Welcome

The mission of this office is to implement and administer the Department of Defense Education Activity's Federally Mandated Programs through advice, monitoring, transparency, official reporting, and training.

Authorities

- DoDEA Privacy Requirements Memorandum
- Privacy Act of 1974
- E-Government Act of 2002
- Social Security Number Fraud Prevention Act of 2017
- DoD Instruction 5400.11, Privacy and Civil Liberties Programs
- DoD Manual 5400.11, Volume 2, Breach Preparedness and Response Plan
- DoD Regulation 5400.11-R, Privacy Program
- DoD Instruction 5400.16, Privacy Impact Assessment (PIA) Guidance
- DoDI 1000.30, Reduction of Social Security Number (SSN) Use Within DoD

SORNs & PIAs
DoDEA System of Records Notices (SORN)

- DoDEA 21
- DoDEA 23
- DoDEA 26
- DoDEA 27
- DoDEA 29
- DoDEA 30
  - DoD-Wide Notices
  - Government-Wide Notices

DoDEA Privacy Impact Assessments (PIA)

- Certificate Program
- FOIA Xpress
- Serious Incident Reports (SIRS)
- Travel Orders Processing System (TOPS)
- DoDEA Notification System (DNS)
- Research Approval Process
- DoDEA Student Information System (DSIS)
- DoDEA Employment Application System (EAS)
- DoD Impact Aid Application & Database
- DoDEA Remote Work Program
- Navigate360

SORN & PIA Related Inquiries/Requests

Please send your requests, general questions, comments, or concerns along with your name, phone number and email address to the DoDEA Privacy Office at the below email address: HQ-privacy@dodea.edu

Report a Breach

Report a Breach of PII

A breach of PII is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. This includes, but is not limited to, posting PII on public-facing websites; sending PII via email to unauthorized recipients; providing hard copies of PII to individuals without a need to know; loss of electronic
devices or media on which PII is stored; use of PII by employees for unofficial business; and all other unauthorized access to and use of PII.

**Immediate actions to be taken if a breach of PII occurs:**

The most important thing to do if you discover that a breach of PII has occurred or is ongoing is to STOP IT as soon as possible.

1. If there is a suspected or confirmed breach of PII, fill out DD Form [DD2959](#), Breach of Personally Identifiable Information (PII) Report, to report it immediately.
2. After you complete the form, submit it to the [Privacy Office](#) within One (1) hour of discovery.

**NOTE:** The DD2959 form should also be used to report updates to previous submissions.

**Repercussions for DoDEA personnel who breach PII security:**

In the event of a breach of PII, the DoDEA employee held responsible will be required to complete the [Safeguarding PII Refresher Training](#) and the [OSD Records and Information Management Training](#). The method of training delivery will be determined by the DoDEA CPO and SCOP. Furthermore, upon successful completion of the prescribed training, responsible employees are obligated to furnish all requisite attestations to their immediate supervisor and the [DoDEA Privacy Office](#).

**NOTE:** The Privacy Act imposes civil and/or criminal penalties on employees who fail to safeguard PII. Non-compliance may result in adverse action being taken against the responsible employee.

**Notification to affected parties:**

1. The DoDEA Breach Response Team will designate the appropriate DoDEA office responsible for generating and sending the official notification letter.
2. The official notification letter MUST be signed by the designated empowered official and securely emailed or sent via certified USPS mail.
3. The official notification letter MUST be sent to those affected within Ten (10) business days from the date of breach discovery.

**Privacy Training & Resources**

**Training Modules:**

- [Privacy for Federal Contractors](#)
- [Safeguarding PII Training (Refresher)](#)
- [DoDEA Records Management Fundamentals](#)
- [Controlled Unclassified Information Training](#)
Privacy Act Training

Additional Resources:

- PII Management Guide
- Safeguarding PII Do's & Don'ts
- Emailing PII Guide
- How to Encrypt Documents Containing PII

Safeguarding Personally Identifiable Information

Important Information on Emails Containing PII

Contacts

Samuel Gotti
Component Privacy Officer (CPO)

James Revell
Senior Component Official for Privacy (SCOP)

Please send your requests, general questions, comments, or concerns along with your name, phone number and email address to the DoDEA Privacy Office at: HQ-Privacy@DoDEA.EDU

All breach related inquiries should be sent to: HQ-Breach@DoDEA.EDU

Website Privacy

The Department of Defense Education Activity (DoDEA) is committed to protecting the privacy of employees, students, and members of the public. The DoDEA.edu website is provided as a public service by the Department of Defense Education Activity Communications Division.

Information presented on this website is considered public information and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested.

If you choose to provide us with personal information -- like filling out a Contact Us form with email and/or postal addresses -- we only use that information to respond to your message or request. We will only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We never create individual profiles or give it to privately owned companies or organizations. DoDEA.edu never collects information for commercial marketing and does not sell or rent any of your personal information. While you must provide an email address or postal address for a response other than those generated automatically in response to questions or comments that you may submit, we recommend that you NOT include any other personal information or other sensitive factors, especially Social Security Numbers.
DoDEA enforces strict adherence to DTM 07-015 and DoDI 1000.30 and has prohibited the intake/distribution of SSN on all methods of collection.

We maintain a variety of physical, technical and administrative safeguards to protect your personal information. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with Office of the Secretary of Defense Records Disposition Schedules, Record Group 330, and National Archives and Records Administration guidelines.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

If you have any questions or comments about the information presented here, please forward them to us using our Contact Us page.

Use of Measurement and Customization Technology:

This website uses measurement and customization technology known as a "cookies." Cookies are used to remember a user's online interactions with a website or online application to conduct measurement and analysis of usage or to customize the user's experience.

Two kinds of cookies are used on this website. A single-session cookie (Tier 1) is a line of text that is stored temporarily on a user's computer and deleted as soon as the browser is closed. A persistent or multisession cookie (Tier 2) is saved to a file on a user's hard drive and is called up the next time that user visits a website. Use of these cookies does not involve the collection of a visitor's personally identifiable information.

The Department of Defense Education Activity does not use the information associated with cookies to track individual user activity on the internet outside DoDEA websites, nor does it share the data obtained through such technologies, without the user's explicit consent, with other departments or agencies. DoDEA does not keep a database of information obtained from the use of cookies.

Cookies are enabled by default to optimize website functionality and customize user experience. Users can choose not to accept the use of these cookies by changing the settings on their local computer's web browser. The USA.gov website, https://www.usa.gov/optout-instructions, provides general instructions on how to opt out of cookies and other commonly used web measurement and customization technologies. Opting out of cookies still permits users to access comparable information and services; however, it may take longer to navigate or interact with the website if a user is required to fill out certain information repeatedly.

Specific Technologies/Vendors:

Tier 1 cookies are used for technical purposes to improve a user experience and to allow users to more easily navigate the website.
Akamai speeds the delivery of content and applications for customers through using automatic, intermediate and temporary information storage to make the onward transmission of that information to other recipients more efficient. Temporary storage processes retain information only as long as is reasonably necessary to transmit the data. Intermediate storage processes retain information only so long as is reasonably necessary for continued transmission, to maintain the security of the network and the data, to monitor and improve website performance and for related administrative purposes. Akamai does not collect, use or disclose your personally identifiable information.

SiteImprove and Google Analytics collect aggregate statistics of website visitor characteristics, traffic, and activity. This information is used to assess what content is of most and least interest, determine technical design specifications, and identify system performance or problem areas. The software records a variety of data, including IP addresses (the locations of computers or networks on the internet), unique visits, page views, hits, referring websites and what hyperlinks have been clicked. Tier 2 cookies are used to distinguish between summary statistics for users who have been to the site before and those that are visiting the site for the first time. The Department of Defense Education Activity does not gather, request, record, require, collect or track any internet users' personally identifiable information through these processes.

Client side opt-out mechanisms allow the user to opt out of web measurement and customization technologies by changing the settings of a specific application or program on the user’s local computer. For example, users may be able to disable persistent cookies by changing the settings on commonly used web browsers. For general instructions on how to opt out of some of the most commonly used web measurements and customization technologies, go to https://www.usa.gov/optout-instructions.

Use of Third-Party Websites and Applications

Third-party websites and applications that are not owned, operated, or controlled by the Department of Defense Education Activity are integral to internet-based operations across DoDEA and used to augment official communication. These capabilities include, but are not limited to, networking services, media sharing services, wikis and data mashups. A list of DoDEA's authorized pages and uses of these services is available at https://www.dodea.edu/aboutDoDEA/DoDEA-Websites.cfm. These sites may collect personally identifiable information and may make it available to the DoDEA and other users; however, the information is not collected on behalf of, nor is it provided specifically for DoDEA. DoDEA does not harvest and additionally collect, maintain, share or otherwise use such personally identifiable information for any purpose other than that for which it is made available to all users.

DoDEA uses the YouTube API Client to display and present videos on dodea.edu. Please visit the YouTube Terms of Services and Google's Privacy Policy for additional information.