

SAIG User Statement

Anyone who accesses Title IV program data and uses resources that access SAIG (such as computers or workstations) must read and sign this statement. Keep a copy of the signed statement for your records. A signed original SAIG user Statement must be completed and maintained by the destination point administrator for each of the destination points (electronic mailboxes) to which you have access.

A SAIG user understands that if he or she intentionally submits false or misleading information to the U.S. Department of Education, he or she will be 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 SAIG user also agrees to comply with all provisions of Section 483 of the Higher Education Act of 1965, as amended.

A SAIG user understands that the information provided to him or her 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 SAIG user, becomes his or her responsibility. Therefore, the SAIG user agrees to protect the privacy of all information that has been provided to him or her by the U.S. Department of Education. The SAIG 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 may be fined not more than \$5,000.

Appropriate Use

At a minimum, appropriate use consists of the following:

- Using SAIG computing resources only for official government business. Any other use must be approved expressly by the U.S. Department of Education.
- Knowing the SAIG destination point administrator for each of the destination points you access and how to contact them.
- Protecting all SAIG information from access by or disclosure to unauthorized personnel.
- Reporting immediately to your destination point administrator any security incidents, potential threats, or vulnerabilities that involve SAIG resources.
- Protecting any tools, such as passwords, that allow you access to SAIG (these tools are called “authenticators”).
- Reporting to your destination point administrator any compromise, suspected compromise, or incidents of sharing of a password or any other authenticator.
- Accessing only systems, networks, data, control information, and software for which you are authorized.
- Ensuring that all information that comes from SAIG is marked according to its sensitivity and is properly controlled and stored.
- Informing your destination point administrator when you no longer need access to a SAIG resource, such as when you change jobs or leave employment.
- Avoiding the introduction of any code that might be harmful to 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 Destination Point Administrator.)

Do Not Send This to SAIG