California MSIX User Account Application – Part 1

STEP 1: Applicant Information

- The Applicant completes the Applicant Information and signs the form.
- The Applicant forwards the form to a Verifying Authority (the Regional MSIX User Administrator). This should be the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure (i.e., The MEP Regional Director or an individual appointed to act as the local Verifying Authority). The Applicant must provide appropriate identification (such as state/district identification badge, passport, driver's license, etc.) to verify their identity.

STEP 2: Identification Verification and Attestation

- The Verifying Authority (Regional User Administrator) completes their own information, reviews the entire application for completeness and accuracy, confirms the Applicant's identification, attests to the Applicant's need of an MSIX account, and confirms the right level of access.
- Upon completion, the Verifying Authority forwards the form to the Approving Authority/State User Administrator (i.e., State MEP staff or individuals appointed to act as the state-level authority and create MSIX accounts).

STEP 3: State Authority Approval

- The State Authority reviews the Applicant and Verifying Authority portions of the application for completeness, completes their own information, signs the form, creates an MSIX account for the Applicant, and files the application in a secure location.
- The State Authority notifies the Applicant that their account was created, and that they will receive two emails from the MSIX to finalize setting up their account.

Applicant - Instructions to the Applicant

Applicant Information

- Complete the applicant information below and sign the form.
- Forward the form to a Verifying Authority. This should be your direct supervisor or an individual that is above the direct supervisor in an official reporting structure. Provide appropriate identification information and proof of cyber security training.

First Name		Last Name			
Cyber Security Training Date					
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	*XXX-XXX-XXXX* Ext.		
MEP Region or Direct-Funded District (if applicable)		School District (if applicable)			

Intended Use

Purpose (select one)	☐ Migrant Education Program Participation, School Enrollment, Placement and Secondary Credit Accrual	☐ Other: Please specify

MSIX Account Information

MSIX Role(s)	☐ **Secondary User** ☐ **Regional Data Administrator**	☐ State Regional Administrator ☐ State User Administrator ☐ State Data Administrator ☐ State Batch Submitter

Job Title

Select all that apply	☐ Regional/Local MEP Administrator or Staff ☐ MEP Recruiter	☐ School Registrar ☐ Student Liaison/Advocate ☐ Teacher ☐ School Guidance Counselor	☐ Other: Please specify	☐ State MEP Administrator or Staff

Signature

I certify that this information is accurate and complete to the best of my knowledge. I will only use the MSIX in accordance with the MSIX Rules of Behavior.

Signature: _____ Date: _____

The Privacy Act of 1974 (5 U.S.C. § 552a) Modified 6/01/2021

Privacy Act Statement

The U. S. Department of Education (Department) will use the information that you provide on the attached MSIX User Application Form to promote secure and appropriate access to the Migrant Student Information Exchange (MSIX) system. The Department owns the MSIX system, including the data stored therein, which has a significant value and is an integral part of the infrastructure that supports the Department's mission, goals and critical operations. It is essential that information in the MSIX system is properly secured and protected against information security related threats and dangers. MSIX has incorporated access controls to protect it against inappropriate or undesired user access. The process of granting and controlling access begins with the completion of the MSIX User Application Form, and the granting of rights and privileges. The MSIX User Application Form serves an integral part of the Department's system to identify and verify authorized users for access to MSIX, assign roles to authorized users of MSIX, tie actions taken within MSIX to a specific user, control access to MSIX and ensure authorized users only have access to MSIX that is needed to perform the actions required by their positions, prevent the inappropriate release of information in MSIX, and document that MSIX users understand the MSIX rules of behavior.

The Department requests the information on the attached Form under the authority provided by section 1308(b)(2) of the Elementary and Secondary Education Act (ESEA), as amended by the Every Student Succeeds Act(P.L. 114-95). Your disclosure of information is voluntary, but if you do not submit the requested information, either on this form or, in a State form, if applicable, that requests that you provide the same information, then you will not be granted access to use the MSIX system.

The Department may disclose information contained in a record in this system of records, under the routine uses listed in this system of records, without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. The Department may make these disclosures on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act of 1974, as amended (Privacy Act), under a computer matching agreement. Routine uses of records maintained in the MSIX system include:
(1) MEP Services, School Enrollment, Grade or Course Placement, Accrual of High School Credits, Student Record Match Resolution, and Data Correction Disclosure. The Department may disclose a record in this system of records to authorized representatives of SEAs, LEAs, or other MEP LOAs to facilitate one or more of the following for a student: (a) Participation in the MEP, (b) enrollment in school, (c) grade or course placement, (d) credit accrual, (e) unique student match resolution, and (f) data correction by parents, guardians, and migratory children.
(2) Contract Disclosure. If the Department contracts with an entity for the purposes of performing any function that requires disclosure of records in this system to employees of the contractor, the Department may disclose the records to those employees who have received the appropriate level security clearance from the Department. As part of such a contract, the Department will require the contractor to agree to establish and maintain safeguards to protect the security and confidentiality of the disclosed records.
(3) Research Disclosure. The Department may disclose records from this system to a researcher if an appropriate official of the Department 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 information 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 will be required to agree to establish and maintain safeguards to protect the security and confidentiality of the disclosed records.
(4) 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 concludes that disclosure is desirable or necessary to determine whether particular records are required to be disclosed under the FOIA or the Privacy Act.
(5) 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 operations), 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 in responding to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
(6) Litigation or Alternative Dispute Resolution (ADR) Disclosure.
(a) Introduction. In the event that one of the following parties is involved in litigation or ADR, or has an interest in 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 his or her official capacity.
(iii) Any employee of the Department in his or her individual capacity where DOJ has agreed to or has been requested to provide or arrange for representation of the employee.
(iv) Any employee of the Department in his or her 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 DOJ, or attorneys engaged by DOJ, is relevant and necessary to 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 DOJ.
(c) Adjudicative Disclosure. 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 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 adjudicative body, person, or entity.
(d) Disclosure to 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 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 a party, counsel, representative, or witness.
(7) Congressional Member Disclosure. The Department may disclose information from a record of an individual to a member of Congress and his or her staff in response to an inquiry from the member made at the written request of that individual. The member's right to the information is no greater than the right of the individual who requested it.
(8) 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.

The System of Record Notice was last published in the federal register on 07/10/2019 (84 FR 32895).

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 collection is 1810-0686. Public reporting burden for this collection of information is estimated to average .5 hours per response, including time for data entry by the SEA or LEA MSIX User Administrator to enter the data into the MSIX system. The obligation to respond to this collection is required to obtain or retain benefit under Title I, Part C of ESSA (P.L. 114-95) Sec. 1304(b)(3) and Sec. 1308 (b)(2). No assurance of confidentiality is being provided. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the U.S. Department of Education, 400 Maryland Ave., SW, Washington, DC 20210-4537 or email ICDocketMgr@ed.gov and reference the OMB Control Number 1810-0686. Note: Please do not submit the completed user application to this address.