



DATA PRIVACY PROCEDURES

I. Our Responsibility:

Everyone at Sumner-Bonney Lake School District plays a crucial role in safeguarding sensitive information. This includes:

- **Protecting confidentiality:** Keeping personal information private and preventing unauthorized access.
- **Following security procedures:** Implementing measures to secure sensitive data, both electronically and physically.
- **Using information appropriately:** Accessing and using personal information only for legitimate work purposes.
- **Artificial intelligence (AI):** Adhering to the guidelines for electronic use, AI, and internet safety outlined in Procedure 2022P – Electronic Resources and Internet Safety.

II. What is Personal Information?

For the purpose of this policy and procedure, "personal information" refers to any data that can be used to identify an individual, such as:

A. Primary Identifiers

The District will implement strict access controls and security measures to safeguard primary identifiers, which directly identify an individual which may include:

- Employee ID Number
- Social Security number
- Driver's license number
- Date of birth
- Contact details (Home address, Phone number, Email)
- Student ID Number
- Parent/Guardian's Name
- Parent/Guardian's contact Information (Home address, Phone number, Email)
- Financial Account Information



B. Secondary Identifiers

The District recognizes that secondary identifiers, when combined with other readily available information, can be used to identify an individual. Therefore, the District will also protect secondary identifiers which may include:

- Medical information
- Leave status
- Disability accommodations
- Performance evaluations
- Background checks
- Disciplinary actions
- Wages and benefits
- Transcripts
- Attendance records
- Training Records
- Gender

III. Securing Personal Information:

The following procedure and protocols shall be used to the extent possible to ensure that personnel records are not lost/stolen and that unauthorized persons do not gain access to these records.

A. Electronically:

- **Password Security:** To ensure the security of district accounts and protect personally identifiable information, all users must adhere to the following password requirements, which may be modified by grade level to accommodate the developmental needs of students:
 - **Length:** Passwords must be at least 15 characters long.
 - **Character Choice:** Use a mix of characters that are memorable to you. Longer passphrases are encouraged. All ASCII characters, including spaces, are allowed.
 - **Password Reuse:** You may not reuse any of your previous 5 passwords.
- **Multi-Factor Authentication (MFA):** All staff are required to have MFA enabled on their district accounts using one of the district's approved MFA methods.
- Electronic records containing personally identifiable information will be redacted before disclosure, unless required by law or with written consent.



- Store confidential electronic data on the district network only. Use district-approved cloud services that meet security standards.
- Never share usernames and passwords with anyone, as the owner of the username will be held responsible for all system activity, unless you have advanced written permission from the Technology Services Department.
- Do not leave laptops or devices containing personal information unattended.
- Do not use the “remember password” feature in Internet browsers.
- Do not insert passwords into email, documents, or other forms of communication.
- Do not store electronic personal information on unencrypted or non-password protected USB devices or computers.
- Do not leave browser windows and applications that may contain access to sensitive/PII data open overnight or on weekends.
- Extra sensitive/confidential data (medical information, social security numbers) should only be accessed on a computer/laptop issued from the District, or via an approved remote desktop connection to a district device utilizing the District’s secure VPN.
- Any Staff configured for VPN access will use the district’s VPN with Multi-Factor Authentication (MFA) enabled when accessing information systems/services when they are not located within the district.
- To access District information systems/services while traveling outside of the United States you must inform the Technology Services Department with the below information. Use of the District’s VPN should be used by approved staff members. Failure to do so prior to travel may result in no access.
 - Include your name.
 - Include start and stop date of travel.
 - Include the name of country or select country code where you will be traveling.

B. Physically:

- Physical documents containing personally identifiable information will be redacted before copying or disclosure, unless required by law or with written consent.
- Use screen locks (i.e., control-alt-delete to lock computer) and secure office doors/file cabinets.
- Do not leave paper records unattended or in plain sight.
- Shred or recycle documents containing personal information securely.
- Be mindful of your surroundings when discussing confidential information verbally.
- Immediately pick up print jobs when using a shared printer for personal information, or print with a security code.
- Do not leave laptops, USB devices, or other equipment that contains personal information in an unattended vehicle (leave at home, work, or keep them with you)



C. AI Systems:

- **Inventory:** The district will maintain an inventory of all AI systems approved for district use that process personal data. This inventory will include:
 - The name of the AI system.
 - The purpose of the AI system.
 - The types of data used.
 - Data sources.
 - Data retention policies.
 - Any relevant vendor information such as contact information in case of a security related event.
- **Data Minimization and Purpose Limitation:**
 - Collect only the minimum necessary student data for the specified education purpose of the AI tool.
 - Clearly define how the AI tool will be used and what data is needed.
- **Access Controls and Encryption:**
 - Implement strict access controls to limit who can access student data within AI systems.
 - Use strong authentication methods to prevent unauthorized access.
 - Encrypt student data both in transit and at rest when possible.
- **De-identification and Anonymization:**
 - Remove identifying information from student data whenever possible.
 - Consider anonymizing data so that it cannot be linked back to individuals.
- **Vendor Due Diligence:**
 - Carefully vet third-party AI vendors to ensure they meet the district's data privacy and security standards.
 - Establish data sharing agreements that specify security requirements whenever possible.
- **Monitoring and Auditing:**
 - Regularly monitor AI systems to ensure they are functioning as intended and that data is being handled responsibly.
 - Conduct periodic audits to assess the security and privacy of AI systems.

IV. Sharing Personal Information:

- When sharing personally identifiable information with authorized third parties, the District will ensure that PII is redacted to the extent necessary to protect the privacy of individuals, unless otherwise required by law or with written consent.
- Only share personal information with authorized individuals who have a legitimate business need to know.



- Obtain written consent before disclosing student education records, as required by FERPA.
- Follow district policies and procedures for responding to data breach incidents.

V. Protecting Sensitive Payment Information

The following procedures for handling **cardholder data (CHD)**, which is any information used to process payments. It also defines **sensitive authentication data (SAD)**, which is additional data used during transactions but not stored.

A. CHD includes:

- **Primary Account Number (PAN):** The 15- or 16-digit number on your card.
- **Additional Information:** When stored with the PAN, the cardholder name, expiration date, and service code are also considered CHD.

B. SAD includes:

- Personal Identification Numbers (PINs)
- Encrypted PIN blocks
- Full magnetic stripe data
- Card verification codes (CVVs) and similar chip data

VI. This Procedure applies to:

- Anyone who handles CHD or works with systems that store, transmit, or process CHD (employees, students, contractors).
- All systems or processes that handle CHD.

VII. District Requirements

- **Encryption:** Encrypt PAN data both while in transit (e.g., online) and at rest (when stored).
- **Device Security:** Secure all equipment containing sensitive information to prevent theft. Do not store sensitive data on unencrypted mobile devices.
- **Remote Access:** Use secure protocols (SSH or VPN) for remote connections to the District network.

VIII. Employee Requirements

- Unencrypted Credit Card Account Numbers (PAN) must not be sent via email, instant message, or chat applications.
- No unencrypted Credit Card data will be stored, processed, or transmitted, within the district's environment.

District Procedure 6501P, Page 5 of 6

Adopted: 7/10/2024

Revised : 02/2025



- Encrypted Credit Card Data will be transmitted only within the designated Payment Card Industry (PCI) environment.

IX. Credit Card Data Retention

- CHD may not be retained for any reason.

X. Reporting Data Security Incidents:

Prompt reporting is crucial for mitigating the impact of data security incidents. By following these steps, you can help protect the district and individuals affected.

- Immediately report any theft or inappropriate disclosure of personal information or CHD to your supervisor and to cybersec@sumnersd.org.
For system wide data breaches and/or loss of equipment containing personal information, you must also contact the Sumner-Bonney Lake Technology Services Department at (253)891-6111.