Superintendent Procedure 6501SP
Series: 6000 – Management Support
Approved By: Dr. Brent C. Jones, Superintendent

6501SP Data Privacy

All district employees and other authorized individuals, including third parties granted access to personal information, are responsible for ensuring sensitive records, files, and data, whether verbal, electronic, or paper, are secured to ensure the privacy and confidentiality of personal information.

For purposes of this procedure, **personal information** includes, but is not limited to: medical information, leave status, Americans with Disabilities Act (ADA) and/or Section 504 accommodation requests, performance evaluations, background check results, investigation reports, disciplinary actions, wages, garnishments, transcripts, interview notes, personal home or cellphone numbers, home address, personal email addresses, emergency contact information, social security number, district ID number, state identification card or driver's license number, date of birth, biometric data, mother's maiden name, tax information, and bank account/routing numbers.

Sensitive records or **sensitive data** include but are not limited to personal information, as described above, as well as any non-personally identifiable information that, if assembled together, would allow a reasonable person to identify an individual.

Many departments have access to and use personal information and other sensitive records for business and/or educational purposes. Sensitive records will only be used for a legitimate business purpose with reasonable security precautions.

Board Policy No. 5260, Personnel Records, requires that staff maintain personnel records and files in a secure location, and Board Policy No. 3231, Student Records, requires that student and education records be treated in a confidential and professional manner. Each of these policies also has a corresponding procedure that further details requirements for the handling of district records and confidential information as do numerous additional School Board policies and procedures, including, but not limited to those listed as additional resources below.

Protocols to Secure Records

The following protocols should be used by all district employees and authorized users to the extent possible to ensure that sensitive records are not lost/stolen and that unauthorized persons do not gain access to these records.

- Use screen locks (i.e., control-alt-delete), close or lock office doors, lock file cabinets at the end of the day or at all times if in an unsupervised area, and use privacy filters, if applicable.
- Do not leave records unattended or in plain view on a desk or in other locations (e.g., a conference room or break room), unless it is a private office, or a door can be locked.
- Immediately pick up print jobs when using a shared printer for personal information or print with a security code.
- Return personal information when no longer needed. If you are responsible for personnel information, review the document retention requirements for public records. Contact the Archives Department (Archives@seattleschools.org) for document retention questions.
- When appropriate or possible, remove identifiable personal information from reports prior to sharing reports with others.
- Try to discuss confidential information and sensitive records in a private setting. For example, it is better to perform an annual performance evaluation in a closed office or conference room when possible.
- Use only district-approved data sharing agreements and ensure proper approvals are in place. The School and Community Partnerships Department maintains a data-sharing agreement process for community-based organizations accessing student level data. Check with the district's Legal Department and Department of Technology Services (Cybersecurity@seattleschools.org) for potential data security implications prior to entering into a contract or data-sharing agreement with a third party. Additional School Board policies and procedures and departments also may apply.
- Do not release personnel records to non-district employees unless you are authorized as part of your job or required by law.

Storage Guidelines

- Store sensitive data and records on the district's network. Use of the district's network is to support educational objectives and job responsibilities. (See the Seattle Public Schools Network Use/Access Agreement for more information regarding employee expectations for use of this service.) Do not save medical information or social security numbers on any personal home computer or device.
- Particularly sensitive records or data (medical information, social security numbers) should only be accessed on a computer or laptop issued from the district, or via an approved remote desktop connection to a district device.

- Do not store electronic personal information on unencrypted or non-password protected USB devices or computers.
- Do not share usernames and passwords with anyone, as the owner of the username will be held responsible for all system activity, unless you have advance written permission from the Department of Technology Services.
- 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).
- Cloud-based services are vetted and must be approved by the Department of Technology Services prior to implementation. This approval will ensure that the service has the necessary security and safety protections for all sensitive data. Any sensitive data accessed or shared electronically through a cloud service should adhere to the following guidelines/rules:
    - Do not store sensitive data on an unauthorized cloud service, including artificial intelligence (AI) cloud-based tools.
    - Verify the list of approved cloud-based services with techline@seattleschools.org. Be aware the list is updated frequently.
    - It is permissible to use cloud-based services to analyze or share aggregate, non-identifiable data.

Examples of Violations of Sensitive Data Handling Protocol

Examples of violations of the district's sensitive data handling protocol include, but are not limited to, the following:

- Leaving documents in plain sight or screens open that contain sensitive data in a shared, open, or easily accessible space.
- Accessing a personnel record to provide a home address or birthdate for a colleague to send an employee a greeting card. Accessing staff or student electronic records must be done for a legitimate business purpose.
- Disclosing your password(s) to the network or other restricted software, without advance permission from the Department of Technology Services.
- Verifying personal information to either an employee or a third party without a completed authorization.

Reporting Violations

Staff violations of the policy and/or sensitive data handling protocol may result in disciplinary action up to and including termination. Staff who are concerned that a violation may have occurred should contact their supervisor. Reports also can be made directly to Human Resources by emailing employeemisconduct@seattleschools.org or online. Human Resources should be contacted directly if the employee's supervisor and/or evaluator is the subject of the report.

When Sensitive Data Can be Released

The district may be required to comply with a lawfully issued subpoena or a request under the Public Records Act, and some information from personnel records and other sensitive records may be disclosable under state law. If you have questions about such disclosure, please contact the district's Public Records Office (publicrecords@seattleschools.org).

Under The Family Educational Rights and Privacy Act of 1974 (FERPA), a school may not generally disclose personally identifiable information from an eligible student's education records to a third party unless the parent/guardian or eligible student has provided written consent. However, there are exceptions to FERPA's general prohibition against non-consensual disclosure of personally identifiable information from education records. Under these specific exceptions, schools are permitted to disclose personally identifiable information from education records without consent, though they are not required to do so. Additional School Board policies and procedures, including many listed as additional resources below, support district compliance with FERPA requirements.

Credit Card Data and Handling

Credit Cardholder Data (CHD) are sensitive records used to process payment card transactions. CHD consists of the following data:

- The Primary Account Number (PAN), which is the 15- or 16-digit number on the front of credit and debit cards. All PANs are considered CHD.
- The cardholder's name, expiration date, and/or service code also are considered CHD when they are stored with a PAN.

Sensitive Authentication Data includes additional data that may be transmitted or processed as part of a payment transaction but may not be stored at any time. Sensitive Authentication Data includes:

- Personal Identification Numbers (PIN)
- Encrypted PIN blocks
- Full contents of any track from the magnetic stripe on the back of the card
- Card verification codes (three- or four-digit card-verification code or value printed on the front of the card or the signature panel) or equivalent data on a chip.

Credit card records and handling requirements detailed in this procedure apply to all:

- Systems or processes that store, transmit, or process CHD

- Employees and contractors who handle CHD or who work with systems that store, transmit, or process CHD

Requirements for Credit Card Data Handling**:**

- PAN data must be encrypted with point-to-point encryption (P2PE) while in transit on public networks (e.g., the Internet) and rendered unreadable when at rest. If encryption is used to render PAN unreadable while at rest, the encryption must meet the minimum encryption standard set forth in the Department of Technology Services IT Security Handbook, which states:
  - Seattle Public Schools shall ensure that all equipment that contains sensitive information will be secured to deter theft. No sensitive data shall be retained on any mobile devices unless that device is encrypted in accordance with the Washington State Security Office's Best Practices.
  - Seattle Public Schools shall ensure that any remote access with connectivity to the district's internal network is achieved using following encryption protocols: Secure Shells (SSH) or virtual private network (VPN) (Layer 2 Tunneling Protocol - L2TP/ Internet Protocol Security - IPSEC).
- Unencrypted Credit Card Account Numbers (PAN) must not be sent via email, instant message, or chat applications.
- No unencrypted CHD will be stored, processed, or transmitted within the district's environment.
- Encrypted CHD will be transmitted only within the designated Payment Card Industry (PCI) environment.
- CHD may not be retained for any reason.

Reporting Disclosure

Immediately report any data theft or inappropriate disclosure of personal information or CHD to your supervisor and to cybersecurity@seattleschools.org. For system-wide data breaches and/or loss of equipment containing personal information, you must also contact the Department of Technology Services at techline@seattleschools.org or 206-252-0333. This includes but is not limited to loss, or theft of files, laptops, hard drives, flash drives, or other storage devices.

Responsibilities of Information Technology Security Officer

The Superintendent or their designee will designate an Information Technology Security Officer (ISO) responsible for maintaining the security of district information technology (IT) including reviewing and making recommendations for implementation of and updates to applicable policies and procedures. The ISO will support the implementation of IT security controls within the Department of Technology Services and in collaboration with schools and divisions across the district and will ensure all district employees have access to annual IT security training. The ISO will maintain an IT Security Handbook containing technical security standards for implementation as an administrative procedure of the Department of Technology Services.

Applicable Policies & Procedures

- Board Policy No. 6501, Data Privacy Policy
- Board Policy No. 2022 and Superintendent Procedure 2022SP, Electronic Resources/Use of the Internet
- Board Policy No. 2080, Assessment
- Board Policy No. 3231 and Superintendent Procedure 3231SP, Student Records
- Board Policy No. 3232 and Superintendent Procedure 3232SP, Parent/Guardian & Student Rights in Administration of Surveys, Analysis or Evaluations
- Board Policy No. 3520 and Board Procedure 3520BP, Student Fees, Fines, or Charges
- Board Policy No. 4265 and Superintendent Procedure 4265SP, School and Community Partnerships
- Board Policy No. 4020, Confidential Communications
- Board Policy No. 4040 and Superintendent Procedure 4040SP, Public Access to District Records
- Board Policy No. 4070, Archives and Records Management, and Superintendent Procedure 4070SP, Electronic Records Management
- Board Policy No. 4280 and Superintendent Procedure 4280SP, Research Activity
- Board Policy No.5006, Unprofessional Conduct of Staff
- Board Policy No. 5230, Job Descriptions/Responsibilities
- Board Policy No. 5251, Ethics
- Board Policy No. 5260 and Superintendent Procedure, Personnel Records
- Board Policy No. 5281, Staff Disciplinary Action & Discharge
- Board Policy No. 6220, Procurement and corresponding Superintendent Procedures

Additional Resources

- **District Resources**
  - Seattle Public Schools Information Technology Security Handbook (available to staff on the MySPS internal website)
  - Staff Network Use Agreement (available to staff on the MySPS internal website)

  - School and Community Partnerships Department – Data Access for Partners
  - Legal Department – Public Records Requests
  - Research and Evaluation Department – Data Available for Research
  - Human Resources – Verification of Employment

- **External Resources**
  - Federal Trade Commission – Children's Online Privacy Protection Act (COPPA): Complying with COPPA: Frequently Asked Questions
  - U.S. Department of Education
    - Student Privacy at the U.S. Department of Education
    - Family Educational Rights and Privacy Act (FERPA)
    - What is the Protection of Pupil Rights Amendment (PPRA)?
    - Individuals with Disabilities Education Act (IDEA)

Policy Cross References:

- 6501 – Data Privacy

Revisions:

- March 18, 2025
- June 8, 2024
- June 17, 2019

Adopted:

- January 27, 2017