978 (Monday through Friday, 8:00 A.M. to 8:00 P.M. Eastern Time) directly.