

Federal Student Aid User Statement

Any individual who accesses Federal Student Aid systems and/or uses resources that access those systems, whether by batch or online, must read this statement. In addition, the Federal Student Aid User Statement must be completed and signed by the user and the Primary Destination Point Administrator and the original must be maintained by the organization. The user should keep a copy of the signed statement for his or her records.

The user understands that intentional submission of false or misleading information to the U.S. Department of Education 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 information provided by the U.S. Department of Education is protected by the Privacy Act of 1974, as amended. Protecting this information, once it is entrusted to the user, becomes his or her responsibility. Therefore, the user agrees to protect the privacy of all information provided to him or her by the U.S. Department of Education. The user understands that any person, including himself or herself, 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.

Appropriate Use of Federal Student Aid Systems

Appropriate uses of Federal Student Aid systems by a SAIG user (list is not exhaustive):

- Must use SAIG computing resources only for official government business.
- Must ensure that a substantially established relationship with the applicant is in place (e.g., the applicant is a resident of the state, has applied for admission to an institution in that state, or the applicant has provided written permission to the state) before accessing Federal Student Aid systems.
- Must know the names of the Primary Destination Point Administrator and/or the Destination Point Administrator for each of the destination points accessed and how to contact those individuals.
- Must protect all Federal Student Aid systems from access by or disclosure to unauthorized personnel.
- Must report immediately to the Destination Point Administrator any security incidents, potential threats, or vulnerabilities that involve SAIG resources.
- Must report to the Destination Point 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 information from the SAIG is marked according to its sensitivity and is properly controlled and stored.
- Must inform the organization's Primary Destination Point Administrator when he or she no longer needs access to a Federal Student Aid system (i.e., the individual is leaving his or her position or his or her job responsibilities have changed).
- Must avoid the introduction of any code that might be harmful to the SAIG.

TG# _____

Destination Point Administrator (DPA) Name _____

SAIG User Name _____
(Print)

SAIG Job Title _____ SSN _____

Phone #(____) _____

SAIG User Signature _____ Date _____

DPA Signature _____ Date _____

(This statement with an original signature must be maintained by the Primary Destination Point Administrator.)

**Do Not Submit This User Statement -
The Signed Original Form Must Be Retained By The Organization**