# Policy Committee Meeting

Monday, October 19, 2026 5:15 PM
Educational Service Center, 775 Marion Road, York, PA 17406

| | | |
|---|---|---|
| 1. | **Call to Order** | **Speaker(s):** Committee Chair |
| 2. | **Roll Call** | **Speaker(s):** Board Secretary |
| 3. | **Discussion Items** | **Speaker(s):** Committee Chair & Assistant Superintendent |
| 3.A. | Policy 616 — Payment of Bills | |
| 3.B. | Policy 830 — Security of Computerized Personal Information/Data Breach Notification | |
| 3.C. | Policy 830.1 — Data Governance — Storage/Security | |
| 4. | **Adjournment** | **Speaker(s):** Committee Chair |

BOARD POLICY

# 616 Payment of Bills Draft 3 10.14.26

| POLICY NUMBER | ADOPTED | VERSION | DOCUMENT STATUS |
|---|---|---|---|
| 616 | 7/11/2011 | v1.9 | DRAFT |

PRINTED
10/16/2026

## Purpose

It is the Board's intent to direct prompt payment of bills but at the same time to ensure that due care has been taken in the review of district bills.

## Authority

Each bill or obligation of this district must be fully itemized, verified and approved by the Board before a check can be drawn for its payment, except that payment of bills prior to Board approval can be made by the Board Secretary/Chief Financial Officer under any of the following conditions:[1] [2] [3]

1. The prompt payment of items that will accrue to the district's advantage.[4] [1]
2. Progress payments to contractors specified in a contract approved by the Board.
3. Orders to cover approved payrolls and agency account deposits.
4. Utility bills in months the Board does not meet.
5. Other payments, deemed to be time sensitive or unanticipated by the Superintendent, will be presented to the Board for retroactive approval.

## Delegation of Responsibility

It shall be the responsibility of the recipient of the goods to verify ~~Chief Financial Officer or designee~~ upon receipt of an invoice ~~to verify~~ that the purchase invoice is in order, goods were received in acceptable condition or services were satisfactorily rendered, funds are available to cover the payment, the Board had budgeted for the item, and invoice is for the amount contracted. Any discrepancies should be reported to the Chief Financial Officer.

Should the invoice vary from the acknowledged purchase order, the Chief Financial Officer or designee shall document on the invoice the reason for such variance.

Should funds not be available in the account to which a proposed purchase will be charged, the Chief Financial Officer or designee shall determine the overage and request the Board make a legal transfer to cover it.[2] [5] [6] **[7]**

All claims for payment shall be provided to the Board on a monthly basis for their approval and recorded in the minutes of the Board meeting.

The list of bills shall include for each:

1. Check number/ACH Voucher number.
2. Check date.
3. Vendor.
4. Amount of remittance.

Upon approval of an order, the Treasurer and Chief Financial Officer shall prepare a check for payment and cancel the commitment placed against the appropriate account.[1]

All checks approved by the Board shall be signed by the President, Board Secretary, and Treasurer.[4] [8] [1]

The Vice-President may sign for the President.[9]

**Guidelines**

Signatures of the President, Vice-President, Treasurer and Board Secretary may be engraved on a signature plate or stamp. Electronic signatures may be used if the law requires a signature unless applicable law requires the records to be signed in nonelectronic form. [10]

No check shall be made out to cash.

Sales Tax

The district is exempt from sales tax on the purchase of tangible, personal property or services that are sold or used by the district. The district shall control use of its sales tax exemption number issued by the Department of Revenue, in compliance with established regulations. The exemption number shall be used only when buying property or services for district use.[11] [12]

The district shall obtain a sales tax license number for school organizations who purchase items to be resold.[11] [13] **[14]**

In order to monitor these activities, the Chief Financial Officer ~~Business Manager~~ shall develop procedures to assure coordination and accumulation of information and proper reporting and remittance to the Department of Revenue.

Recipient of Nonsufficient Fund (NSF) Checks

The Board authorizes the Chief Financial Officer or designee ~~business office~~ to establish and administer guidelines regarding collection of payment for NSF checks and associated service charges. The Chief Financial Officer or designee will determine whether notification by certified mail, with return receipt, and whether filing charges with the district magistrate will be pursued.

The Board shall authorize a service charge for each NSF check.

The Board directs that any payor ~~individual~~ issuing more than one (1) NSF check to the district will be advised that checks may no longer be accepted from that payor ~~individual~~. The Chief Financial Officer or designee will determine if any further checks will be accepted.

Electronic Funds Transfer (EFT)

The Board authorizes the business office to establish guidelines for Electronic Funds Transfers (EFT) of the school district.

It is the policy of the district to comply with all state laws relating to Electronic Funds Transfers (EFT).

---

## Legal Footnotes

[1] 24 P.S. 439
LEGAL REFERENCE

[2] 24 P.S. 607
LEGAL REFERENCE

[3] 24 P.S. 1155
LEGAL REFERENCE

[4] 24 P.S. 427
LEGAL REFERENCE

[5] 24 P.S. 609
LEGAL REFERENCE

[6] 24 P.S. 687
LEGAL REFERENCE

[7] Pol. 612 — Purchases Not Budgeted
POLICY REFERENCE

[8] 24 P.S. 433
LEGAL REFERENCE

[9] 24 P.S. 428
LEGAL REFERENCE

[10] 65 P.S. 302
LEGAL REFERENCE

[11] 61 PA Code 32.23
LEGAL REFERENCE

[12] 72 P.S. 7204
LEGAL REFERENCE

[13] 72 P.S. 7208
LEGAL REFERENCE

[14] Pol. 618 — Student Activity Funds
POLICY REFERENCE

BOARD POLICY

# 830 Security of Computerized Personal Information/Breach Notification Draft 2 10.13.26

| POLICY NUMBER | VERSION | DOCUMENT STATUS | PRINTED |
|---|---|---|---|
| 830 | v1.3 | DRAFT | 10/14/2026 |

## Purpose

The Board is committed to the security of the district's computerized data and to addressing the risk of a breach of the district's systems involving the possible disclosure of personal information. This policy addresses the manner in which the district will respond to unauthorized access and acquisition of computerized data that compromises the security and confidentiality of personal information.

## Authority

The Board requires that records containing personal information be securely maintained, stored and managed in compliance with state and federal laws, regulations, Board policy, administrative regulations and the district's Records Management Plan.[1] [2] [3] [4] [5] [6] [7] [8]

The Board directs the district to provide notice as required by law to any individual ~~resident of the Commonwealth~~ whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.[1]

## Definitions

**Breach of the security of the system** - unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the district as part of a database of personal information regarding multiple individuals and that causes, or the district reasonably believes has caused, or will cause, loss or injury to any individual ~~resident of the Commonwealth~~. Acquisition of personal information by an employee or agent acting in good faith on behalf of the school district is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the district and is not subject to further unauthorized disclosure.[9]

**Determination** - a verification or reasonable certainty that a breach of the security of the system has occurred.[9]

**Discovery** - the knowledge of or reasonable suspicion that a breach of the security of the system has occurred.[9]

**Encryption** - 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.[9]

**Personal information** - includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted:[9]

1. Social Security number.
2. Driver's license number or state identification card number issued instead of a driver's license.
3. 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.
4. Medical information, meaning any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional.[9]

5. Health insurance information, meaning an individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.[9]

6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.[9] **[10]**

**Records** - means any material, regardless of its physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed or electromagnetically transmitted. This term does not include publicly available directories containing information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.[9]

**Redact -** includes, but is not limited to, alteration or truncation such that no more than the last four (4) digits of a Social Security number, driver's license number, state identification card number or account number is accessible as part of the data. [9]

**Delegation of Responsibility**

The Superintendent or designee shall ensure that the district provides notice, as required by law, of any breach of the security of the district's systems.[1]

The Superintendent, in collaboration with appropriate administrators, shall develop administrative regulations to implement this policy, which shall include, but not be limited to:[1]

1. Procedures following discovery of a breach.

2. Procedures for the determination of a breach and whether breach notification is required under the law.

3. Breach notification procedures including timeline requirements, who must be notified and methods for such notice.

**Guidelines**

Upon determination of a breach of the security of the system, the Superintendent or designee shall provide notice to the district attorney in the county where the breach occurred and to any individual ~~resident of the Commonwealth~~ whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Such notice shall be made in accordance with the provisions of law regarding timelines and methods of notification.[1]

The notice shall be made without an unreasonable delay, except when a law enforcement agency determines and advises the district in writing, citing the applicable section of law, that the notification would impede a criminal or civil investigation, or the district must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system.[11][12]

The district shall also provide notice of the breach if the encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of security of the encryption, or if the security breach involves a person with access to the encryption key.**[1]**

---

## Legal Footnotes

**[1]** **73 P.S. 2301 et seq**
LEGAL REFERENCE

**[2]** **Pol. 113.4 — Confidentiality of Special Education Student Information**
POLICY REFERENCE

**[3]** **Pol. 216 — Student Records**
POLICY REFERENCE

**[4]** **Pol. 324 — Personnel Files**
POLICY REFERENCE

**[5]** **Pol. 800 — Records Management**
POLICY REFERENCE

**[6]** **Pol. 800.1**
POLICY REFERENCE
*Referenced policy is not available in this policy book.*

**[7]** **Pol. 815 — Acceptable Use of Computers, Email, Network Resources, and Internet Access**

**[8]** **Pol. 830.1**
POLICY REFERENCE
*Referenced policy is not available in this policy book.*

POLICY REFERENCE

[9] **73 P.S. 2302**
LEGAL REFERENCE

[10] **Pol. 801 — Public Records**
POLICY REFERENCE

[11] **73 P.S. 2303**
LEGAL REFERENCE

[12] **73 P.S. 2304**
LEGAL REFERENCE

CENTRAL YORK SCHOOL DISTRICT

POLICY PORTAL™ PSBA

BOARD POLICY

# 830.1 Data Governance-Storage/Security

| POLICY NUMBER | VERSION | DOCUMENT STATUS | PRINTED |
|---|---|---|---|
| 830.1 | v1.2 | DRAFT | 9/21/2026 |

Proposed addition Proposed deletion

## Purpose

The district is required to collect, create, store and manage data and information. Accurately maintaining and protecting such data is essential for efficient district operations, legal compliance, confidentiality and upholding trust with the school community.

This policy addresses the Board's commitment to sound data governance related to the integrity and security of the data collected, maintained, stored and managed by the district.

## Authority

The Board recognizes the importance of establishing and maintaining a system of data governance that addresses district staff responsibilities and complies with federal and state laws and regulations regarding data storage, security and records management. The district's data governance system shall meet or exceed industry and/or government standards for data protection and privacy of personal information.[1][2]

The Board directs that the creation, collection, retention, retrieval and disposition of district records shall be governed by Board policy and the district's Records Management Plan and Records Retention Schedule.[3]

The Board directs notifications of a breach of the security of the district's computerized data system involving an individual's personal information to be conducted in accordance with law and Board policy. [4] [5]

## Definitions

**Confidential Data/Information** - information regarding which law, Board policy or contract prohibit disclosure or that may be disclosed only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information and other personal information regarding students, employees and district residents.[6][7][8]

**Critical Data/Information** - information that is essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations.

**Data Governance** - the district's comprehensive system to ensure the integrity of data created, collected, stored, secured and managed by the district.

**Encryption** - 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.[9]

**Personal Information** - includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following when not encrypted or redacted:[5][9]

1. Social Security number.
2. Driver's license number or state identification card number issued instead of a driver's license.
3. 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.
4. Medical information, meaning any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional.[9]
5. Health insurance information, meaning an individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.[9]
6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.[9][10]

**Records Management Plan** - the system implemented by the district for the storage, retention, retrieval and disposition of all records generated by district operations.[3]

**Records Retention Schedule** - a comprehensive listing stating retention periods and proper disposition of records.[3]

### Delegation of Responsibility

The Superintendent, in coordination with the Director of Information Technology, shall develop procedures necessary to implement this policy.

All individuals who are granted access to confidential and/or critical data/information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such data/information.[5][11]

The Director of Information Technology shall conduct regular vulnerability and risk assessments to monitor the integrity of the district's system of data governance.

The Superintendent shall ensure that this policy is reviewed at least annually and updated as necessary.[1][2]

## Guidelines

The district's system of data governance shall include, but not be limited to, the following:

1. Data security controls that meet or exceed industry and/or government standards for data protection and privacy, to ensure that only authorized individuals have access to computerized data.
2. A plan for backup and recovery of data to protect against information loss. Redundant backup systems of data storage shall be securely maintained in separate physical locations or in separate data storage systems.
3. Training requirements for individuals who have access to confidential and/or critical data and information.
4. Provisions to minimize the risk of unauthorized access, alteration or erasure of computerized data.[5]
5. An inventory of all software applications, digital tools and platforms, and related instruments comprising the data governance system.
6. Procedures for addressing a breach of data and cybersecurity incidents.[5]
7. Procedures and acceptable use provisions for access to data and protection of privacy and personal information for students, staff and district residents.[5][12]
8. A requirement that all service providers retained or contracted by the district for data governance and records management purposes meet or exceed industry and/or government standards for data protection and privacy of personal information.

Use of Personal Electronic Devices and Resources

The district prohibits storage of confidential and/or critical data/information of the district on a personal electronic device, personal email account or other personal platform. District staff and service providers shall use district-controlled accounts and platforms to securely access, store or transmit confidential and/or critical data/information of the district.

Service Providers

Service providers retained or contracted by the district shall comply with law, Board policy, administrative regulations and district procedures regarding data security and integrity of data containing confidential and/or critical data/information of the district.[3][5]

The district shall ensure that the agreement or contract for service with a service provider who may have access to confidential and/or critical data/information reflects appropriate data security provisions.

Consequences

Failure to comply with law, Board policy, administrative regulations or procedures regarding data governance and security may result in the following disciplinary measures and possible pursuit of civil and criminal sanctions:[13][14][15]

1. Employees may be disciplined up to and including termination.
2. Volunteers may be excluded from providing services to the district.

3. The termination of a business relationship with a service provider.

## Legal Footnotes

[1] 73 P.S. 2305.1
LEGAL REFERENCE

[2] 73 P.S. 2305.2
LEGAL REFERENCE

[3] Pol. 800
LEGAL REFERENCE

[4] 73 P.S. 2301
LEGAL REFERENCE

[5] Pol. 830
LEGAL REFERENCE

[6] Pol. 113.4
LEGAL REFERENCE

[7] Pol. 216
LEGAL REFERENCE

[8] Pol. 324
LEGAL REFERENCE

[9] 73 P.S. 2302
LEGAL REFERENCE

[10] Pol. 801
LEGAL REFERENCE

[11] Pol. 828
LEGAL REFERENCE

[12] Pol. 815
LEGAL REFERENCE

[13] Pol. 317
LEGAL REFERENCE

[14] Pol. 818
LEGAL REFERENCE

[15] Pol. 916
LEGAL REFERENCE

## Legal References

No additional references listed.