

SECTION: OPERATIONS

TITLE: ELECTRONIC RECORDS
RETENTION

ADOPTED: February 8, 2010

REVISED:

MOON AREA SCHOOL DISTRICT

	<p style="text-align: center;">800. ELECTRONIC RECORDS RETENTION</p> <p>1. Purpose In today’s school district environment, employees and students create and maintain an increasing portion of their records using computers. Electronic records must be managed alongside traditional records to ensure compliance with state and federal regulations and to preserve institutional history.</p> <p>The purpose of this policy is to inform all school district employees of the requirements and responsibilities for management and disposition of electronic records.</p> <p>2. Authority The electronic records retention policy set forth herein applies to all employees of the school district and applies to all electronic records that are made or received in the transaction of the school district or in the operations of the school district.</p> <p>3. Definitions The term electronic record means any record that is created, received, maintained or stored on school district workstations or central servers, archival or backup drivers or media. Examples include, but are not limited to:</p> <ol style="list-style-type: none"> 1. Electronic mail (e-mail). 2. Word processing documents, PDF files and other files. 3. Databases. <p>The term legal custodian shall mean the originator of an e-mail message or the creator of an electronic document, if that person is a school district employee, School Board member, contractor or agent; otherwise it is the school district employee to whom the message is addressed or to whom the electronic document was sent. If the record is transferred, by agreement or policy, to another person for archival purposes, then that person becomes the legal custodian.</p> <p>Official records retention and disposition schedules are the general and departmental program schedules that have been or will have been approved by the Superintendent or his/her designee.</p>
--	--

<p>4. Guidelines</p>	<p><u>General Requirements</u></p> <p>Maintenance and disposal of electronic records, as determined by the content, is the responsibility of the legal custodian and must be in accordance with guidelines established by the Board of School Directors and also in compliance with approved records retention and disposition schedules. Failure to properly maintain electronic records may expose the school district and individuals to legal risks.</p> <p>The Technology Director is responsible for ensuring compliance with this policy and with the public records act. This individual will coordinate with the building principal or administrator the necessary action to be in compliance with this policy.</p> <p>When an employee leaves the school district or is transferred to a different building, the principal, in conjunction the Technology Coordinator, is responsible for designating a new custodian and ensuring that any public records in the separating employee's possession are properly transferred to the new custodian or are properly archived in accordance with this policy.</p> <p>The Technology Coordinator is responsible for the transfer of the electronic records to the new custodian before the accounts are scheduled to be deleted or archived.</p> <p>Each employee is responsible for periodically reviewing any application files, documents, spreadsheets, databases or other electronic records to ensure the timely deletion of records that are no longer needed to conduct school district business, which will allow adequate storage space on school district servers.</p> <p><u>Electronic Records</u></p> <p>Work-related electronic records are school district records and must be treated as such. Each custodian must take responsibility for retaining school district records as directed in official records retention and disposition schedules. E-mail that does not meet the definition of a public record, e.g. personal e-mail or junk e-mail, should be deleted immediately from the system. All electronic records that have been deleted by the e-mail user shall be deleted from archival computer system back-up files following a thirty (30) day period.</p> <p><u>Audio Records</u></p> <p>Voice mail and other electronically recorded audio files will be disposed of in a manner consistent with electronic mail files. In accordance with applicable law, including but not limited to Pennsylvania's wiretapping laws, the school district reserves the right to record telephone conversations for safety, security and quality control purposes.</p>
----------------------	---

Instant Messaging

The school district does not support the use of Instant Messaging (IM).

Backup Files

Information Technology Services performs a backup on a regular schedule of the e-mail and electronic files stored on central serves for disaster recovery. These backups are to be used for system restoration purposes only. The Technology Coordinator or the technology staff is not the legal custodian of messages or records, which may be included in such backups.

Litigation Holds

When litigation against the school district or its employees is filed or threatened, the law imposes a duty upon the school district to preserve all documents and records that pertain to the issues. As soon as the Superintendent is made aware of pending or threatened litigation, a litigation hold directive will be issued to the legal custodians. The litigation hold directive overrides any records retention schedule that may have otherwise called for the transfer, disposal or destruction of the relevant documents, until the hold has been cleared by the Superintendent after consultation with the solicitor. E-mail and computer accounts of separated employees that have been placed on a litigation hold will be maintained by the Technology Director until the hold is released. No employee who has been notified of a litigation hold may alter or delete an electronic record that falls within the school of that hold. Violation of the hold may subject the individual to disciplinary action, up to an including dismissal, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Security Of Electronic Records

The school district shall implement and maintain an effective records security program that incorporates the following:

1. Ensure that only authorized personnel have access to electronic records.
2. Provide for backup and recovery of electronic records to protect against information loss. Documented disaster recovery plans and procedures shall be established for all electronically records systems by the Technology Director. Disaster recovery plans and procedures must be reviewed and updated at least annually.

<p>5. Delegation of Responsibility SC 433</p>	<p>3. Ensure school district personnel are trained to safeguard sensitive or classified electronic information.</p> <p>4. Minimize the risk of unauthorized alteration or erasure of electronic records.</p> <p><u>Enforcement</u></p> <p>Failure to comply with this policy and associated guidelines and procedures will result in disciplinary action and penalties applicable by law.</p> <p>This policy will be reviewed periodically by the Technology Director in cooperation with other administrators to ensure the policy remains current with the evolving technology structure of the school district.</p> <p>References:</p> <p>School Code – 24 P.S. Sec. 433, 518</p> <p>Right-to-Know Law – 65 P.S. Sec. 67.101 et seq.</p> <p>Family Educational Rights and Privacy Act – 20 U.S.C. Sec. 1232g</p> <p>Federal Rules of Civil Procedure – 16, 26, 34, 37, 45</p> <p>Board Policy – 004, 006, 105.2, 114, 138, 203, 203.1, 209, 212, 216, 216.1, 314, 324, 326, 334, 414, 424, 426, 434, 514, 524, 526, 601, 609, 610, 618, 619, 702, 706, 716, 801, 810, 810.1, 912</p>
---	---