



**KEYSTONE OAKS SCHOOL DISTRICT  
1000 KELTON AVENUE  
PITTSBURGH, PA 15216**

**BOARD OF SCHOOL DIRECTORS**

**WORK SESSION  
LOCATION – PARKWAY WEST  
TUESDAY, OCTOBER 10, 2023  
7:00 PM**

**BUSINESS/LEGISLATIVE SESSION  
TUESDAY, OCTOBER 17, 2023  
7:00 PM**

**KEYSTONE OAKS SCHOOL DISTRICT  
SCHOOL DIRECTORS' CALENDAR OF EVENTS**

**Tuesday, October 10, 2023 – Work Session**

**7:00 PM Meeting**

- Call to Order – President
- Pledge of Allegiance
- Public Comment
- Review of Reports
- Public Comment
- Adjournment

**Tuesday, October 17, 2023 – Business/Legislative**

**7:00 PM Meeting**

- Call to Order – President
- Pledge of Allegiance
- Public Comment
- Approval of Reports
- Public Comment
- Adjournment

# **BOARD PRESIDENT'S REPORT**

**OCTOBER 17, 2023**

**Mrs. Theresa Lydon**

## **BOARD ACTION REQUESTED**

### **I. BOARD MINUTES**

It is recommended that the Board approve the Work Session Minutes of September 12, 2023 and the Business/Legislative Minutes of September 19, 2023.

## **FOR INFORMATION ONLY**

- I.** Parkway West Career and Technology Center Report *Mrs. Annie Shaw*
- II.** SHASDA Report *Mr. Santo Raso*
- III.** PSBA/Legislative Report *Mrs. Theresa Lydon*
- IV.** News from the Boroughs
- V. EXECUTIVE SESSION**

# SUPERINTENDENT'S REPORT

OCTOBER 17, 2023

Dr. William P. Stropkaj

## BOARD ACTION REQUESTED

### I. SECOND READING POLICY 800: RECORDS MANAGEMENT PLAN

It is recommended that the Board approve the SECOND READING of Policy 800: *Records Management Plan*.

### II. SECOND READING POLICY 800.1: ELECTRONIC SIGNATURES/RECORDS

It is recommended that the Board approve the SECOND READING of Policy 800.1: *Electronic Signatures/Records*.

### III. SECOND READING POLICY 830: SECURITY OF COMPUTERIZED PERSONAL INFORMATION/BREACH NOTIFICATION

It is recommended that the Board approve the SECOND READING of Policy 830: *Security of Computerized Personal Information: Breach Notification*.

### IV. SECOND READING POLICY 830.1: DATA GOVERNANCE-STORAGE/SECURITY

It is recommended that the Board approve the SECOND READING of Policy 830.1: *Data Governance-Storage/Security*.

### V. APPROVAL OF COMPREHENSIVE PLAN

The Administration recommends that the Board approve the Comprehensive Plan to be submitted to the Pennsylvania Department of Education.

#### For Information Only

The plan has been on display for 28 days.

### VI. PROFESSIONAL DEVELOPMENT

It is recommended that the Board approve the following Professional Development requests:

<b>Dr. William P. Stropkaj, Ed.D.</b>	SXSW EDU 2024	\$7,160.00
<b>Mr. Joseph A. Kubiak</b>	Houston, TX	(total for both)
	March 4 – 7, 2023	

For Information Only

The Grable Foundation will be giving the District \$5,000.00 to attend SXS EDU 2024. Total District funds requested is \$2,160.00.

**Ms. Desiree Burns**

Council of Administrators of Special Education (CASE) \$875.00  
Pittsburgh, PA  
November 8 – 10, 2023

# PUPIL PERSONNEL REPORT

OCTOBER 17, 2023

Dr. William P. Stropkaj

## BOARD ACTION REQUESTED

### I. GLOBAL WORDSMITHS LANGUAGE SERVICES AGREEMENT

It is recommended that the Board approve the Services Agreement between Global Wordsmiths LLC and the Keystone Oaks School District effective September 19, 2023 through September 30, 2025.

#### For Information Only

Global Wordsmiths LLC will provide the District Language Translation Services and Language Interpretation Services. The District compensates Global Wordsmiths based on the services it provides to the District. The cost varies for *Consecutive Interpretation Services, Consecutive Pre-Scheduled Video Remote Interpretation Services, On-Demand Telephonic Interpretation Services and Written Translation Services.*

# PERSONNEL REPORT

OCTOBER 17, 2023

Mrs. Theresa Lydon, Chairperson

## BOARD ACTION REQUESTED

### I. RESIGNATIONS

It is recommended that the Board accept the following resignations:

<u>Name</u>	<u>Position</u>	<u>Effective Date</u>
Chelsea Allan	Paraprofessional	October 3, 2023
Kathleen Pietropaulo	Paraprofessional	October 5, 2023
Paul Whalen	Custodian	October 6, 2023
Beth Whitney	Teacher – Special Education – High School	September 21, 2023

### II. APPOINTMENTS

#### 1. Food Service Personnel

It is recommended that the Board approve the following individual as a Food Service employee for the 2023/2024 school year:

<u>Name</u>	<u>Hourly Wage</u>
Patricia Joseph	\$13.50

#### 2. Food Service Personnel – Change in Hourly Wage

It is recommended that the Board approve the change in hourly wages for the following Food Service Personnel retroactive to October 1, 2023:

<u>Employee</u>	<u>New Hourly Wage</u>
Lyssa Glaze	\$14.50
Nicole Paris	\$14.50

#### 3. Approval of Activity Stipends

In compliance with the *Keystone Oaks Education Association Collective Bargaining Agreement 2020-2026*, it is recommended that the Board approve the following individuals for the 2023/2024 school year:

<u>Activity</u>	<u>Position</u>	<u>Sponsor</u>	<u>Stipend</u>
<b>Basketball (V, Boys)</b>	Head Coach	<b>Gary Goga</b>	\$6,500.00
	Assistant	<b>Johnny Lee</b>	\$3,250.00
<b>Basketball (MS, Boys)</b>	Head Coach	<b>Ian Barrett</b>	\$2,500.00
	Assistant	<b>Keith Buckley</b>	\$3,000.00
	Assistant	<b>OPEN</b>	\$1,500.00
<b>Basketball (V, Girls)</b>	Head Coach	<b>Jim Feeney</b>	\$6,500.00
	Assistant	<b>Mike Orosz</b>	\$3,250.00
<b>Basketball (MS, Girls)</b>	Head Coach	<b>OPEN</b>	\$2,500.00
	Assistant	<b>Keith Buckley</b>	\$3,000.00
	Assistant	<b>Amy Torcaso</b>	\$1,000.00
<b>Best Friends (HS)</b>		<b>Pamela Gianoglio</b>	\$750.00
		<b>Joyelle Galiszewski</b>	\$750.00
<b>Chess Club (MS)</b>		<b>Patrick Falsetti</b>	\$1,500.00
<b>FBLA</b>		<b>Kimberly Smykal</b>	\$3,000.00
<b>Girls Who Code</b>	Volunteer	<b>Haylie Toth</b>	
<b>Swimming</b>	Head Coach	<b>Jeff DiGiacomo</b>	\$5,000.00
	Assistant	<b>Rachael McShane</b>	\$2,500.00
	Volunteer	<b>Dani Sakulski</b>	
	Volunteer	<b>Trent Ladner</b>	
<b>Volleyball (MS, Girls)</b>	Head Coach	<b>Hope Harris</b>	\$3,000.00
	Assistant	<b>Gina Huss</b>	\$1,500.00
<b>Wrestling (V)</b>	Head Coach	<b>Brian Hutchin</b>	\$5,000.00
	Assistant	<b>OPEN</b>	\$2,500.00
<b>Wrestling (MS)</b>	Head Coach	<b>Blaine Johnson</b>	\$3,000.00

#### **4. Volunteer Gymnastic Coaches**

It is recommended that the Board approve Lauren Bradford and Danielle Cain as Volunteer Gymnastic Coaches for Sydney Maegle (Freshman).



**5. After-School Tutoring Program**

It is recommended that the Board approve the following individual to participate in the After-School Tutoring Program for the 2023/2024 school year:

**Employee**

**School**

Brandi Forester

Dormont Elementary School

**III. FAMILY AND MEDICAL LEAVE**

It is recommended that the Board approve the following individual for Family and Medical Leave:

Employee #4982 – September 16, 2023 to June 10, 2024

**IV. SABBATICAL LEAVE**

It is recommended that the Board approve the following individual for sabbatical leave:

**Melissa Palmieri**

Middle School – Learning Support

2<sup>nd</sup> semester 2023/2024 school year

**FINANCE REPORT  
OCTOBER 17, 2023**

**Mr. Nafis Hill, Chairperson**

**BOARD ACTION REQUESTED**

**I. ACCOUNTS PAYABLE APPROVAL LISTS THROUGH SEPTEMBER 30, 2023**

The Administration recommends approval of the following Accounts Payable lists as presented in the *Finance Package*:

A. General Fund as of September 30, 2023 (Check No. 70397-70627)	\$2,340,225.79
B. Food Service Fund as of September 30, 2023 (Check No. 9765-9770)	\$138,907.86
C. Athletics as of September 30, 2023 (Check No. 3469-3477)	\$4,218.43
D. Capital Reserve as of September 30, 2023 (None)	\$0.00
<b>TOTAL</b>	<b>\$2,483,352.08</b>

**FOR INFORMATION ONLY**

**I. EXPENDITURE/REVENUE 2023 – 2024 BUDGET to ACTUAL / PROJECTION**

<b>ACCT</b>	<b>DESCRIPTION</b>	<b>2023-2024 BUDGET TOTAL</b>	<b>2023-2024 3 MONTH SEPTEMBER/ACTUAL</b>	<b>OVER (UNDER) BUDGET</b>
<b>Revenue</b>				
6000	Local Revenue Sources	\$ 32,672,317	\$ 20,168,793	\$ (12,503,525)
7000	State Revenue Sources	\$ 13,333,933	\$ 3,073,485	\$ (10,260,448)
8000	Federal Revenue Sources	\$ 805,962	\$ 630,428	\$ (175,534)
<b>Total Revenue</b>		<b>\$ 46,812,212</b>	<b>\$ 23,872,706</b>	<b>\$ (22,939,506)</b>
				<b>(OVER) UNDER BUDGET</b>
<b>Expenditures</b>				
100	Salaries	\$ 20,607,107	\$ 2,203,964	\$ 18,403,143
200	Benefits	\$ 13,416,990	\$ 912,454	\$ 12,504,536
300	Professional/Technical Services	\$ 1,929,206	\$ 166,453	\$ 1,762,753
400	Property Services	\$ 1,493,800	\$ 296,161	\$ 1,197,639
500	Other Services	\$ 5,446,273	\$ 709,715	\$ 4,736,558
600	Supplies/Books	\$ 1,715,234	\$ 963,242	\$ 751,992
700	Equipment/Property	\$ 1,015,150	\$ 878,696	\$ 136,454
800	Other Objects	\$ 87,100	\$ 41,741	\$ 45,359
900	Other Financial Uses	\$ 1,101,352	\$ 1,699,963	\$ (598,611)
<b>Total Expenditures</b>		<b>\$ 46,812,212</b>	<b>\$ 7,872,388</b>	<b>\$ 38,939,824</b>
<b>Revenues exceeding Expenditures</b>		<b>\$ -</b>	<b>\$ 16,000,318</b>	<b>\$ 16,000,318</b>
<b>Other Financing Sources/(Uses)</b>				
	Interfund Transfers In (Out)	\$ -	\$ -	\$ -

## II. SUMMARY OF STUDENT ACTIVITIES ACCOUNTS AS OF SEPTEMBER 30, 2023

Bank Account - Status	Middle / High School	Athletics
Cash Balance - 09/01/2023	\$ 214,539.66	\$ 6,710.57
Deposits	\$ 1,498.31	\$ 12,119.91
Subtotal	\$ 216,037.97	\$ 18,830.48
Expenditures	\$ -	\$ 3,900.93
Cash Balance - 09/30/2023	\$ 216,037.97	\$ 14,929.55

## III. BANK BALANCES

### BANK BALANCES PER STATEMENT AS OF SEPTEMBER 30, 2023

	BALANCE
<b>GENERAL FUND</b>	
FNB BANK	\$ 2,629,619
PAYROLL (pass-thru account)	\$ 6,316
FNB SWEEP ACCOUNT	\$ -
ATHLETIC ACCOUNT	\$ 14,930
PLGIT	\$ 11,308,548
FNB MONEY MARKET	\$ 9,661,764
PSDLAF	\$ 170,515
INVEST PROGRAM	\$ 190,561
OTHER POST-EMPLOYMENT BENEFITS	\$ 2,072,133
COMPENSATED ABSENCES	\$ 449,085
	<b>\$ 26,503,471</b>
<b>CAFETERIA FUND</b>	
FNB BANK	\$ 866,112
PLGIT	\$ 1,077,226
	<b>\$ 1,943,338</b>
<b>CONSTRUCTION FUND / CAP RESERVE</b>	
FNB BANK	\$ 43,088
PLGIT - G.O. BOND SERIES C OF 2014/ 12-19	\$ 843
	<b>\$ 43,931</b>
<b>GRAND TOTAL</b>	<b>\$ 28,490,740</b>

**BUILDINGS, GROUNDS &  
TRANSPORTATION REPORT**

**OCTOBER 17, 2023**

**Mr. Santo Raso, Chairperson**

**BOARD ACTION REQUESTED**

**I. RFP – ARCHITECT FOR RENOVATIONS**

It is recommended that the Board approve the administration to obtain proposals for an architect to complete a study of the three (3) elementary buildings for the purpose of future renovations.

**II. RFP – ARCHITECT FOR MARQUEES**

It is recommended that the Board approve the administration to obtain proposals for an architect for the purpose of designing marquees at all five school buildings in the District.

# ACTIVITIES & ATHLETICS REPORT

OCTOBER 17, 2023

Mr. Thomas LaPorte, Chairperson

## BOARD ACTION REQUESTED

### I. COMPETITIVE EVENT

It is recommended that the Board approve the following competitive event:

#### **Golf (Level III)**

Penn State University

October 15 – 17, 2023

Number of Students – 1

Activity Sponsor – Dennis Sarchet

District Funds Requested for Students - \$500.00

District Funds Requested for Sponsor - \$703.00

Total Maximum District Funds Requested - \$1,201.58

KEYSTONE OAKS SCHOOL DISTRICT

# Policy Guide



Policy No. 826 800

Section OPERATIONS

Title RECORDS MANAGEMENT PLAN

Adopted NOVEMBER 16, 2009

Last Revised NOVEMBER 21, 2013

<b>POLICY NO. 800826 RECORDS MANAGEMENT PLAN</b>		
<b>Section 1</b>	<p><b><u>Purpose</u></b></p> <p>The Board recognizes the importance of establishing and maintaining a Records Management Plan that defines district staff responsibilities and complies with federal and state laws and regulations.</p>	
<b>Section 2</b>	<p><b><u>Authority</u></b></p> <p>The Board shall retain, as a permanent record of the District, Board minutes, annual auditor's reports and annual financial reports. All other financial records, including financial account books, orders, bills, contracts, invoices, receipts and purchase orders, shall be retained by the District for a period of not less than six (6) years.</p> <p>All other district records shall be retained in accordance with state and federal laws and regulations and the District Records Management Plan approved by the Board.</p> <p>The District shall make a good faith effort to comply with all proper requests for record production. Selective destruction of records in anticipation of litigation is forbidden.</p>	<p>SC 518</p> <p>65 P.S. 67.901 Pol. 623</p>
<b>Section 3</b>	<p><b><u>Definitions</u></b></p> <p><b>Electronic Mail (Email) System</b> - a system that enables users to compose, transmit, receive and manage text and/or graphic electronic messages and images across local area networks and through gateways connecting other networks. This information</p>	

**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

consists primarily of messages but may include attachments such as calendars, directories, distribution lists, word processing documents, spreadsheets and other electronic documents.

**Litigation Hold** - a communication ordering that all records and data relating to an issue being addressed by current or potential litigation or investigation be preserved for possible production during the litigation or investigation.

**Records** - information, regardless of physical form or characteristics, that documents a transaction or activity of the district and that is created, received or retained pursuant to law or in connection with a transaction, business or activity of the District. The term includes a document, paper, letter, map, book, tape, photograph, film or sound recording, information stored or maintained electronically and a data-processed or image-processed document.

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

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

**Section 4**

**Delegation of Responsibility**

Any individual responsible for the collection, maintenance and/or security of records on behalf of the District shall comply with state and federal laws and regulations, Board policies, district procedures and the Records Management Plan.

**Records Coordinator**

In order to maintain a Records Management Plan that complies with federal and state laws and regulations and Board policy, the Board designates the Assistant to the Superintendent for Operations as the District's Records Coordinator who shall serve as the chairperson of the Records Management Committee.

The Records Coordinator shall be responsible to:

65 P.S. 67.102



**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

1. Ensure that training appropriate to the user's position and level of responsibility is provided. Such training may include:
  - a. Operation, care and handling of the equipment and software.
  - b. Requirements of the Records Retention Schedule.
  - c. Protocols for preserving and categorizing district records.
  - d. Procedures and responsibilities of district staff in the event of a litigation hold.
  - e. Identification of what is and what is not a record.
  - f. Disposal of records.
2. Review the Records Management Plan periodically to ensure that record descriptions and retention periods are updated as necessary.
3. Identify, when the retention period expires, the specific records to be disposed of and ensure that all identified records are properly disposed of annually.

Records Management Committee

A committee responsible for the development and recommendation of the District's Records Management Plan shall be established by the Board. The Records Management Committee shall give primary consideration to the most efficient and economical means of implementing the recommended Plan. Members of the Committee shall include the:

1. Open Records Officer.
2. Superintendent.
3. Board Secretary.
4. District solicitor.

Pol. 801

SC 433

**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

5. Director of Information Technology or designee.
6. Assistant to the Superintendent for Operations.

The Records Management Committee shall meet annually to evaluate the effectiveness and implementation of the Records Management Plan and recommend changes as needed.

**Section 5**

**Guidelines**

Records Management Plan

The District's Records Management Plan shall be the principal means for the storage, retention, retrieval and disposition of manual and electronic records, including emails. The Plan shall not rely primarily on backup systems to manage the retention and disposition of records.

The Records Management Plan shall include:

1. Comprehensive listing of records and data of the District.
2. Criteria to distinguish records of the school district from the supplemental personal records of individual employees.
3. System(s) of records storage and retrieval to be used, including in what form the records will be stored, maintained, reproduced and disposed.
4. Preservation measures to protect the integrity of records and reduce the risk of a data breach. Such measures shall include encryption or other appropriate security procedures.
5. Data map or flow chart detailing the sources, routes and destinations of electronic records.
6. Procedures and employee(s) designated for determining whether an item is a record.

65 P.S. 67.708  
20 U.S.C. 1232g

73 P.S. 2301 et seq  
Pol. 830, 830.1

**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

7. Procedures for adding, revising or deleting records and data, and any other details necessary to implement the Records Management Plan.
8. Records Retention Schedule.
9. Provisions for the storage and retrieval of records in the event of an emergency or disaster.
10. Staff positions authorized to access district records.
11. Procedures to be implemented in the event of a litigation hold that immediately suspends disposition of all records relevant to the current or potential claim. Such procedures shall specify:
  - a. Who can initiate a litigation hold.
  - b. How and to whom a litigation hold is communicated.
  - c. Who will determine which records are subject to the litigation hold.
  - d. Who will be responsible for collecting and preserving such records and data.
  - e. Who will be responsible for monitoring and ensuring the District's compliance with the litigation hold.
  - f. In what format the records will be collected.

Pol. 830.1

When possible, records and data shall be stored in their original form, including metadata, such as creation date, author, type of file, etc.

For any record not covered by the Records Retention Schedule, the Records Management Committee shall determine how long the record shall be kept and recommend any necessary revisions to the retention schedule.

**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

The District shall store, maintain and dispose of records in a manner that protects any sensitive, proprietary or confidential information or individual privacy rights, and helps conserve natural resources.

Manual Records

Manual records, which include all records not stored electronically, shall be retained and disposed of in accordance with the Records Management Plan.

Manual records shall be indexed in an organized and consistent manner, reflecting the way the records will be retained and referenced for later retrieval.

The district requires that all manual record systems be assessed annually and all vital information be entered into an electronic records system for long-term storage and backup recovery.

The District shall develop and maintain adequate and up-to-date documentation about each manual record system.

Documentation may:

1. List system title and responsible employee(s) or office.
2. Define the contents of the system, including record formats.
3. Identify vital records and information.
4. Determine restrictions on access and use.

Electronic Records

Electronic records shall be retained and disposed of in the same manner as records in other formats and in accordance with the Records Management Plan.

Electronic records shall be indexed in an organized and consistent manner, reflecting the way the records will be retained and referenced for later retrieval.

**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

The District shall develop and maintain adequate and up-to-date documentation about each electronic record system.

Documentation may:

1. List system title and responsible employee(s) or office.
2. Specify all technical characteristics necessary for reading or processing the records stored on the system.
3. Identify all defined inputs and outputs of the system.
4. Define the contents of the system, including records formats and database tables.
5. Identify vital records and information.
6. Determine restrictions on access and use.
7. Describe update cycles or conditions.

Email Records

Email messages, in and of themselves, do not constitute records. Retention and disposition of email messages depend on the function and content of the individual message.

Records on an email system, including messages and attachments, shall be retained and disposed of in accordance with the District's Records Management Plan.

Email messages and attachments that do not meet the definition of records shall be deleted as required by the Records Management Plan.

Email records may be maintained as an electronic record or be printed and maintained as a manual record.

For each email considered to be a record, the following information shall be retained:

1. Message content.
2. Name of sender.

**POLICY NO. 800826**  
**RECORDS MANAGEMENT PLAN**

- 3. Name of recipient.
- 4. Date and time of transmission and/or receipt.

Service Providers

The Board requires service providers contracted by the District to create, maintain, retain and dispose of district records in accordance with the Records Management Plan.

65 P.S. 67.506

Previously Revised: November 21, 2013

References:

School Code – 24 P.S. Sec. 433, 518

PA Right-To-Know Law – 65 P.S. Sec. 67.102, 67.506, 67.708, 67.901

Family Educational Rights and Privacy Act – 20 U.S.C. Sec. 1232g

Breach of Personal Information Notification Act – 73 P.S. Sec. 2301 et seq

Board Policy – 623, 801, 830, 830.1

# Policy Guide



Policy No. 800.1

Section OPERATIONS

Title ELECTRONIC SIGNATURES/RECORDS

Adopted \_\_\_\_\_

Last Revised \_\_\_\_\_

<b>POLICY NO. 800.1 ELECTRONIC SIGNATURES/RECORDS</b>		
<b>Section 1</b>	<p><b><u>Purpose</u></b></p> <p>Under certain conditions, electronic records and signatures satisfy the requirements of a manual record and/or signature when transacting business. The Board recognizes that the effectiveness of electronic records and signatures depends upon the authenticity and reliability of the signatures and the context in which the electronic records are created, transferred and stored. Therefore, the Board adopts this policy to allow for the use of and acceptance of electronic records and signatures and to establish the guidelines under which electronic signatures may be utilized by the District.</p>	73 P.S. 2260.101 et seq
<b>Section 2</b>	<p><b><u>Authority</u></b></p> <p>The Board authorizes the use of electronic signatures in place of manual signatures to conduct district business unless a manual signature is required by law or regulations. Electronic signatures shall have the full force and effect of a manual signature when used in accordance with this policy and applicable law and regulations. Only positions that are authorized by a Board Resolution may use electronic signatures on behalf of the District.</p> <p>Electronic records filed with or issued by the District shall have the full force and effect of paper records when the requirements of this policy and applicable law and regulations are satisfied.</p>	73 P.S. 2260.101 et seq.  15 U.S.C. 7001 et seq 73 P.S. 2260.301 et seq Pol. 800

	<p style="text-align: center;"><b>POLICY NO. 800.1</b> <b>ELECTRONIC SIGNATURES/RECORDS</b></p> <p>This policy applies to the use of electronic records and signatures when permitted or required in connection with district programs and operations.</p> <p><b>Section 3</b>    <b><u>Definitions</u></b></p> <p><b>Electronic record</b> – any record created, generated, sent, communicated, received, or stored by electronic means.</p> <p><b>Electronic signature</b> – an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. More simply, it is a paperless means of committing to a contract or other document in a manner that indicates the signer’s intent to bind themselves and/or the District.</p> <p><b>Section 4</b>    <b><u>Delegation of Responsibility</u></b></p> <p>The Superintendent or designee shall develop administrative regulations to direct staff on the parameters for authorized use of electronic signatures related to district programs and operations.</p> <p><b>Section 5</b>    <b><u>Guidelines</u></b></p> <p><b><u>Electronic Recordkeeping</u></b></p> <p>The maintenance of electronic records and signatures by the district shall comply with the electronic recordkeeping requirements of state and federal laws and regulations and the District’s Records Management Plan.</p> <p>Electronic records created or received by the District shall be appropriately attributed to the individual(s) responsible for their creation, authorization and/or approval.</p> <p>The District may specify the type of electronic signature required on an electronic record, the manner and format in which the electronic signature must be affixed to the electronic record, and the criteria that must be met when an individual uses a third party to file a document if electronic records must be signed by electronic means.</p>	<p>Pol. 800 15 U.S.C. 7006 73 P.S. 2260.103</p> <p>15 U.S.C. 7006 73 P.S. 2260.103</p> <p>Pol. 800</p> <p>73 P.S. 2260.502</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------



**POLICY NO. 800.1  
ELECTRONIC SIGNATURES/RECORDS**

The District shall implement and maintain electronic recordkeeping systems to securely receive, store, and reproduce electronic records and signatures relating to transactions in their original form.

73 P.S. 2260.103,  
2260.305, 2260.306

Such a system shall allow the District to implement:

1. A security procedure for the purposes of verifying that an electronic signature is that of a specific person or for detecting changes or errors in the information in an electronic record.
2. Appropriate control processes and procedures to ensure adequate preservation, disposition, integrity, security, confidentiality and auditability of electronic records.
3. A consistent manner and format in which the electronic records must be created, generated, sent, communicated, received and stored.

73 P.S. 2260.502

73. P.S. 2260.502

Electronic Signatures

An electronic signature may be used if the law requires a signature unless there is a specific law, regulation, or order that requires records to be manually signed. The issuance and/or acceptance of an electronic signature by the District shall be permitted in accordance with the provisions of this policy and all applicable state and federal laws and regulations. Such electronic signature shall have the full force and effect of a manual signature only if the electronic signature satisfies all of the following requirements:

73 P.S. 2260.101 et seq  
15 U.S.C. 7001 et seq  
21 P.S. 483.1 et seq  
Pol. 716

1. The signing employee is authorized to manually sign the document on behalf of the District.
2. The electronic signature identifies the individual signing the document by their name and position.
3. The individual signing with an electronic signature has signed a statement of exclusive use.

**POLICY NO. 800.1  
ELECTRONIC SIGNATURES/RECORDS**

4. The identity of the individual signing with an electronic signature is capable of being validated through the use of an audit trail.
5. The electronic signature and the document to which it is affixed cannot be altered once the electronic signature has been applied.
6. The electronic signature conforms to all other provisions of this policy.

The District shall maintain a secure log of each employee authorized to utilize an electronic signature in connection with district business.

This policy does not require a specific method for executing an electronic signature. The employee signing a particular document is responsible for verifying that the method chosen is appropriate for the nature of the transaction. Employees must consider confidentiality, authentication of signatures, and verification that the document signed is, in all respects, identical to the one to which the signer intends to bind the District.

Any electronic signature that appears to be forged, altered, or otherwise not authentic, or that is not compliant with law or regulation, this policy or related administrative regulation, is not a valid signature. Should an electronic signature be deemed invalid, the Superintendent or designee may require a manual signature.

All other policies that apply to the execution of contracts or other documents on behalf of the District remain in full force and effect.

Pol. 800

**POLICY NO. 800.1**  
**ELECTRONIC SIGNATURES/RECORDS**

References:

Electronic Transactions Act – 73 P.S. Sec. 2260.101 et seq,  
2260.103, 2260.301, 2260.305, 2260.306, 2260.502

Electronic Records and Signatures in Commerce – 15 U.S.C.  
Sec. 7001 et seq, 7006

Uniform Real Property Electronic Recording Act – 21 P.S. Sec.  
483.1 et set

Board Policy – 716, 800, 815

KEYSTONE OAKS SCHOOL DISTRICT

# Policy Guide



Policy No. 830

Section OPERATIONS

Title SECURITY OF COMPUTERIZED PERSONAL INFORMATION/BREACH NOTIFICATION

Adopted \_\_\_\_\_

Last Revised \_\_\_\_\_

	<b>POLICY NO. 830 SECURITY OF COMPUTERIZED PERSONAL INFORMATION/BREACH NOTIFICATION</b>	
<b>Section 1</b>	<p><b><u>Purpose</u></b></p> <p>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.</p>	
<b>Section 2</b>	<p><b><u>Authority</u></b></p> <p>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.</p> <p>The Board directs the District to provide notice as required by law to any resident of the Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.</p>	<p>73 P.S. 2301 et seq Pol. 113.4, 216, 800, 800.1, 830.1, 874</p> <p>73 P.S. 2301 et seq</p>
<b>Section 3</b>	<p><b><u>Definitions</u></b></p> <p><b>Breach of the security of the system</b> - unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information</p>	<p>73 P.S. 2302</p>

**POLICY NO. 830  
SECURITY OF COMPUTERIZED PERSONAL  
INFORMATION/BREACH NOTIFICATION**

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 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.

**Determination** - a verification or reasonable certainty that a breach of the security of the system has occurred. 73 P.S. 2302

**Discovery** - the knowledge of or reasonable suspicion that a breach of the security of the system has occurred. 73 P.S. 2032

**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. 73 P.S. 2302

**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: 73 P.S. 2302

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.
5. Health insurance information, meaning an individual's health insurance policy number or subscriber

73 P.S. 2302

73 P.S. 2302

<b>Section 4</b>	<p><b>POLICY NO. 830</b>  <b>SECURITY OF COMPUTERIZED PERSONAL INFORMATION/BREACH NOTIFICATION</b></p>	
	<p>identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.</p>	
	<p>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.</p>	
	<p>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.</p>	<p>73 P.S. 2302 Pol. 801</p>
	<p><b>Records</b> - 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.</p>	<p>73 P.S. 2302</p>
	<p><b>Redact</b> - 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]</p>	<p>73 P.S. 2302</p>
<p><b><u>Delegation of Responsibility</u></b></p>		
<p>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.</p>	<p>73 P.S. 2301 et seq</p>	
<p>The Superintendent, in collaboration with appropriate administrators, shall develop administrative regulations to implement this policy, which shall include, but not be limited to:</p>	<p>73 P.S. 2301 et seq</p>	
<ol style="list-style-type: none"> <li>1. Procedures following discovery of a breach.</li> <li>2. Procedures for the determination of a breach and whether breach notification is required under the law.</li> </ol>		

<p><b>Section 5</b></p>	<p style="text-align: center;"><b>POLICY NO. 830 SECURITY OF COMPUTERIZED PERSONAL INFORMATION/BREACH NOTIFICATION</b></p> <p>3. Breach notification procedures including timeline requirements, who must be notified and methods for such notice.</p> <p><b><u>Guidelines</u></b></p> <p>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 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.</p> <p>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.</p> <p>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.</p> <p>References:</p> <p>Breach of Personal Information Notification Act – 73 P.S. Sec. 2301 et seq, 2302, 2303, 2304</p> <p>Board Policy – 113.4, 216, 800, 800.1, 801, 830.1, 874</p>	<p>73 P.S. 2301 et seq</p> <p>73 P.S. 2303, 2304</p> <p>73 P.S. 2301 et seq</p>

# Policy Guide



Policy No. 830.1

Section OPERATIONS

Title DATA GOVERNANCE - STORAGE/SECURITY

Adopted \_\_\_\_\_

Last Revised \_\_\_\_\_

<b>POLICY NO. 830.1 DATA GOVERNANCE – STORAGE/SECURITY</b>	
<b>Section 1</b>	<p><b><u>Purpose</u></b></p> <p>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.</p> <p>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.</p>
<b>Section 2</b>	<p><b><u>Authority</u></b></p> <p>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.</p> <p>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.</p> <p>The Board directs notifications of a breach of the security of the District's computerized data system involving an individual's</p>
	<p>73 P.S. 2305.1, 2305.2</p> <p>Pol. 800</p> <p>73 P.S. 2301 et seq Pol. 830</p>



<p><b>Section 3</b></p>	<p style="text-align: center;"><b>POLICY NO. 830.1</b> <b>DATA GOVERNANCE – STORAGE/SECURITY</b></p> <p>personal information to be conducted in accordance with law and Board policy.</p> <p><b><u>Definitions</u></b></p> <p><b>Confidential Data/Information</b> - 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.</p> <p><b>Critical Data/Information</b> - information that is essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations.</p> <p><b>Data Governance</b> - the District's comprehensive system to ensure the integrity of data created, collected, stored, secured and managed by the District.</p> <p><b>Encryption</b> - 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.</p> <p><b>Personal Information</b> - 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:</p> <ol style="list-style-type: none"> <li>1. Social Security number.</li> <li>2. Driver's license number or state identification card number issued instead of a driver's license.</li> <li>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.</li> <li>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.</li> </ol>	<p>Pol. 113.4, 216, 874</p> <p>73 P.S. 2302</p> <p>Pol. 830 73 P.S. 2302</p> <p>73 P.S. 2302</p>
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

<p><b>Section 4</b></p>	<p><b>POLICY NO. 830.1</b>  <b>DATA GOVERNANCE – STORAGE/SECURITY</b></p>	
	<p>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.</p>	<p>73. P.S. 2302</p>
	<p>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.</p>	
	<p>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.</p>	<p>73 P.S. 2303  Pol. 801</p>
	<p><b>Records Management Plan</b> - the system implemented by the district for the storage, retention, retrieval and disposition of all records generated by district operations.</p>	<p>Pol. 800</p>
	<p><b>Records Retention Schedule</b> - a comprehensive listing stating retention periods and proper disposition of records.</p>	<p>Pol. 800</p>
	<p><b><u>Delegation of Responsibility</u></b></p>	
	<p>The Superintendent, in coordination with the Assistant to the Superintendent for Operations shall develop procedures necessary to implement this policy.</p>	
<p>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.</p>	<p>Pol. 623, 830</p>	
<p>The Assistant to the Superintendent for Operations or designee shall conduct regular vulnerability and risk assessments to monitor the integrity of the district's system of data governance.</p>		
<p>The Superintendent shall ensure that this policy is reviewed at least annually and updated as necessary.</p>	<p>73 P.S. 2305.1,  2305.2</p>	

<p><b>Section 5</b></p>	<p style="text-align: center;"><b>POLICY NO. 830.1</b> <b>DATA GOVERNANCE – STORAGE/SECURITY</b></p> <p><b><u>Guidelines</u></b></p> <p>The District's system of data governance shall include, but not be limited to, the following:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Training requirements for individuals who have access to confidential and/or critical data and information.</li> <li>4. Provisions to minimize the risk of unauthorized access, alteration or erasure of computerized data.</li> <li>5. An inventory of all software applications, digital tools and platforms, and related instruments comprising the data governance system.</li> <li>6. Procedures for addressing a breach of data and cybersecurity incidents.</li> <li>7. Procedures and acceptable use provisions for access to data and protection of privacy and personal information for students, staff and district residents.</li> <li>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.</li> </ol> <p><b><u>Use of Personal Electronic Devices and Resources</u></b></p> <p>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</p>	<p>Pol. 830</p> <p>Pol. 830</p> <p>Pol. 816, 830</p>

	<p style="text-align: center;"><b>POLICY NO. 830.1</b> <b>DATA GOVERNANCE – STORAGE/SECURITY</b></p> <p>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.</p> <p><u>Service Providers</u></p> <p>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.</p> <p>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.</p> <p><u>Consequences</u></p> <p>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:</p> <ol style="list-style-type: none"> <li>1. Employees may be disciplined up to and including termination.</li> <li>2. Volunteers may be excluded from providing services to the District.</li> <li>3. The termination of a business relationship with a service provider.</li> </ol> <p>References:</p> <p>Breach of Personal Information Notification Act – 73 P.S. Sec. 2301 et seq, 2302, 2305.1, 2305.2</p> <p>Board Policy – 113.4, 216, 623, 800, 801, 816, 817, 818, 830, 874, 916</p>	<p>Pol. 800, 830</p> <p>Pol. 817, 818, 916</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------