Administrative Procedure

Mission Public Schools

Section:	**District Administration**	
Title:	**Safeguarding Personal and Confidential Information**	**2.4.2**

Purpose

Public bodies must keep paper and electronic records safe and secure as required by the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Information Protection Act (PIPA). A privacy breach occurs when there is unauthorized access to our collection, use, disclosure, or disposal of personal information. The most common privacy breach happens when the personal information of students, their parents, outside agencies, or employees is stolen, lost, or mistakenly disclosed. For example, when a computer is stolen, personal information is mistakenly emailed to the wrong person, or a USB flash drive is lost.

General Guidelines:

This procedure is for all staff interacting with and storing confidential, personal, and sensitive information about a student, parent, employee, volunteer, trustee, or other person interacting with the School District. Thoughtful steps are necessary to ensure personal information is secure. Personal information refers to recorded information about an identifiable individual.

Procedure:

To protect confidential information, general records kept by employees which are deemed necessary personal or confidential, or related to ongoing student safety and programming, employees will:

1. Respect information given confidentially from students, parents, and colleagues.
2. Ensure others are not able to overhear a conversation when personal information is being discussed, such as a student’s program or support needs.
3. Share only necessary information with the staff who need the information to do their work with the student, employee, parent, or other person.
4. Ensure staff that when you provide personal information regarding another person, the information either returns to you, or is deleted, and/or shredded by the other person.
5. Ensure that student G4 files, employee files, or other files containing personal information, remain locked at all times, and have restricted or controlled access.

Your Desk at Work:

1. Do not leave personal information related to a student, employee or another individual visible on your computer or in any printed format so that others can see.
2. Lock the screen, log off or shut down your computer when not using it.
3. Use strong passwords and encryption.
4. Store any records, files, or paper information in a locked file cabinet, or locked desk drawer when not in use. Do not leave documents on your desk overnight.
5. On the “Subject” line of emails, do not put the name of the student/parent/employee in case this is seen by an unauthorized person. Instead, use initials in the “Subject” line and refer to the full name in the body of the email.
6. Sending emails or documents electronically that contain personal information should be encrypted, with the password to access the personal information sent in a separate email.

When Transporting files:

1. Employee files and records, or student G4 files, should only be transported out of a building as part of a formal file transfer process.

2. Individuals should never take a file out of a building to work on in another location, without the expressed permission of the principal or manager. If necessary, make copies of specific information needed only. When you return to work, destroy any copies securely.
3. Ensure your laptop and/or your encrypted USB flash drives are locked in the trunk of a vehicle before transporting. Ensure you travel directly from work to home/school and secure devices before going elsewhere. The laptop should never be left unattended in a vehicle, even in the trunk.
4. If storing information at home or school, ensure it is in a locked filing cabinet or desk drawer. Ensure the room or building is also locked.
5. When working in locations outside of your office, paper and electronic records need to be kept under the constant control of the employee, including during meals, and other breaks. If this is not possible, then the records need to be temporarily stored in a secure location, such as a locked room or desk drawer.

Your Desk at Home:

1. Use the same precautions as listed in the “Desk at Work” section.
2. In addition, ensure you do not use your personal email to transfer records containing personal information for work purposes.
3. Ensure you are working from a secure internet access point when working from home or another location (e.g. Starbucks), or while working on personal or confidential information.
4. Avoid viewing personal information collected and used for work while in public or where unauthorized people can see it. Use a privacy screen if you are working in such an environment.
5. Do not share a laptop containing personal information with other individuals, including family members and friends.
6. Ensure all paper information is stored in a locked file cabinet or drawer at home.

Your Online Storage:

1. Follow all MPSD policies and procedures for ensuring personal information is stored securely using a district-approved computer application. Whenever possible, personal information should be stored on District network drives only. Files that must be stored on a laptop or in another location must be encrypted with a password to protect access to personal information should the device be lost or stolen.
2. Use only district-approved Apps, services, and software to ensure personal information is not improperly collected, used, or disclosed, including improper collection, unauthorized use, and unauthorized disclosure.

Privacy Breach:

If a breach of privacy occurs, or items are lost or stolen that may contain personal or confidential information, notify your Principal, Supervisor, Director, or Manager immediately. The Principal, Supervisor, Director, or Manager will report the incident to the District Privacy Officer, using the Privacy Breach Procedure.

Date Approved: March 2022
Legal Reference: *Access to Information and Protection of Privacy Act*

Cross Reference: *Access to Information and Protection of Privacy and Personal Information Policy*
Privacy Management Program (includes procedures 2.4.1 to 2.4.7)
Computer Network Procedure
Network, Internet, and Wi-Fi Procedure for Students
Network, Internet, and Wi-Fi Procedure for Employees