Board Policy XX: DRAFT - Data Classification Policy and Protection Guidelines
Adopted:
Approved:

Making Waves Academy Data Classification Policy and Protection Guidelines

Purpose

The purpose of the Making Waves Academy ("MWA") Data Classification Policy and Protection Guidelines is to establish a framework for generally classifying organizational and educational data based on its level of sensitivity, value, and criticality to MWA. The classification of data will aid in determining baseline security measures and is designed to work in conjunction with related MWA policies and procedures and to ensure only authorized disclosure of confidential and otherwise protected information. Additionally, these guidelines define (1) the requirements for handling and protecting information at each stage of its lifecycle from creation to destruction and (2) the minimum security standards required for any electronic device that may be used to access or store Sensitive or Protected Data owned or used by MWA staff. Generally, Public Data does not require any level of protection from disclosure, but appropriate precautions should be taken to protect original (source) documents from unauthorized modification.

Policy Statement

It is the policy of MWA to comply with state and federal laws regarding the classification, maintenance and use of organizational and educational data, including but not limited to the Family Educational Rights And Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99), and Education Code Sections 49073.1 and 60607(c)(1). Accordingly, MWA has implemented additional policies and procedures related to data classification that may be applicable and otherwise supersede this policy. MWA's related policies include:

- Educational Records and Student Information Policy
- Employee Policies and Procedures Handbook
- Fiscal Policies and Procedures
- Digital Programs and Digital Privacy Policy
- Student Technology and Internet Safety Policy
- Document Retention and Destruction Policy
- Other policies: ________________________

Scope

The Data Classification Policy and Protection Guidelines are applicable to all MWA employees and will be reviewed on an annual basis or more frequently, as needed.

Data Classification

MWA classifies data as **Protected**, **Sensitive**, or **Public** data with corresponding policies and procedures for appropriately protecting such data. The Managing Director of Information Technology will make all final determinations on data classifications.

A. Protected Data
Protected Data is information that is protected by statutes, regulations, MWA policies and procedures or other contractual language. An example of Protected Data includes but is not limited to student educational records. This data shall not be disclosed to unauthorized individuals, agencies or external sources except as specifically authorized by law.

B. Sensitive Data
Sensitive Data is highly confidential or personal information which, if breached or disclosed to unauthorized persons, could result in legal liability, fines, penalties, theft and/or fraud. An example of Sensitive Data includes but is not limited to MWA financial and network data, which is information that, in the normal course of MWA operations, is generated by computer systems, voice systems, and network devices and includes but is not limited to login data, source and destination internet protocol (IP) addresses, session times, and file information. This information may be obtained, stored, and reported for legitimate business, compliance and audit purposes but shall not be disclosed to unauthorized individuals except as authorized by law and/or applicable MWA policy.

C. Public Data
Public Data is information that may be disclosed to any person regardless of their affiliation with MWA. The classification is not limited to data that is of public interest or intended to be distributed to the public, but also applies to data that does not require any level of protection from disclosure. Public Data and other low risk data may be shared with a broad audience both within and outside of the MWA community and no steps need be taken to prevent its distribution. Examples of Public Data include press releases, school announcements, directory information, and other data typically distributed on the MWA website.

Data Protection Measures

MWA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, MWA shall follow industry best practices as outlined in the MWA Making Waves Academy Data Classification Policy and Protection Guidelines. Additionally, MWA shall follow best practices for notifying affected parties, including students and/or parents and guardians. Concerns about security breaches must be reported immediately to the Managing Director of Information Technology who will collaborate with the MWA Leadership Team to determine whether a security breach has occurred. If MWA determines that one or more employees, volunteers, or vendors have substantially failed to comply with MWA's data-related policies and procedures, MWA will identify appropriate consequences, which may include termination of employment or contract and further legal action. Concerns about security breaches that involve the Managing Director of Information Technology must be reported immediately to the MWA Chief Executive Officer. MWA will provide and periodically update, in keeping with industry best practices, resources for students, families, staff, and volunteers in preparing for and responding to a security breach. MWA will make these resources available on its website.

Additionally, as additional data security, MWA employees will:

- Complete a data confidentiality and security training.
- Consult with MWA data owners when creating or disseminating reports containing data.
- Use password-protected and school-authorized computers when accessing any student or personnel records.
- Refrain from sharing individual passwords for school computers or data systems.
- Log out of any data system and portal and close internet browsers after each use.
- Store sensitive data in appropriately secured locations. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally-owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
- Keep printed reports with personally identifiable information in a locked location while unattended and use the secure document destruction service provided at MWA when disposing of such records.
- Refrain from sharing personally identifiable data during public presentations, webinars, etc. If users need to demonstrate student/staff level data, demo records should be used for such presentations.
- Redact any personally identifiable information when sharing sample reports with general audiences.
- Delete files containing sensitive data after use on computers or move them to secured servers or personal folders accessible only by authorized parties.
- Refrain from using email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of any data the Managing Director of Information Technology should be consulted.
- Use secure methods when sharing or transmitting sensitive data. The approved method is sharing within secured server folders for internal file transfer.
- Refrain from transmitting student/staff-level data externally unless expressly authorized in writing by the data owner and only via approved methods.
- Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Data Retention and Destruction

MWA shall retain and dispose of records, including pupil records, in accordance with the MWA Document Retention and Destruction Policy.

Conflicts with Other Laws or Regulations

To the extent that any part of this policy may be construed to conflict with applicable state or federal laws and regulations, the applicable laws and regulations shall control.

Requirements for Protection

Each classification of data has different requirements for protection throughout the lifecycle of use. The requirements for each Protected Data and Sensitive Data are detailed below.

Public Data	**All Uses**	Public Data and other low risk data may be shared with a broad audience both within and outside of the MWA community and no steps need be taken to prevent its distribution. Examples of Public Data include press releases, school announcements, directory information, and other data typically distributed on the MWA website.
Protected Data & Sensitive Data	**Collecting Data**	Reduce or eliminate collection where not required for school-related or other business function. Collection of some types of Protected/Sensitive Data may require the approval of the appropriate School Administrator.
	Accessing Data	Access to some Protected/Sensitive Data (e.g. FERPA-related data) requires approval of the appropriate School Administrator. Devices used to access Protected/Sensitive Data must meet MWA's minimum security standards. School Administrators must also ensure that appropriate protocols are in place to immediately remove access to Protected/Sensitive Data Data upon change in employment status of any individual with access.
	Sharing Data	If you are uncertain if Protected/Sensitive Data should be shared, the request should be escalated to the appropriate School Administrator. As in the case of collecting Protected/Sensitive Data, such information should only be shared if required for school-related or other business functions. Protected/Sensitive Data and information may be shared internally without School Administrator approval if the recipient of the data has a need-to-know basis and is entrusted with the same type of information for their job function. Note: Non-disclosure language or a confidentiality agreement may be appropriate. For example: ● MWA teachers may consult with other teachers about a student's performance, as appropriate. ● Sharing information with vendors and third parties requires the approval of the appropriate School Administrator.
	Printing, Copying & Scanning Data	Printers often store the printed document on a local hard drive, potentially allowing unauthorized access to the information. Avoid printing Protected/Sensitive Data unnecessarily and from common use or public printers.
	Sending Data	**Via Paper or Hard Copy:** Address to the specific intended party and send in sealed security envelopes. Mark with "For intended recipient only". If sending outside MWA, paper or hard copies should only be sent via certified mail or with an authorized courier.

		Via Electronic Transmission: Particularly sensitive data or large volumes of Protected/Sensitive Data should be encrypted during transmission. It is required that MWA employees use MWA's secure email and appropriate device. If Protected/Sensitive Data is to be stored on removable media (CD/DVD/USB/External HD) or in the cloud, please see the section below regarding the proper storage.
		Via Facsimile: Facsimile (fax) machines often store faxed messages in memory, potentially allowing unauthorized access. Facsimile of Protected/Sensitive Data is strictly prohibited.
		Via Smart Phone and Tablet Devices (e.g., iPads): The use of smart phones to access Protected/Sensitive Data, such as through email, puts that data at higher risk of unintended disclosure. Individuals accessing Protected/Sensitive Data via such a device must ensure that the devices comply with MWA's minimum security standards.
	Storing Data	**Paper or Hard Copy:** Keep in locked filing cabinets in physically secure areas that are accessible only by authorized individuals. Keep the number of copies of the data to a minimum.
		Electronic: Encryption of stored data is recommended. Devices used to store Protected/Sensitive Data must meet MWA's minimum security standards. Cloud services may be used if they have been approved for this purpose by the appropriate School Administrator.
		Electronic Media (CD, DVD, USB, Etc.: Encryption of stored Protected/Sensitive Data is required. Store media in a secure location when not in use. Media should be erased or destroyed as soon as it is no longer needed.
	Auditing	Each school and/or organization department should conduct periodic reviews of where Protected/Sensitive Data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols. Verify that procedures for removing access are documented and accurate.
	Incident Reporting	Any unauthorized disclosure or loss of Protected/Sensitive Data must be reported to the appropriate School Administrator. The School Administrator(s) should report significant unauthorized disclosures or losses of Protected/Sensitive Data to the Executive Director. If a School Administrator or other MWA employee is unsure if an incident is significant, they may contact [insert MWA contact/data point-person] to discuss. (Examples include: A large quantity of information, sensitive personally identifiable information, a stolen/lost laptop known to contain Protected/Sensitive Data, etc.).
	Destroying Data	**General:** Review MWA's Record Retention and Destruction Policy and the information in this destruction section before disposing of records. Do not destroy records that are the subject of a litigation hold or that must be retained pursuant to the MWA Record Retention Policy. All record destruction me be coordinated with the Managing Director of IT.
		Paper & Disposable Electronic Media (CDs, DVDs): If consistent with MWA's Record Retention and Destruction Policy, such media should be physically destroyed using a cross-cut shredder or similar appropriate technology and then recycled or discarded.

		Electronic Files (Data) Reusable Electronic Storage Devices (USB keys, disk drives): If consistent with MWA's Record Retention and Destruction Policy, such media and/or data should be deleted using an approved secure deletion program.
		All Electronic Storage Media at End of Life, including Disk Drives: If consistent with MWA's Record Retention and Destruction Policy, functional electronic media that can be overwritten using a secure erase tool may be recycled or disposed of. Non-functional electronic media (e.g., damaged disk drives) must be physically destroyed.
		Device End of Lease or End of Life (Printers, Copiers, Multi-function office machines): Devices such as these may contain hard drives which must be properly erased, or "wiped", prior to leaving MWA control (returned to the vendor, sent to surplus, donated, disposed of, etc.) and must be coordinated with the Managing Director of IT.

Exceptions

MWA's Managing Director of IT is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and will be based on the implementation of appropriate compensating controls.

Important

Failure to comply with these Data Protection Guidelines may result in harm to individuals, organizations and/or MWA. The unauthorized or unacceptable use of Protected and Sensitive Data, including the failure to comply with these guidelines, constitutes a violation of MWA policy and may subject the individual to revocation of the privilege to access or use Protected and/or Sensitive Data or MWA equipment and technology, or disciplinary action, up to and including termination of employment.