NEW YORK STATE
MIGRANT EDUCATION PROGRAM

Confidential Information Security Policy

New York State Migrant Education Program
Office of Identification & Recruitment

Summary

The purpose of this document is to establish the policies and procedures that NYS Migrant Education staff must follow in order to protect confidential information and ensure the appropriate handling of personal data protected by FERPA and the Privacy Act. The objectives of this policy are:

- Protect and safeguard the data of Migrant families and their children;
- Prevent improper disclosure of NYS Migrant Education Program data;
- Establish procedures for proper handle and disposal of sensitive information.

Preface

Our migrant families and students trust us with a large amount of their confidential information. It is our responsibility to them to keep that information safe, especially in an increasingly digital world. This document contains an explanation of certain types of confidential data, information on federal laws that control how we must treat confidential data, an introduction of documents and information systems that will use that confidential data, and the policies and procedures designed by the New York State Migrant Education Program to aid in securing that data. These policies and procedures are not intended to replace any that already exist at your current workplace, but rather to enhance them. Data security is a constantly developing field, and so this document is subject to change.

What is Personally Identifiable Information (PII)?

The U.S. Government Accountability Office defines Personally Identifiable Information as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[1] Examples of relevant Personally Identifiable Information include, *but are not limited to*:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, or driver's license number
- Address information, such as street address or email address
- Telephone numbers, including mobile, business, and personal phone numbers
- Information about an individual that can be linked to one of the above, including date of birth, place of birth, race, employment information, educational information, etc.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) of 1974 is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

[1] GOA Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008, http://www.gao.gov/new.items/d08536.pdf

- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest
    - Other schools to which a student is transferring
    - Specified officials for audit or evaluation purposes
    - Appropriate parties in connection with financial aid to a student
    - Organizations conducting certain studies for or on behalf of the school
    - Accrediting organizations
    - To comply with a judicial order or lawfully issued subpoena
    - Appropriate officials in cases of health and safety emergencies
    - State and local authorities, within a juvenile justice system, pursuant to specific State law

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information, you may call 1-800-USA-LEARN (1-800-872-5327) (voice). Individuals who use TDD may use the Federal Relay Service.

Or you may contact us at the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-8520

The National Certificate of Eligibility

In New York State, we are required to document every migrant child’s eligibility for the Migrant Education Program on the National Certificate of Eligibility (COE) created by the U.S. Department of Education (ED). The COE provide access to the Migrant Educational Programs (MEP) staff to obtain additional information regarding child protected information. If the parent choose to consent and signed the COE he/she is authorizing the school district and the State Educational Agency to: release, transfer, and/or receive the child’s education and health records, including immunizations, records, current enrollment information, report card/transcripts and standardized test results, to/from other school districts, educational agencies, and other pertinent agencies.
It is very important to keep in mind that the COE is a federal document that needs to handle carefully. The information included on the COE is private and needs to be protected. While some families grant rights to access private information, staff from the New York Migrant Education Program should only access the necessary data to perform their duties. The information obtained should only be used for official purposes related to providing services.

The Migrant Student Information Exchange MSIX

The Migrant Student Information Exchange (MSIX) allows states to share demographic and educational information on migrant children who travel from State to State to facilitate a student's 1) participation in the MEP; 2) enrollment in school; 3) grade or course placement; 4) credit accrual; and 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 is an information system and is to be used for official use only. MSIX has created its own rules of behavior (for more information see https://msix.ed.gov/msix/formattedROB.html). Failure to comply with the MSIX Rules of Behavior may result in revocation of your MSIX account privileges, job action, or criminal prosecution.

Rules of Behavior

Protocols and responsibilities to protect sensitive information:

All information stated on the Certification of Eligibility (COE), MIS2000, MSIX, and other Migrant Education related information (farm names, addresses, and family records) are to be used for official use of Migrant Programs only (see below). Employees must read, understand, and comply with these Rules of Behavior. Failure to comply with the Rules of Behavior may result in corrective action, revocation of your job and/or criminal prosecution.

The following Rules of Behavior and security practices are designed to:

- Ensure only authorized employees have access to private information
- Tie actions taken to a specific user
- Ensure only employees have access to the information required by their position
- Ensure NYS Migrant Education information is not released without consent

User Credentials:

It is expected that all staff working with the NYS Migrant Education Program that possess and/or have access to data regarding migrant families have protected username and passphrase to login into their device(s). (e.g. MSIX accounts, ECOE tablets, computers, etc.) However, it is also important for you to comply with the following rules governing user credentials:

- Protect your logon credentials at all times.
- Never share your user id and/or passphrase with anyone else. You are responsible for all actions taken with your user credentials.
- Staff should create strong passphrases, in accordance with authentication guidelines. (e.g. a minimum of at least 8 characters, alphanumeric, special character). Likewise, we expect staff to change passphrases at periodic intervals.
- Multi factor authentication should be used with accounts wherever it is available.

User Accounts:

All accounts used to access NYS Migrant Education Program data or student information must be under the direct administration of their governing institution. In this context, administration is defined as the ability for the governing institution to monitor actions performed by these accounts, to audit communications sent and received by these accounts, and to regulate access controls to these accounts. The governing institution must be able to suspend access to these accounts on demand without participation by the end user. This requirement extends to all email accounts used to transmit student data or communicate as a representative of the NYSMEP for any official purpose.

Personal email accounts, such as free email services like Gmail and Yahoo, are not permitted for use in this setting as the governing institution has no administrative control over these accounts. The free office suites bundled with these types of accounts may not be used to store, edit, or share any data on behalf of the NYSMEP. Similarly, email accounts provided by outside school districts or other employers may not be used by employees of the NYSMEP for any purposes relating to their work with the program.

Permissible accounts deemed to be under the direct administration of a governing institution are the accounts managed either directly by the NYSMEP, a sponsoring institution of a NYSMEP program, or a vendor directly contracted by the NYSMEP. For example, if a program operates as a sponsored program by a college, university, or school district, then the accounts provided by that college, university, or school district are permissible for use by the program. Program directors should familiarize themselves with the process of account creation and suspension at their sponsoring institution. Any accounts hosted by these institutions should be made accessible to employees at the beginning of their employment and access to them should be terminated immediately upon the conclusion of their employment. At no point during the span of their employment should an employee be asked to use a personal email account, social media account, or other account outside of the direct administration of the governing institution for any official purposes.

Accounts provided by the NYSMEP to its employees should utilize robust security protocols such as multi factor authentication to access the accounts.

If at any point a user account is suspected of being compromised, immediate action must be taken by the governing institution to suspend the account to prevent any potential data breach. These actions should include disabling the user account until the passphrase used for the account has been reset and only the legitimate end user of the account has been authenticated.

Protection of NYS Migrant Education Information:

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

- Certificates of Eligibility, Student School Records, Health Records, Farm Directories, Housing Directories and any other documents containing sensitive Personally Identifiable Information (PII) should be keep in a safe location with access only the MEP staff.
- Filing cabinets containing information about migrant students and their families should be locked during non-business hours.
- Records from previous years should be maintained in locked containers for a period of time stated by federal legal requirements, and then be properly destroyed.
- Only use accounts provided by your governing institution for the storage and communication of any work related content.
- Lock your computer before you leave it unattended by pressing the < Windows > + < L > keys on your keyboard when leaving your seat.
- Media (including reports) and forms (e.g. COE) containing information about migrant students and their families should be removed from your workplaces (desktops, cars, etc.) during non-business hours.
- Store materials containing students' 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 migrant families' information should be properly cleansed or destroyed:
  - Shred paper media and compact discs prior to disposal.
  - Hard drives and other magnetic media should be erased using appropriate software that will overwrite the data three times so as to make the information unreadable.
  - Note that simply deleting files from magnetic media does not remove the information from the media.
  - Do not disclose private information to any individual without informing your immediate supervisor.

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 with NY Migrant Education data, contact your immediate supervisor and the ID & R/MIS2000 Director immediately. For example, if you suspect someone may have used your user id to log in to MSIX, you should contact the ID & R/MIS2000 Director to reset your passphrase.
- Other warning signs that migrant students' data may have been compromised on your personal and/or work computer include, but are not limited to: inappropriate images or text on the web pages, data formats that are not what is expected, and/or missing data. 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 they are entering a passphrase for a system to covertly

acquire that passphrase. To protect against this type of attack, slouch over your keyboard slightly when keying in your passphrase to block the view of a possible onlooker.

- **Social Engineering** - Social engineering is a term for ways used to trick people into telling confidential information. An example is a surprise phone call from someone claiming to be Microsoft, saying that that've found something wrong with your copy of Office. They may suggest that you should give them your passphrases or let them take control of your computer to fix it. You should never give your information out to anybody for any reason, no matter how real they may sound over the phone. You should always question anything that doesn't sound right to you. A good idea is to ask for a callback number, then hand up and call that number. Often, someone trying to steal your information will give you a fake telephone number. Always report any suspicious behavior like this to your supervisor immediately.
- **Virus Scanning** - Scan documents or files downloaded to your computer from the Internet for viruses and other malicious code. Virus scanning software should also be used on email attachments.
- **Faxing** - When faxing information, call the recipient of the fax and let them know it is coming. Ask them to go to the fax machine so they can pull it off right away so any sensitive information is not left lying around the office. Append the message at the bottom of this page to the cover page of the fax.
- **Emails** -If a METS is aware of a migrant student relocating, the program should designate a Data Specialist to send the receiving State/LOA/Regional Office an email notification via MSIX. The staff should be cautious to not enter personally identifiable information (PII) in their email message.
- When sending an email, avoid utilizing private information (e.g. student name and/or DOB) in the body of the email, and instead use a Unique ID number such as an MIS2000 ID number or MSIX ID number.
- If personally identifiable information (PII) must be communicated through email, it should be sent as a passphrase-protected attachment and encrypted using appropriate software. Never include the passphrase in the email. The passphrase to the file must be communicated to the intended recipient by means outside of email.
- All electronic confidential documents (email, fax) maintained by the MEP shall be safeguarded against possible misuse by adding the following paragraph at the end of the message as follow:

"This electronic message or fax is intended to be for the use only of the named recipient, and may contain information from the Migrant Education Program that is confidential or privileged, or protected FERPA. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately, either by contacting the sender at the electronic mail address noted above or calling (your program) at (your telephone number), and delete and destroy all copies of this message. Thank you"

Breaches of Information:

This section provides the steps that NYS Migrant Education employees are obliged to follow if they suspect or are witnesses of the following behavior: misuse of information, providing information to unauthorized individuals/organizations, other criminal activities or activities that compromise the safety of migrant students' information.

Step 1: Contain the breach

If possible, staff should try to take any available step to contain the breach. Disconnect the device from the internet by pulling the network cable out or turning off Wi-Fi. Do not power off the device unless absolutely necessary. Take note of everything that happened immediately before the event, and keep the device securely in your possession.

Step 2: Contact immediate supervisor

Move quickly to let your supervisor know about the possible breach.

Step 3: Contact the ID&R / MIS2000 Director

It is vital that you provide information to the Director since he/she has the authority and ability to perform measures to contain/mitigate the breach and take action to protect all the NYS Migrant data.

Step 4: Document the breach

In many occasions, the ID&R / MIS2000 Director might request that you participate in a detailed evaluation of the events leading to the breach for official records, prevention, and other uses.

For any concerns related to this Policy or to request access to MSIX;
Contact Will Messier, Director of ID&R / MIS2000 / MSIX at 518-289-5618
wilfred.messier@oneonta.edu

Secure Equipment Tracking and Disposal:

Equipment purchased with New York State Migrant Education Program funds must be physically tagged in such a way that it cannot be easily mistaken for a personal possession. When an item on inventory has outlived its expected useful lifespan or is damaged beyond repair, it will be marked for disposal. It is important that any migrant data is irrecoverably removed from storage media before disposal. Deleting files from computers alone is insufficient, as these files can still be recovered with readily available software. The storage media must instead be subject to a data sanitization process. For magnetic hard disk drives, a DoD 5220.22-M compliant, three-pass overwrite procedure will be employed on the disk. For solid state drives, reset procedures will be employed as appropriate for the specific technology used and may vary by device. Computers that are eligible for reuse through the New York State CREATE program will be made available to the program after the data sanitization process is complete, in accordance with the disposal policies of the New York State Education Department (NYSED) and SUNY Oneonta.

NEW YORK STATE
MIGRANT EDUCATION PROGRAM

General Data Security Policy & Procedures Reference Sheet

- Work areas should have a lockable drawer, cabinet, or container where sensitive physical documents should be kept when left unattended. No documents should be left in vehicles.

- Workstation computers should be secured with a strong passphrase known only to the operator. The drives of these computers should be fully encrypted with appropriate encryption software, such as BitLocker or File Vault.

- Only user accounts under the administration of the program or a sponsoring institution can be used to access NYSMEP data. These accounts should be secured with a strong passphrase and two factor authentication when available.

- Workstation computers should be locked using < Windows > + < L > or powered off when left unattended.

- Magnetic media, such as computer hard drives, containing Personally Identifiable Information (PII) should be properly erased with software that will overwrite the information three times before being disposed of. Flash media should be erased according to manufacturer specifications.

- Workstation computers should have antivirus software installed. Any attachments downloaded from the internet or email should be scanned with this antivirus software for malicious code prior to opening them.

- When sending emails regarding migrant families or individuals, only use a unique identifier, such as those assigned by MSIX or MIS2000, to refer to them. Do not include any other forms of Personally Identifiable Information (PII), such as their first name, in the body of your email.

- If Personally Identifiable Information (PII) needs to be sent over email, it should be sent as a passphrase-protected attachment using the tools available in the Microsoft Office suite of applications, or by using a zipping tool such as 7-zip. This passphrase should NEVER be included in the email, and should instead be sent to the recipient through alternative means, such as a phone call.

- If it is suspected that a workstation computer has been compromised, or there is a threat that Personally Identifiable Information (PII) may have been stolen from the workstation computer, then the workstation computer should be immediately disconnected from the internet through appropriate means. The supervisor should be immediately notified, and the workstation computer should remain powered on if possible while disconnected from the internet.

- Any suspicious attempts to request Personally Identifiable Information (PII) by unauthorized parties should be reported to the supervisor.