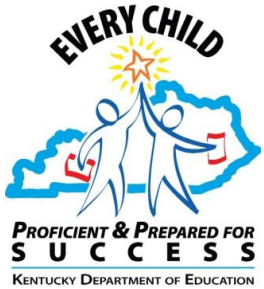
KENTUCKY



Student Records Exchange Policies and Procedures Manual

Kentucky's Policy and Procedures

Christina Benassi

August 2014

ABSTRACT:

In order to be in compliance with the Office of Migrant Education (OME) standards, Kentucky has adopted the *Records Exchange Advice Communication and Technical Support (REACTS) Policy and Procedures Manual*. This manual is designed to assist new Migrant Student Information Exchange (MSIX) users with the direction Kentucky uses for its records exchange. The MSIX user responsibilities are listed in order to help users understand their roles and responsibilities. By following these policies and procedures, Kentucky will have a quality control system.

Table of Contents

Executive Summary **4**
Document Overview **5**
MEP Records Transfer Requirements **6**
Federal Level 6
State Educational Agencies (SEAs) 6
Local Educational Agencies (LEAs) 6
Records Exchange Background 7
Responsibilities of MSIX Users **8**
Rules of Behavior 8
Responsibilities 8
heather.rhorer@education.ky.gov 8
Monitoring 8
MSIX Security Controls 9
User Credentials 9
Protection of MSIX Information 10
Other Security Considerations 11
MSIX Use and Administration **13**
User Manuals 13
Online Help 13
MSIX Help Desk 13
MSIX Roles and Responsibilities 14
Creating MSIX Users 17
MSIX Record Maintenance **19**
SEA Data Upload Schedule 19
Records Transfer Procedures **20**
Records Transfer Collaboration **22**
Minimum Data Elements (MDEs) **23**
MSIX Support Staff **24**
References **26**
Appendices **26**
Acronyms **26**

	Kentucky
	Records Exchange Staff Policies and Procedures

Executive Summary

In order to be in compliance with the Office of Migrant Education (OME) standards, Kentucky has adopted the *Records Exchange Advice Communication and Technical Support (REACTS) Policy and Procedures Manual*. Records Exchange procedures and responsibilities will be discussed in detail. Readers will know their roles and responsibilities with Migrant Student Information Exchange (MSIX). Regional clerks will learn how maintenance is to be done on MIS2000, Kentucky's Migrant database, in order for uploads to occur to MSIX. There are detailed procedures mentioned on how to perform a records exchange when users receive an e-mail alert or work list items. There are references and acronyms to assist readers with records exchange terminology.

Document Overview

The purpose of this document is to provide information about the Migrant Education Program's national implementation of Migrant Student Information Exchange (MSIX) records exchange initiative by providing basic information concerning policy and procedures that are pertinent to Kentucky. By creating a formal document, Kentucky can establish a written and systematic approach to records exchange based on the proper adoption of agreed-upon policies and procedures that would lead to effective execution of inter/intrastate transfer of migrant student records. According to Public Law 107 SEC 1308, the state should develop effective methods for electronic transfer of student records in determining the number of migratory children in each state. In addition, Kentucky can deliver professional, accurate and timely student placement services to a highly mobile student population by following the policies and procedures outlined in this document.

MEP Records Transfer Requirements

Federal Level

The Migrant Education Program (MEP) is authorized under Sections 1301-1309 of Part C of Title I of the Elementary and Secondary Education Act (ESEA), as amended by the No Child Left Behind (NCLB) Act to collect the necessary set of minimum data elements (MDE) to be transferred between state MEPs. The United States Department of Education (USED) developed and maintains the MSIX that State and Local Education Agencies use to transfer records on a national level.

State Educational Agencies (SEAs)

In particular, State Education Agencies (SEAs) are required under Section 1304 (b)(3) and 1308 (b) to promote interstate and intrastate coordination by providing educational continuity through the timely transfer of pertinent school records (including health information) when children move from one school to another, whether or not the move occurs during the regular school year. This responsibility includes carrying out activities that provide for educational continuity through the timely transfer of pertinent school records, including health information, for migratory children, whether or not they move during the regular school year.

For more information, please reference, Title I, Part C Education of Migratory Children Non-Regulatory Guidance.

Local Educational Agencies (LEAs)

In particular, Local Education Agencies (LEAs) are required to use the MSIX consolidated record for the purposes of enrollment, placement and credit accrual as outlined in the SEA's interconnection agreement (IA).

Migrant Student Information Exchange (MSIX)

Records Exchange Background

The timely transfer of education records for migrant children between schools has been a longstanding challenge. Migrant children often enroll in multiple schools for varying amounts of time each year as their families migrate in search of temporary or seasonal work in agriculture or fishing. MEP staffs continue to find it difficult to share and consolidate student information that schools, local educational agencies and states collect on migrant children in a timely and meaningful way that helps school personnel make appropriate decisions when the students arrive. These conditions and those shown below prompted the need for an exchange of student records.

- **High Movement** — highly mobile migrant student population
- **Short Notice** — students move from state-to-state often without notice
- **Lack of Data** — timely and accurate educational information not always available
- **Placement Errors** — students placed in incorrect courses or grades
- **Loss of MEP Services** — students not provided the most beneficial MEP services

In response to this challenge and a Congressional mandate to link the existing migrant student information systems, the USED implemented the Migrant Student Record Exchange Initiative. The goals of this initiative are:

- **Goal 1**: Create an **electronic exchange** for the transfer of migrant student education data among the states.
- **Goal 2**: Promote the **use** of the MSIX application.
- **Goal 3**: Ensure the use of the consolidated migrant student record for the purposes of **enrollment, placement and accrual of credits** of migrant students.
- **Goal 4**: Produce **national data** on the migrant population.

At the heart of this initiative is the Migrant Student Information Exchange (MSIX), an online system containing migrant student records from all participating states to facilitate the national exchange of migrant students' educational information among the states. MSIX is available to state and local Migrant Education Program (MEP) staff along with other users from the MEP community.

The MSIX does not replace existing state migrant student record systems. Rather, it links them in a minimally invasive manner to collect, consolidate and make critical education data available. The MSIX also leverages available information provided by the states to USED's Education Data Exchange Network (EDEN)/EDFACTS system to ease the data collection burden on states. MSIX offers many benefits to promote its usability.

MSIX does the following:

- retrieves and views student information
- contains the minimum data elements necessary for the proper enrollment, grade and course placement and accrual of credits for migrant children
- produces a single "consolidated record" for each migrant child that contains information from each state in which the child was ever enrolled

Responsibilities of MSIX Users

Rules of Behavior

Responsibilities

MSIX is an information system and is to be used for official use only. Users must read, understand and comply with these Rules of Behavior. Failure to comply with the MSIX Rules of Behavior may result in revocation of your MSIX account privileges, job action or criminal prosecution.

MSIX users must complete a basic security awareness training course prior to being granted access to the system. The security topics addressed in this document provide the required security awareness content, so it is important that you read through this entire text. Users also must complete annual security awareness refresher training. MSIX will prompt you to reread the Rules of Behavior annually (or more often due to changes in the system or regulations) to meet this requirement.

Kentucky is set up into four regions with their own Regional User Administrators. These regional administrators can create/modify school- or district-level user accounts and reset passwords. Before MSIX users call or e-mail the State User Administrators, they should first contact their Regional User Administrators.

Northeastern Region	**Southeastern Region**
jackie.roth@fleming.kyschools.us	Michael.Hay@EKU.EDU
bill.thompson@fleming.kyschools.us	Sara.haney@eku.edu
rebecca.white@fleming.kyschools.us	Jeffery.vincent@eku.edu
Laura.puente@fleming.kyschools.us	
Cara.doyle@fleming.kyschools.us	
Central Region	**Western Region**
april.harper@barren.kyschools.us	cindy.sasser@kctcs.edu

MSIX State User Administrator: At the state level, only Christina Benassi, and Heather Rhorer can change your password. Please e-mail them if you are having password issues and if you cannot reach the regional administrators.

christina.benassi@education.ky.gov

heather.rhorer@education.ky.gov

Monitoring

MSIX is a U.S. Department of Education computer system. System usage may be monitored, recorded and subject to audit by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Unauthorized use of this system is prohibited and subject to criminal and civil penalties.

System personnel may provide to law enforcement officials any potential evidence of crime found on USED computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, RECORDING and AUDIT.

MSIX Security Controls

MSIX security controls have been implemented to protect the information processed and stored within the system. MSIX users are an integral part in ensuring the MSIX security controls provide the intended level of protection. It is important to understand these security controls, especially those with which you directly interface. The sections below provide detail on some of those controls and the expectations for MSIX users.

MSIX security controls are designed to:

- ensure only authorized users have access to the system
- ensure users are uniquely identified when using the system
- tie actions taken within the system to a specific user
- ensure users only have access to perform the actions required by their position
- ensure MSIX information is not inappropriately released
- ensure MSIX is available to users when needed

Examples of security controls deployed within MSIX include:

- Automated Session Timeout – Users are automatically logged out of MSIX after 30 minutes of inactivity. This helps ensure unauthorized users do not gain access to the system.
- Role-Based Access Control – User IDs are assigned a specific role within MSIX. This role corresponds to the user's job function and restricts access to certain MSIX capabilities.
- Audit Logging – Actions taken within MSIX are captured in log files to help identify unauthorized access and enforce accountability within the system.
- Incident Response – If a user suspects his/her user ID has been subject to unauthorized use, contact the MSIX help desk immediately.
- Communication Protection – Traffic between a user's Web browser and the MSIX servers is encrypted to protect it during transmission.

The sections below describe several other security controls in place within MSIX. It is important that you understand and comply with these controls to ensure the MSIX security is maintained.

User Credentials

User credentials are the mechanism by which MSIX identifies and verifies users. These are your user ID and password. User IDs uniquely identify each MSIX user and allow the MSIX System Administrators to attribute actions taken within the system to a specific user. This tracking is important in enforcing accountability within the system. Passwords are used by MSIX to verify a user's identity. It is important for you to comply with the following rules governing user credentials:

- Protect your log-on credentials at all times.
- Never share your user ID and/or password with anyone else. You are responsible for all actions taken with your user credentials.
- Your passwords must:
    - be changed upon initial log-in to MSIX
    - contain at least eight characters
    - contain a mix of letters (upper and lower case), numbers and special characters (e.g., #, @)
    - be changed at least every 90 days
    - not repeat your previous six passwords
- Do not write your password down or keep it in an area where it can be easily discovered.
- Avoid using the "remember password" feature.
- User accounts are disabled after three consecutive invalid attempts are made to supply a password.
- User accounts that have been disabled can only be enabled once per day.
- Reinstatement of a disabled user account can only be reinstated by a Help Desk technician or a system administrator.

Protection of MSIX Information

You are required to protect MSIX information in any form. This includes information contained on printed reports, data downloaded onto computers and computer media (e.g., diskettes, tapes, compact discs, thumb drives) or any other format. In order to ensure protection of MSIX information, you should observe the following rules:

- Log out of MSIX if you are going to be away from your computer for longer than 15 minutes.
- Log out of MSIX or lock your computer before you leave it unattended by using the < Ctrl > < Alt > < Delete > key sequence when leaving your seat.
- Media (including reports) containing MSIX information should be removed from your desktops during non-business hours.
- Store media containing MSIX information in a locked container (e.g., desk drawer) during non-business hours.
- Store digital information in an encrypted format where technically possible.
- Media containing MSIX information should be properly cleansed or destroyed.
    - Shred paper media and compact discs prior to disposal.
    - Diskettes and other magnetic media should be cleansed using appropriate software or a magnetic field with sufficient strength so as to make the information unreadable.
        - Note that simply deleting files from magnetic media does not remove the information from the media.
        - Media containing encrypted information can be excluded from the cleansing process, although it is recommended.
- If the access that you have been granted within MSIX is more than required to fulfill your job duties, it should be reported to appropriate personnel.
- Do not disclose MSIX information to any individual without a "need-to-know" for the information in the course of his/her business.

Other Security Considerations

This section describes some additional security items of which you should be aware.

- Incident Response - If you suspect or detect a security violation in MSIX, contact the MSIX Help Desk immediately. For example, if you suspect someone may have used your user ID to log in to MSIX, you should contact the MSIX Help Desk. Other warning signs that MSIX may have been compromised include, but are not limited to: inappropriate images or text on the Web pages, data formats that are not what is expected, missing data or MSIX is not available. While these may not be attributed to a compromise, it is better to have it checked out and be sure than to take no action.
- Shoulder Surfing - Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. An example of shoulder surfing is when a person looks over someone else's shoulder while he/she is entering a password for a system to covertly acquire that password. To protect against this type of attack, slouch over your keyboard slightly when keying in your password to block the view of a possible onlooker.
- Social Engineering - Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. For example, a typical social engineering attack scenario is a hacker posing as an authorized user calling a system help desk posing as that user. The hacker, through trickery, coercion or simply being nice coaxes the help desk technician into providing the log-in credentials for the user he is claiming to be. The hacker then gains unauthorized access to the system using an authorized user's credentials.

  The example above is one example of a social engineering technique. Another is when a hacker calls a user at random and pretends to be a help desk technician. Under the guise of purportedly fixing a problem, the hacker requests the user's log-in credentials. If provided, the user has unwittingly provided system access to an unauthorized person.

  To defeat social engineering, simply question anything that doesn't make sense to you. For example, a help desk technician should never ask a user for his/her log-in credentials to resolve a problem. If you receive a call from someone, and you are not sure who he/she is, ask for a callback number. Hang up and call back to the number provided. Hackers will typically provide a bogus number. Ask questions. If the answers you receive do not make sense, end the call and report the incident to your local security organization.

- Faxing - When faxing MSIX information, call the recipient of the fax and let him/her know it is coming. Ask him/her to go to the fax machine so the item can be pulled off right away so any sensitive information is not left lying around the office.
- Virus Scanning - Scan documents or files downloaded to your computer from the Internet for viruses and other malicious code. Virus scanning software also should be used on e-mail attachments.

FERPA and the Privacy Act

The Family Educational Rights and Privacy Act (FERPA) permits SEAs, LEAs and other local operating agencies to use MSIX to exchange personally identifiable information from

education records on migratory children, without written parental consent, so long as the information is used only for official MEP purposes in accordance with these Rules of Behavior. See U.S. Department of Education *Memorandum to State Directors of Migrant Education* on FERPA and MSIX dated April 2, 2008, available at http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf. In addition, as a system of records under the federal Privacy Act, authorized users may use and disclose information from MSIX only for the "routine uses" published by USED in its MSIX system of records notice, which allows disclosure to facilitate a student's:

1) participation in the MEP
2) enrollment in school
3) grade or course placement
4) credit accrual
5) unique student match resolution

See 72 Fed. Reg. 68572-76 (Dec. 5, 2007). *No other disclosures of a student's name or other personally identifiable information may be made from MSIX without the prior written consent of the parent or student.*

MSIX Use and Administration

Online training modules are available and segmented by user type:

User Type	Online Access
MSIX Government Administrator	https://msix.ed.gov/msix/training/gov/msix_user_training.htm
MSIX Primary User	https://msix.ed.gov/msix/training/gov/msix_user_training.htm
MSIX Secondary User	https://msix.ed.gov/msix/training/secondary/msix_user_training.htm
MSIX State Regional Administrator	https://msix.ed.gov/msix/training/sra/msix_user_training.htm
MSIX Data Administrator	https://msix.ed.gov/msix/training/da/msix_user_training.htm
MSIX User Administrator	https://msix.ed.gov/msix/training/ua/msix_user_training.htm

In the event that Kentucky has a new MSIX user, training will be offered upon request and once a year at the Annual Fall Academy in September. If additional training is required, KDE staff will assist. Prior to receiving an MSIX account, an application and appropriate training above should be administered.

The four regional clerks will be provided training annually at the Fall Academy.

User Manuals

User Manuals are available for the MSIX Application online at the MSIX Trainer's Corner at https://msix.ed.gov/msix/training.html.

Online Help

The MSIX Application provides online help to assist in the primary functions of MSIX.

MSIX Help Desk

The MSIX Help Desk is available for users with issues regarding their accounts such as password resets, updates to personal information and general MSIX information. To receive a password reset, please contact your MSIX State User Administrator or Regional User Administrator. You can find a User Administrator by using the User Administrator Search or by contacting the MSIX Help Desk at MSIXSupport@deloitte.com or (866) 878-9525. To maintain the security of MSIX data, the MSIX Help Desk cannot reset passwords.

MSIX Roles and Responsibilities

MSIX is used by personnel at the district, region, state and national levels. MSIX is used mainly by the front-line educators that need migrant student data to make time-sensitive and appropriate decisions on enrollment, grade or course placement, and accrual of credits. These users are typically the local school registrars and counselors or Migrant Education Program (MEP) specialists.

State MEP users also require access to MSIX; some of these users directly interface with migrant students and others provide administrative and technical support to the MEP. USED personnel are also MSIX users; however, USED requires MSIX for national trend and statistical analysis purposes only.

The table below identifies the specific user roles and responsibilities for MSIX. It includes a description of the user's MSIX job responsibilities, role functions available within the system and the potential kinds of individuals who may perform in each role. A second table follows that provides essentially the same information but in a snapshot, abbreviated form.

Table 1.1: MSIX User Roles and Responsibilities

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
School- and District-Level Roles			
MSIX Primary	MSIX Primary Users can query student records in all states. These users also can initiate the merge and split process for student records in their states.	▪ Search, display and print student records for students in all states ▪ Initiate merge and split of student records ▪ E-mail notification of an arrival or departure of a student ▪ Export Student Records to File	▪ Guidance Counselors ▪ MEP Data Entry Staff ▪ Recruiters ▪ Registrars ▪ Teachers
MSIX Secondary	MSIX Secondary Users can query student records in all states.	▪ Search, display and print student records for students in all states ▪ E-mail notification of an arrival or departure of a student	▪ Guidance Counselors ▪ MEP Data Entry Staff ▪ Recruiters ▪ Registrars ▪ Teachers
District Data Administrator	District Data Administrators can validate or reject near matches, merges and splits of student records. These users also can initiate the merge and split process for student records in their districts.	▪ Search, display and print student records for students in all states ▪ Generate Reports ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ E-mail notification of an arrival or departure of a student ▪ Export Student Records to File	▪ State MEP Administrators ▪ MEP Data Entry Staff
Regional-Level Roles			
Regional Data Administrator	Regional Data Administrators can validate or reject near matches, merges and splits of student records. These users can initiate the merge and split process for student records in their regions. These users also will serve as secondary points of contact for escalation issues.	▪ Search, display and print student records for students in all states ▪ Generate Reports ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ E-mail notification of an arrival or departure of a student ▪ Export Student Records to File	▪ State MEP Administrators ▪ MEP Data Entry Staff
Regional User Administrator	Regional User Administrators establish and manage user accounts for users in their regions.	▪ Create User accounts ▪ Assign User Role(s) ▪ Update User account information ▪ Deactivate User accounts ▪ Reset passwords	▪ State-identified
State-Level Roles			
State Data Administrator	State Data Administrators can validate or reject near matches, merges and splits of student records. These users can initiate the merge and split process for student records in their states. They also can resolve data quality issues and serve as the primary points of contact for escalation issues.	▪ Search, display and print student records for students in all states ▪ Generate Reports ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ E-mail notification of an arrival or departure of a student ▪ Export Student Records to File	▪ State MEP Administrators ▪ MEP Data entry staff
State User Administrator	State User Administrators establish and manage user accounts for users in their state.	▪ Create User accounts ▪ Assign User Role(s) ▪ Update User account information ▪ Deactivate User accounts ▪ Reset passwords	▪ State-identified

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
State Region Administrator	State Region Administrators establish and maintain the regional structure and associated districts for states that choose to use regions.	▪ Enable and disable regional structure ▪ Create new regions ▪ Associate districts to regions ▪ Edit regions	▪ State MEP Administrators ▪ MEP Data entry staff
U.S. Department of Education (USED) User Roles			
Government Administrator	Government Administrators can generate summary level standard and ad hoc queries on a state, regional or national level.	▪ Generate Reports	▪ OME
OME User Administrator	OME User Administrators establish and manage user accounts for all State User Administrators.	▪ Create user accounts ▪ Assign State User Administrator role ▪ Update user account information ▪ Deactivate user accounts ▪ Reset passwords	▪ OME
Privacy Act Administrator	Privacy Act Administrators can enter statements provided by students and parents that formally dispute the data contained in a student's MSIX record. They also can query and view student records from all states in order to comply with the privacy act requirements.	▪ Search, display and print student records ▪ Enter dispute statements into a student's MSIX record	▪ OME

Table 1.2: MSIX User Roles and Responsibilities – A Snapshot View

Function	Primary User	Secondary User	District Data Admin	Regional Data Admin	State Data Admin	State Region Admin	Regional User Admin	State User Admin
My Account	X	X	X	X	X	X	X	X
Search, Display & Print Student Records in all States	X	X	X	X	X			
Export Student Records to File	X		X	X	X			
Generate Reports			X	X	X			
Send Student Move Notices	X	X	X	X	X			
Initiate Student Merges and Splits	X		X	X	X			
Validate / Reject Student Merges and Splits			X	X	X			
Access District Worklist Items			X					
Access Region Worklist Items				X				
Access State Worklist Items					X			
Create / Modify State User Level Accounts								X
Create / Modify Regional Level User Accounts							X	X
Create / Modify School or District Level User Accounts							X	X
Reset Passwords							X	X
Enable Regional Functionality						X		
Create / Modify Regions						X		

Creating MSIX Users

When creating a new MSIX account, you must sign the MSIX user application found on the Kentucky Department of Education's webpage under Migrant Documents and complete appropriate training and include the certificate after the training. The completed application and certificate must then be sent to the Regional Coordinator for approval and copied to Christina Benassi at KDE (christina.benassi@education.ky.gov).

Each Regional Office will have copies of all MSIX user applications and certificates. Since the certificates are a new mandate, anyone signed up for MSIX after September 15, 2012 will be required to complete the training before receiving an account.

In Kentucky, all recruiters and advocates have access to MSIX. Currently, we are working on involving counselors and teachers to get their own MSIX accounts. Anyone that works with migrant students and families could potentially gain access to MSIX if the reasoning is valid and supported. HEP/CAMP personnel are not permitted to own their own MSIX accounts.

MSIX Users
Only staff identified by each MEP User Administrator will have access to MSIX in order to protect student information. Statutory Requirements: In accordance with the Privacy Act of 1974, the Family Educational Rights and Privacy Act (FERPA) and the Federal Information Security Management Act (FISMA).

MSIX Users	
New Accounts	If a new account is needed, an SEA, LEA or LOA user should contact the MSIX State User Administrator to receive instructions on what documentation is needed in order to gain access.
Passwords	Passwords are to be changed at least every 60 days, or they will automatically expire. Password resets can be done by your State User Administrator and Regional User Administrator.
Closing Accounts	State MSIX users that no longer need access must notify the MSIX State User or District Administrator, who will delete the user's account.

MSIX Record Maintenance

SEA Data Upload Schedule

SEA Upload Times	The state MIS2000 server machine uploads to the MSIX on a daily basis at 3 a.m. ET. Any new or changed information that has been uploaded to the state MIS2000 server will be uploaded to MSIX.
Regional Service Center Uploads/MEP Staff Upload Times	The MEP/Regional sites upload manually upon completion of the student's enrollment with the school district, immediately after the student has received his/her class assignments; at the end of every grade reporting period; at the end of every school term; and upon the student's withdrawal from school or from the Migrant Education Program.

Records Transfer Procedures

1. Managing Student move alerts from MSIX e-mails: When a clerk, coordinator or recruiter receives a move alert from MSIX, he/she notifies the correct district of the move in order to sign up the family. Follow-up e-mails or phone calls should be sent to the person notifying the state as a form of courtesy.
2. Work list maintenance such as response and resolution times, delegation of work list items and escalation process.
    - Work list items are to be completed by the clerks, coordinators and KDE staff.
    - Work list items should take no more than two weeks to complete.
3. Staffing Plan: Each of the four regions has its own quality control plan. In 2012, they were mandated to have a back-up for the clerks, and training will be received at the annual Fall Academy in September. In the event that the back-up could not attend the training, it is the responsibility of the clerks to train their back-ups.

Regions	**Clerk Back Up**	**Regional Quality Control Process**	**Number of people that look at a COE before it is signed**
Western Region	The Regional Coordinator	The clerk looks over the COEs, makes note of any questions and passes them along to the coordinator.	Two – Clerk and Coordinator
Southeastern Region	Regional Recruiters	Two regional recruiters review the COEs, or a regional recruiter and assistant director review the COEs. Then the COE is given to the clerk for a final review and finally to the regional director for final review and signature.	Four – Regional Recruiter/ Assistant Director/ Clerk/ Regional Director
Central Region	The Regional Coordinator	The clerk receives the COE and flags it if there are any questions for the coordinator. The coordinator then reviews and signs the COE.	Two – Clerk and Coordinator

Northeastern Region	Regional Recruiter and Coordinator	The coordinator reviews the COE, and then the clerk reviews. If it is a questionable COE, then at least 2-3 others will review the COE.	Two – Clerk and Coordinator

Records Transfer Collaboration

Records Transfer Inter/Intrastate Collaboration	
Kentucky creates several collaboration opportunities within MEPs and respective school districts and with school staff that serve migrant students. Specifically, SEAs and LOAs will develop operational systems that seek to develop and support collaboration with other states on the exchange of migrant student data. For example, MEP staff should consider querying MSIX data their daily responsibility and to move away from seeing it as an "add-on" task. By querying student data in a timely and systemic manner, personnel beyond the SEA will be knowledgeable about records transfer, and ensure the continuity of services for children who migrate from one state or school district to another. Statutory Requirements: Title I, Part C, Sections 1304 (b)(1)(B) and (C); 1304 (b)(3); 1304(c)(1)(B); 1306(a)(1)(A), (F), and (G); 1308(a), (b) and (d); Section 3124 of Title II, Part A.	
Alerting student moves via MSIX e-mails	If a local operating MEP is aware of a migrant student relocating, the program should designate a MSIX user to send the receiving state/LOA an e-mail notification via MSIX. Additionally, the sending user will notify the receiving state/LOA, when possible, of the child's move. The MSIX e-mail to the receiving state/LOA should provide as much information as possible to ensure that the proper family and student(s) are efficiently and effectively assisted. Staff must be cautious to not enter social security numbers (SSNs) or other personal identifiable information (PII) in their e-mail message. When sending move alerts from Kentucky, be considerate of other states' guidelines when transmitting move alerts. The MSIX identification number and name will automatically be generated. You may want to include your name and number for the correspondent to notify you for further questions.
E-mails on student moves E-mail notification	When an MSIX user receives notification from a state/LOA that worklist items need to be addressed in MSIX, initial contact such as a simple reply to the sender of the MSIX e-mail should be done within a 24-hour period, when possible. All items should be resolved within five business days, and when possible, no later than two weeks.

Minimum Data Elements (MDEs)

Minimum Data Elements	
Minimum Data Elements (MDEs) are data fields that Kentucky must collect and maintain in our migrant student databases, MIS2000, in order to transfer that data to other states via MSIX. The MDEs are transmitted on an agreed schedule from MIS2000 to MSIX. Most states transmit the MDE nightly on any new migrant student or for students whose information has changed since it was originally transmitted to MSIX. Kentucky's submissions are daily at 3 a.m. ET. The MDE will enable SEAs to exchange a minimum set of data elements that have been identified as necessary for fulfilling the requirements of the MEP for continuity of instruction.	
Recruiter responsibility	It is the responsibility of the MEP recruiter to collect the initial information on the migrant family. Once the information is collected on the certificate of eligibility (COE), the MSIX data administrator and the Regional Clerks will ensure the data are electronically uploaded to MSIX.
Initial enrollment	It is the responsibility of the MEP recruiter to initially enroll the migrant family. Once all the applicable information is collected, it should be transmitted to MSIX within 10 days of the date the child is initially identified as eligible for the MEP. It is understood that in some rare situations that may not occur.
School or program update	It is the responsibility of the MEP specialist, the regional coordinator and regional clerk to update school or program records. Once all the applicable information is collected, it should be transmitted to MSIX within 30 days after the end of a school or program term.
Interstate child update	It is the responsibility of the MEP specialist to update the child's MSIX record within four days of a MSIX request for data based on a child's interstate move.

MSIX Support Staff

Job Responsibilities	State MSIX Lead	Technical Lead	User Administrator	Data Administrator	ID&R Coordinator	MEP Specialist
Coordinate the development and implementation of MSIX training and information.	X					
Create user accounts and resets passwords.			X			
Attend meetings hosted by OME.	X					
Work with the MSIX Contractor to address technology concerns and keep up to date on statewide database system issues.		X				
Develop policies and procedures on "how to" implement records transfer within the state.	X					
Work closely with I&R staff at SEA and LOA on implementing records exchange.	X					
Manage and support worklist items.				X		
Create MSIX user reports.			X			
Develop strategies to collaborate as inter/intrastate users.	X					
Work with end users, parents and students to promote MSIX as a viable tool for records exchange.	X					
Work closely with the MSIX State Lead to implement MSIX.						X
Coordinate the I&R of MEP staff on how to implement records transfer procedures and best practices.					X	

Job Responsibilities	State MSIX Lead	Technical Lead	User Administrator	Data Administrator	ID&R Coordinator	MEP Specialist
Provide I&R training for current/enrolled students and appropriately updating MSIX information in a timely manner.					X	
Train staff on using and becoming knowledgeable MSIX users, including how to work with incoming/outgoing MSIX e-mail notifications.	X					
Develop procedures for staff to prioritize MSIX responsibilities.	X					
Initiate the I&R of new/current MEP students and then upload their information to MSIX in a timely manner.					X	
Focus on the "re-signature" (e.g., re-interviewing) process for current/enrolled students by using MSIX data to facilitate the processing of information.					X	
Establish MSIX as a valuable recruitment and placement tool by keeping student information current.					X	

References

Title I, Part C - Education of Migratory Children, Section 1304(b)(3) (URL)
Title I, Part C - Education of Migratory Children, Section 1308 (b) (URL)
MSIX Rules of Behavior

Appendices

MSIX User Administrator Guide for Managing User Accounts (scroll down to appropriate section)
User Application for Access to MSIX (scrolled down to User Access Form)

Acronyms

Term	Definition
I&R	Identification and Recruitment
KDE	Kentucky Department of Education
LEA	Local Education Agency
LOA	Local Operating Agency
MDE	Minimum Data Elements
MEP	Migrant Education Program
MSIX	Migrant Student Information Exchange
PII	Personal Identifiable Information
REACTS	Records Exchange Advice, Communication and Technical Support
REI	Records Exchange Initiative
SEA	State Education Agency
SSN	Social Security Number
USED	U.S. Department of Education