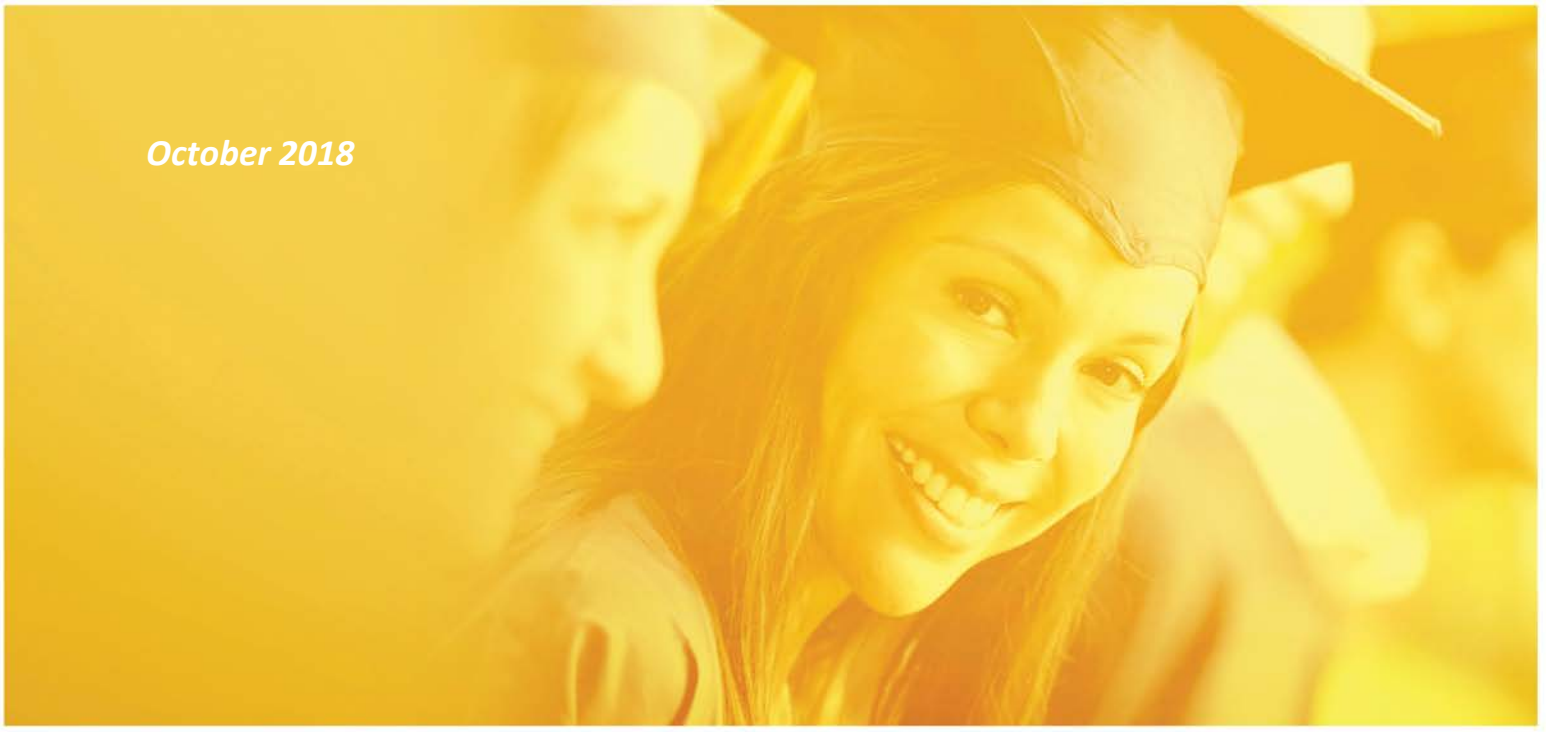
Army Educational Outreach Program

AEOP PII Guidance



October 2018

AEOP PII Guidance

In the context of recent and evolving threats to our national security, the AEOP herewith emphasizes the need for vigilance in protecting the personally identifiable information (PII) of its key stakeholders, to include students, educators, partners, and colleagues. We collectively are the first line of defense and are responsible for protecting the personal information of one another.

This memorandum reminds all who obtain, access, store and transmit the data that has been entrusted to us, that PII must be treated with the utmost care, at all times. Any personal information that is collected, stored, or contained in our systems shall be handled so that the security and confidentiality of the information is preserved and protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. The privacy of an individual is a personal and fundamental right that will be respected and protected by all members of the AEOP Consortium.

A cultural shift toward social media as a preferred form of communication and networking means that extra care must be taken when operating in these public domains. Diligence must be exercised so that PII is not posted publicly through our interactions over social media. This document will outline the information that constitutes PII, as well as practices, for collecting, safeguarding, and transmitting it.

For questions regarding the safe handling of PII, please contact either the AEOP lead organization or AEOP's Cooperative Agreement Managers.

Definitions

- **PII:** Any information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date, and place of birth, mother's maiden name and biometric records, including any other personal information, which is linked or linkable to a specific individual. This information can be in hardcopy (paper) or electronic format, stored on desktop computers, laptops, personal electronic devices such as blackberries, and found within databases. This includes but is not limited to education records, financial transactions, medical files, criminal records or employment history

- **High Impact PII**: Any organizational-wide, program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service. Also any compilation or electronic records containing PII on less than 500 individuals identified by the information or data owner as requiring additional protection measures.

Safeguarding and Handling

Appropriate administrative, technical and physical safeguards will be maintained to ensure the security and confidentiality of PII of consortium administration, members, partners, students, teachers, parents, and all associated personnel and to protect against any compromise which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual whose information is stored or transferred in either hardcopy or electronic form.

Safeguarding PII requires all who have access to:

1. Minimize the collection of PII.
2. Ensure that compromise of PII is immediately reported to the AEOP Lead Organization
3. Reduce the use of or use alternatives to Social Security Numbers (SSN) whenever possible.
4. Ensure mobile computing devices or removable electronic media do not store or process High Impact PII without express approval from the U.S. Army.
5. Ensure mobile computing devices or removable electronic media that process or store High Impact electronic PII records are restricted to areas that are protected by adequate safety measures.
6. Ensure PII is only electronically transmitted through encrypted and secure mediums. PII may not be transmitted via unencrypted email nor may it be sent via facsimile (fax).

Storage

1. Do not store PII on media or devices with unregulated access.
2. Cover or place documents in an out-of-sight location when those without an official need to know enter the workplace.
3. Any PII stored on a shared drive or within a collaborative application should be controlled allowing only those with a need to know to have access. If PII is stored on a shared drive or within a collaboration application that is unable to properly safeguard the information by limiting access controls to the material then the data must be protected from being opened by individuals who do not have an official need to know.
4. PII should never be stored on personally owned information systems including computers, smart phones, tablets, memory cards, portable hard disks, etc.
5. Store PII to preclude unauthorized access during non-work hours. The PII should be stored in a locked desk, file cabinet, bookcase or office that is not accessible during non-duty hours.

Collecting, Transmitting and Transporting

1. All requests for PII should include an appropriate Privacy Statement to ensure the individuals(s) providing the PII understands how it will be used and/or distributed.
2. Only individuals with a valid need-to-know should transmit or receive PII in hardcopy or electronic form.
3. When mailing PII, use an opaque envelope, ensure it is properly sealed, is not marked with any reference to its contents and is addressed to the attention of an authorized recipient.
4. When physically transporting PII, ensure the information is adequately protected.

5. Restrict discussions of PII over the telephone lines to a minimum for the official purposes only. Do not discuss PII within an open environment where it could be potentially overheard by those who do not have an official need to know.
6. Ensure that all electronic records containing PII shall be transmitted by an Army approved encrypted or protected format. Only individuals with a valid need-to-know should transmit or receive PII in hardcopy or electronic form. Facsimile transmission is not an appropriate transportation method for PII.
7. If in doubt as to the adequacy of protection measures, do not post, store, transport or transmit PII.
8. The AMRDEC Safe Site is a viable alternative to unencrypted email and facsimile transmission (https://safe.amrdec.army.mil/safe/), as long as either the sender or receiver has a Common Access Card (CAC Card).

Internet and Social Media

1. PII should not be posted on publicly accessible websites, social media, or other locations on the internet.
2. Social media must be administered and actively monitored to ensure that public interaction with consortium managed accounts do not post or allude to PII. Swift action must be taken to take down, or correct PII posted via public interaction within consortium channels.
3. No aggregate of information posted publicly on the internet should allude to or infer possible PII.
4. If in doubt as to the adequacy of protection measures, do not post, store, transport or transmit PII.