MINERSVILLE AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: RECORD RETENTION AND DESTRUCTION

ADOPTED: September 24, 2012

REVISED:

801.1 - RECORD RETENTION AND DESTRUCTION

1. Purpose	It is the policy of the Minersville Area School District that its records, including both paper and electronic, be retained as long as determined necessary to meet legal, audit, educational and business requirements. In each case, the official retention periods must be as short as possible in order to reduce the risk of identity theft and/or breaches of privacy, computer fraud and related harms, to minimize the use of valuable space, to promote efficiency, to assist in the day-to-day operations of the School District, and to reduce the cost of storage and unneeded records inventory. The School District employees must take reasonable measures to protect against unauthorized access to or use of records and information/data, and properly retain and dispose of paper and electronic records, information and data.
2. Authority	The Record Retention and Destruction Policy has been formulated and approved by the Board of School Directors.
3. Delegation of Responsibility	The Superintendent is granted the authority to create and enforce the School District Records and Retention and Destruction schedule. The Record Retention and Records Destruction Policy and the Schedule shall be under the day-to-day supervision of the Superintendent, who may delegate responsibilities to others while maintain the ultimate authority to enforce the Policy and the Schedule. The Superintendent is responsible for the destruction of the School District records. Delegation of responsibilities may be made by the Superintendent if clear guidance is provided to those with delegated responsibility while maintaining the ultimate authority to enforce the Policy and the Schedule. The Superintendent, and/or Designee, must use due diligence when hiring a document destruction contractor to dispose of material. Due diligence could include (a) reviewing an independent audit of a disposal company's operations and/or compliance with various defined destruction laws; (b) obtaining information about the disposal company from references; (c) requiring that the disposal company be certified by a recognized trade association; and (d) reviewing and evaluation the disposal company's information security policies and/or procedures.
4. Guidelines	Training Employees will be provided a copy of this Policy and the Schedule and periodically receive training to ensure compliance with them and to explain how they should be applied.

Litigation hold requirements, the proper retention and disposal methods for information, data, media, and hardware, among others, must be predominant topics in the training sessions.

Litigation Hold

When the School District reasonable anticipates that litigation may ensue and/or the School District has been given notice that a legal action is reasonably anticipated, threatened, pending, imminent, or initiated or a government investigation will occur, destruction of records must be suspended immediately. Notice could occur before the filing of a Complaint, and assumes that the School District is previously aware of an incident or event that is subject to a suit.

The Superintendent must be made aware of events or incidents that are likely to lead to legal action. Counsel must be notified immediately. Counsel will be responsible for evaluation the defenses available to the School District, identifying the records that may be relevant to a legal action, and responding to the suspension of the retention and destruction policies and schedule under the guidelines of the School District.

The School District records that need to be retained due to pending litigation, litigation, or government investigations must be reviewed frequently. Contact must be made with the Superintendent to verify possession of the most current list of records that should be considered protected (i.e. not to be destroyed) due to pending litigation or in litigation or subject to government investigation. Be aware that the court considers all recorded information as a record regardless of the medium of storage of the information. All records that relate to pending litigation, litigation, or regulatory proceedings must be retained during the pending litigation and/or proceeding.

Groups or classes of records must be destroyed in the ordinary course of business under the Policy and the Schedule, which is designed to meet the legitimate needs of the School District. *Selective destruction of records in anticipation of litigation is forbidden.*

Interpretation

The Superintendent, and/or Designee, will be responsible for interpreting any portions of the Policy statement or the Schedule as they may apply to specific situations. Any communication involving specific records retention or destruction requirements should be checked against the School District's required ethical conduct policy.

Exceptions

Requests for exceptions from this Policy should be submitted to the Superintendent. In order to obtain an exception from the Policy, there must be a program that will assure compliance with the basic objectives stated within the Policy, at least as effectively as this Policy and the Schedule.

Review

The Superintendent must review the Policy and the Schedule annually. Suggested changes should be submitted to the Superintendent. Changes in the Schedule made necessary by School District changes and/or changes to the law must be communicated directly to the Superintendent who, after considering the recommendation, may cause appropriate changes to be made in the Schedule, and changes and/or additions to the Policy must be communicated directly by the Superintendent to the Board of Directors who after consideration may cause appropriate changes to be made in the Policy.

Audit

The Superintendent is responsible for auditing the existence and content of the written records retention and destruction program and schedule. The Superintendent is responsible for auditing the actual implementation of the Policy and Schedule.

The School District may hire an outside party to conduct an audit on compliance with this Policy and the Schedule and prepare a written audit report.

Storage

Designating appropriate storage is an important consideration. A storage system should permit the necessary records to be easily located, managed, searched, retrieved and produced.

Storage is a critical consideration in responding to subpoenas, discovery requests, investigations, regulatory requests, educational, and business needs, and Right-to-Know law requests. Accessibility can also facilitate the document retention, production, and destruction components of the records retention and destruction program.

Security of the records is critical for confidential records, particularly records pertaining to employee records such as personnel files, medical records, and insurance forms; student records; government records designated as confidential; and some transactions, financial and tax records. Restricted accessibility and protection are crucial.

Preservation is an important storage consideration. A proper environment conducive to maintaining the integrity of the records is critical. This includes, but is not limited to, secure software, electronic security protections, acid-free folders, climate control, anti-magnetic interference, and fire protection. Off-site storage of vital records is permitted. Anti-virus, anti-spyware, anti-spam, and other software should be maintained and updated regularly.

Disaster Recovery

The record retention and destruction program seeks to identify and preserve records for disaster recovery where the informational value to the School District is so great, and the consequence of loss is potentially so severe to the continuity of the School District, that special protection is warranted. Records that qualify as disaster recovery records include but are not limited to:

a. Legal, financial, tax and organization status records;
b. Obligations to employees, vendors, and students;
c. Ownership of assets and inventory;
d. Intellectual property and achievements not recognized elsewhere; and information on critical decision-making.

Archival Records

Records that have value beyond their original purpose because they document significant educational and/or business activities or services should be safeguarded as a permanent resource. The following considerations should apply to the preservation of records:

a. An archival collection should be prepared that includes, among other things, the minute books, each annual auditor's report, each annual financial report, trademarks, copyrights, deeds, financial records, and photographs.
b. Special consideration should be made to evaluate whether in-school or outside protection is best.
c. Loaned or gifted archival materials to other sources should be maintained by the Superintendent.

Destruction

Proper retention and disposal and/or destruction of paper and electronic records are required.

Records must be disposed of and destroyed by shredding, erasing, or otherwise modifying the information of the record to make the record unusable, unreadable, indecipherable or non-reconstructable through generally available means. Other means include, but are not limited to, burning or pulverizing the records. Information that is stored electronically must be made irretrievable before disposal. Protected Health Information must be destroyed pursuant to the National Institute of Standards and Technology ("NIST") security standards.

Destruction of records includes discarding and abandoning information, as well as the sale, donation, and/or transfer of computers or other media where that information is stored.

Records must be destroyed within seven (7) days of the period designated in the Minersville Area School District Retention and Destruction Schedule, unless an exception is granted by the Superintendent and/or Designee, in writing and a new destruction date is recorded or a litigation hold is relevant.

Destruction of the records (original and copies) may not occur without the approval of the Superintendent.

Consequences for Violation

Employees must be aware that violations of this Policy may result in a variety of disciplinary actions, including but not limited to, warnings, loss of privileges, position reassignment, oral and written reprimands, suspensions (with or without pay), dismissal and/or legal proceedings.

	Violations of this Policy may be reported to appropriate legal authorities, whether local, state or federal law enforcement. The School District will cooperate to the extent legally required with authorities in such investigations.
Reference	Minersville Area School District Records Retention and Records Destruction notebook as published August 2012 for specific details.

Minersville Area School District
PO Box 787
Minersville, PA 17954

Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws

If you suspect information may have been disclosed or used improperly, or you have questions about data breaches generally, contact:

Primary
Mr. M. Joseph Brady, Superintendent
570-544-1400 #1009

Alternate
Mr. Michael Hoptak, Computer Technology Support Specialist
570-544-1400 #2008

The Bollinger Law Firm, LLC
(July 2011)

What type of data is at risk?

Your duties differ depending on the type of data that is at risk. Check the types of data that may have been potentially exposed.

- ☐ Protected Health Information that is subject to HIPAA: Individually identifiable health information held or transmitted in any form or medium.

  This definition *does not* include individually identifiable information in educational records that are maintained by an educational agency or institution or by a person acting for such agency or institution, and are subject to Family and Educational Rights and Privacy Act ("FERPA"), unless at its discretion the Intermediate Unit chooses to include them in this definition, or an exception applies.

  This definition *does not* include FERPA records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice, unless at its discretion the Intermediate Unit chooses to include them in this definition.

- ☐ An individual's first name or first initial and last name in combination with and linked to a social security number.
- ☐ An individual's first name or first initial and last name in combination with and linked to a driver's license number or a state identification number issued in lieu of a driver's license.
- ☐ An individual's first name or first initial and last name in combination with and linked to a financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
- ☐ Other

If you checked Protected Health Information, follow the section titled Protected Health Information for required actions regarding such information.

If you checked any of the next three check boxes related to individually identifiable information, follow the section titled Personal Information for required action regarding this information.

If you checked Other, such information may or may not require further action. Therefore, you will need to determine the type of data, and information about the data breach, then call your attorney.

Protected Health Information

1. Was there a breach of unsecured protected health information?

First, it is necessary to determine if there was a breach of the protected heath information or whether the protected health information was secured or unsecured.

- ☐ *Breach* – the acquisition, access, use, or disclosure of protected health information which comprises the security or privacy of the protected health information. *"Comprises the security or privacy of the protected health information"* means that it poses a significant risk of financial, reputational, or other harm to the individual. For example, an individual's zip code does not compromise the security or privacy of the protected health information.

  Breach *does not* include any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of the Intermediate Unit or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted.

  Additionally, breach *does not* include any inadvertent disclosure by a person who is authorized to access protected health information by the Intermediate Unit or business associate to another person authorized to access protected health information by the Intermediate Unit or business associate, or organized health care arrangement in which the Intermediate Unit participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

  Lastly, breach *does not* include a disclosure of protected health information where the Intermediate Unit or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

  Access means the ability to read, write, modify, or communicate data/information or otherwise use any system resource.

- ☐ *Unsecured* – Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology. Your Information Technology provider may help in determining this answer. Protected health information is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:
  - ☐ Electronic protected health information has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached.

- ☐ The media on which the protected health information is stored or recorded have been destroyed. For paper, film, or other hard copy media, it has been shredded or destroyed such that the personal health information cannot be read or otherwise cannot be reconstructed. Redaction is not sufficient. For electronic media, it has been cleared, purged, or destroyed such that the protected health information cannot be retrieved.

If *both* check boxes have been checked, continue to the next section for legally required actions.

If the incident was not a breach, *or* if the protected heath information was secured, no further action may be necessary, except to prepare and retain a summary of the incident, consider whether you should report the incident to your insurance company, and modify your security. Confirm your considerations with your attorney before proceeding.

2. What actions must be performed?

Notification to individuals

The Intermediate Unit must, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the Intermediate Unit to have been, accessed, acquired, used, or disclosed as a result of such breach. A breach is "discovered" as of the first day on which the breach is known to the Intermediate Unit, or, by exercising reasonable diligence would have been known to the Intermediate Unit. The Intermediate Unit shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Intermediate Unit.

- ☐ Notification to individuals must be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The only exception would be if a law enforcement official states to the entity or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security. In this case, follow written instructions from law enforcement regarding delaying notification or document oral instructions to that effect including the identity of the official making the statement and the length of delay. If it is an oral statement, the delay cannot be for more than 30 days.
- ☐ The content of the notification must contain the following elements to the extent possible and in plain language:
  - ☐ A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - ☐ A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

- ☐ Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- ☐ A brief description of what the Intermediate Unit is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- ☐ Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

☐ *Written Notice.* The notice must be in writing and sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

- ☐ If the Intermediate Unit knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual is required. The notification may be provided in one or more mailings as information is available.

☐ *Substitute Notice.* In the case in which there is insufficient or out-of-date contact information that precludes written notice, a substitute form of notice reasonably calculated to reach the individual must be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.

- ☐ In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
- ☐ In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice must:
  - ☐ Be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the Intermediate Unit, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
  - ☐ Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

☐ *Additional notice in urgent situations.* In any case deemed by the Intermediate Unit to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.

Notification to the media

For a breach of unsecured protected health information involving *more than 500* residents of a State or jurisdiction, an entity must notify prominent media outlets serving the State or jurisdiction.

- ☐ Notification to the media must be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Notification to the media shares the same

law enforcement exception as notification to individuals. Follow the exception outlined above if law enforcement asks you to delay notification.

- ☐ The content of the notification to the media must include the same plain-language elements as the notification to individuals. Follow the above checklist to ensure compliance.

Notification to the Secretary of Heath and Human Services

The Intermediate Unit must notify the Secretary following the discovery of a breach of unsecured protected health information.

- ☐ For breaches involving 500 or more individuals, the Intermediate Unit must provide notification to the Secretary of HHS contemporaneously with the notification to individuals as outlined above and in the manner specified on the Heath and Human Services website.
- ☐ For breaches involving less than 500 individuals, the Intermediate Unit must maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification to the Secretary of HHS for breaches occurring during the preceding calendar year in the manner specified on the Health and Human Services website.

Notification by a business associate who discovers a breach

A business associate must, following the discovery of a breach of unsecured protected health information, notify the Intermediate Unit of the breach.

- ☐ Notification to the Intermediate Unit must be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Notification to the media shares the same law enforcement exception as notification to individuals. Follow the exception outlined above if law enforcement asks you to delay notification.
- ☐ The notification must include, to the extent possible, the following:
  - ☐ The identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
  - ☐ Any other available information that the Intermediate Unit is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

Personal Information

1. Was there a breach of the security of the system?

First, it is necessary to determine whether a breach of the security of the system actually occurred and whether unencrypted and unredacted personal information was at risk.

- ☐ *Breach of the security of the system* – The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the Intermediate Unit as part of a database of personal information regarding multiple individuals and that causes or the Intermediate Unit reasonably believes has caused or will cause loss or injury to any resident of Pennsylvania.

  This definition *does not* include a good faith acquisition of personal information by an employee or agent of the Intermediate Unit for the purposes of the entity if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

  Check this box if you know an unauthorized person had access to or acquired the information or whether you reasonably believe an unauthorized person had access to or acquired the information.

- ☐ *Unencrypted* – Encrypted data has been transformed by an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Your Information Technology provider can help determine if the data was encrypted.

  Check this box if the breach is linked to the security of the encryption.

  Check this box if the security breach involves a person with access to the encryption key.

- ☐ *Unredacted* – Unredacted data includes, but is not limited to, alteration or truncation such that a driver's license number, or a State identification card number, or an account number, or not more than the last four digits of a Social Security number, is accessible as part of the data.

- ☐ *Personal Information* – Personal information includes an individual's first name or first initial and last name in combination with and linked to either a Social Security number, driver's license number or a State identification card number issued in lieu of a driver's license, or financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

  The term *does not* include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

Action is required if every check box above has been marked. Confirm with your attorney before proceeding. If the data breach notification law of another state and Pennsylvania's law apply consult with your attorney.

2. What actions must be performed?

- ☐ Take measures necessary to determine the scope of the breach.
- ☐ Restore the reasonable integrity of the data system.
- ☐ Report the breach of the system's security and any information pertaining to the breach to the local, state, or federal law enforcement agency for investigation or handling in advance of the disclosure to any resident, or others.

The notification may be delayed if a law enforcement agency determines and advises the Intermediate Unit in writing specifically referencing this section that the notification will impede a criminal or civil investigation, or will compromise an investigation into National or homeland security. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

Notification to Individuals

Any resident of Pennsylvania whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person must be notified.

- ☐ A resident of Pennsylvania may be determined to be an individual whose principal mailing address, as reflected in the computerized data that is maintained, stored or managed by the Intermediate Unit, is in Pennsylvania.
- ☐ Notification may be provided by any of the following methods:
  - ☐ Written notice to the last known home address for the individual.
  - ☐ Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
  - ☐ E-mail notice, if a prior business relationship exists and the person or Intermediate Unit has a valid e-mail address for the individual.
  - ☐ Substitute notice, if the Intermediate Unit demonstrates one of the following:
    - ☐ The cost of providing notice would exceed $100,000.
    - ☐ The affected class of subject persons to be notified exceeds 175,000.
    - ☐ The entity does not have sufficient contact information.

    Substitute notice must consist of all of the following:

    - ☐ E-mail notice when the Intermediate Unit has an e-mail address for the subject persons.

- ☐ Conspicuous posting of the notice on the Intermediate Unit's Internet website if the Intermediate Unit maintains one.
- ☐ Notification to major state-wide media.

☐ Notification must be made without unreasonable delay.

Notice of Vendors

A vendor that maintains, stores, or manages computerized data on behalf of the Intermediate Unit must provide notice of any breach of the security system following discovery by the vendor to the Intermediate Unit on whose behalf the vendor maintains, stores, or manages the data. The Intermediate Unit must be responsible for making the determinations and discharging any remaining duties.

Notification of consumer reporting agencies

When an entity provides notification under Pennsylvania's *Breach of Personal Information Notification Act* to more than 1,000 persons at one time, the Intermediate Unit must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices.

A consumer reporting agency is an agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, public record information and credit account information from persons who furnish that information regularly and in the ordinary course of business.