STUDENT DATA SECURITY PROCEDURE

This procedure applies to school district employees including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive student information. In addition, some third parties such as contractors or vendors, may be required to abide by parts of or in whole this policy as indicated in contractual requirements.

This procedure contains the following five sections pertaining to student data security:
A. Authorization and Authentication Mechanisms for Assessing Student Data B. Administrative, Physical and Logical Security Safeguards, Including Employee Training and Data Encryption C. Privacy and Security Compliance D. Processes for Identification of and Response to Data Security Incidents, Including Breach Notification and Mitigation Procedures E. Standards for Retention and Verified Destruction of Student Data

Failure to comply with this or any other security policy will result in disciplinary actions up to and including termination of employment. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

SECTION A: Authorization and Authentication Mechanisms for Assessing Student Data

1. Access Authorization 2. Assigned Security Responsibility 3. Automatic Log-off 4. Password Management 5. Unique User Identification

1. ACCESS AUTHORIZATION

Access Authorization refers to granting access to sensitive information, to include but not limited to student data and other sensitive information. This includes, for example, authorization required to access a workstation, transaction, program, process or other mechanism.

The individual's job description must be reviewed to determine their:

- Individual rights
- The group that this individual belongs to

The principle of least privilege and separation of duties shall be factors that influence the access rights granted to an individual or a group. The fundamental principle of "need to know" will be applied within the District to determine access privileges. Access to sensitive information will be granted only if that individual has a legitimate business need for the information. Reasonable efforts will be made to limit the amount of

information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

2. ASSIGNED SECURITY RESPONSIBILITY

Assigned Security Responsibility refers to the individual who is responsible for the development and implementation of the policies and procedures required by the School District. This individual's ultimate goal is to protect the confidentiality, integrity, and availability (CIA) of critical information assets at the School District and to ensure compliance with the impacted regulations. The School District will assign final responsibility of security to the individual employed in the position of Technology Director for purposes of data and other technology security issues.

Responsibilities of the Technology Director include (but are not limited to):

- Ensuring all policies, procedures, and plans required by regulations are developed, implemented, and maintained as necessary
- Monitoring changes in legislation that may affect the School District and its security position
- Monitoring changes and advances in technology that may affect the School District and its security position
- Performing technical and non-technical evaluations or audits on security processes in order to find and correct weaknesses and guard against potential threats to security
- Acting as an internal consultant and external spokesperson for the School District in all issues related to security
- Ensures a system for reporting and responding to security incidents (as well as violations of regulations)
- Encourage, on an ongoing basis, security awareness to school district employees

If the Technology Director is not able to meet the requirements of this policy, or is no longer affiliated with the organization, the District will assign these responsibilities as directed by the Superintendent.

3. AUTOMATIC LOGOFF

Automatic Logoff refers to implementing electronic procedures that terminate an electronic session after a predetermined time of inactivity.

The School District will maintain procedures for Automatic Logoff of systems that contain sensitive information after a period of inactivity. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the system is located.

The School District will periodically inspect systems to ensure that the automatic session logoff capability is configured correctly.

4. PASSWORD MANAGEMENT

The School District requires
that:

• Passwords used on District related sites must be different than passwords used on personal accounts or equipment

Users must select strong passwords. Example characteristics of strong passwords are:

• At least six characters in length
• A mixture of letters and numbers
• Not a word, sequence, or pattern
• Different from the previous 6 passwords
• Not contained in the user's user id
• Unique to each system

Where applicable, systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

Members of the workforce must follow these guidelines for passwords:

• Don't reveal a password over the phone to ANYONE
• Don't reveal your password in an e-mail message
• Don't talk about a password in front of others
• Don't hint at the format of a password, like, "my family name"
• Don't reveal a password on questionnaires or security forms
• Don't share a password with others

If someone demands a password, refer them to this document or have them call the Director of Technology. Members of the workforce must not write passwords down or store them where they can be accessible to others. All passwords are to be treated as sensitive, confidential information.

5. UNIQUE USER IDENTIFICATION POLICY

Unique User Identification refers to assigning a unique name and/or number for identifying and tracking user identity. Each individual that accesses sensitive information will be granted some form of unique user identification, such as a login ID. At no time will any school district employee allow anyone else to use his or her unique ID.

The District has a standard convention for assigning unique user identifiers. The District maintains a secure record of unique user identifiers assigned.

SECTION B: Administrative, Physical and Logical Security Safeguards, Including Employee Training and Data Encryption

1. Audit Controls 2. Email Security 3.

Facility Access Controls 4. Information System Activity 5. Network Security 6. Portable Device 7. Protection and Malicious Software 8. Remote Access 9. Security Awareness and Training 10. Termination Procedure 11. Wireless Security 12. Workstation Security

1. AUDIT CONTROLS

Audit Controls refers to the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.

Audits may be conducted to:

• Ensure confidentiality, integrity, and availability of sensitive information

• Investigate possible security incidents and ensure conformance to the School District security policies

• Monitor user or system activity where appropriate

The School District will identify critical systems that require event auditing capabilities. The School District will define the events to be audited on all such systems. At a minimal, event auditing capabilities will be enabled on all systems that process, transmit, and/or store sensitive information. Events to be audited may include, and are not limited to, logins, logouts, file accesses, and deletions and modifications.

The School District will ensure the protection of all audit reports and log files. The School District will review the usage of software and application tools to review audit files.

When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of the School District's Technology department.

This access may include:

• User level and/or system level access to any computing or communications device

• Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on the School District's equipment or premises

• Access to work areas (labs, offices, cubicles, storage areas, and so on)

• Access to interactively monitor and log traffic on the School District's networks

2. EMAIL SECURITY

Email Security refers to protecting the confidentiality and integrity of sensitive information that may be sent or received via email.

The District recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages. The District will evaluate emerging encryption solutions for email and implement them.

The District provided e-mail systems are intended for official and authorized purposes only. E-mail messages are considered by the School District to be company property. Therefore, e-mail equipment operated by or for School District staff is subject to the same restrictions on their use as any other company furnished resource provided for use by school district employees.

Electronic information about an individual should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.

E-mail system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate School District management officials. However, School District officials will have access to e-mail messages whenever there is a legitimate purpose for such access, e.g., technical or administrative problems.

3. FACILITY ACCESS CONTROLS

Facility Access Controls refers to implementation of procedures to limit physical access to the District's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

The School District will safeguard the facility and equipment from unauthorized physical access, tampering and theft. The District will continually assess potential risks and vulnerabilities to sensitive information and develop, implement and maintain appropriate safeguards to ensure compliance with the requirements of the impacted regulation.

All repairs and modifications to the physical components of the facility shall be documented and maintained by the District. Maintenance of all hardware and software will be reviewed regularly.

4. INFORMATION SYSTEM ACTIVITY REVIEW

Information System Activity Review refers to regularly reviewing records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The District will clearly identify all critical systems that process sensitive information. The District implements security procedures to review records of information system activity on critical systems that process sensitive information.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible, of the following, as reasonable and appropriate:

• User IDs
• Dates and times of log-on and log-off
• Terminal identity, IP address and/or location, if possible
• Records of successful and rejected system access attempts

Agreement with vendors must be deployed to protect against unauthorized changes and operational problems.

The District's Technology Director will clearly identify:
• The systems that must be reviewed
• The information on these systems that must be reviewed
• The types of access reports that are to be generated
• The security incident tracking reports that are to be generated to analyze security violations
• The individual(s) responsible for reviewing all logs and reports

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

5. NETWORK SECURITY

Network Security refers to secure communication devices and data on the School District network.

School District will:
• Use encryption as much as possible to protect data
• Use firewall(s) to secure critical segments
• Deploy Intrusion Prevention Systems (IPS) on all critical segments
• Disable all services that are not in use or services that have use of which you are not sure
• Use wrappers around all services to log their usage as well as to restrict connectivity

6. PORTABLE DEVICES

Portable Devices refers to any mobile device that is capable of storing or transmitting sensitive information. Sensitive information may only be stored on portable systems if appropriate encryption mechanism(s) are installed on the device. Strong password controls must be implemented for all users of portable devices. When working on portable devices from a remote location, including from home, only secure connections must be used to access sensitive information. Protection against malicious software should be in place and be kept up to date. Devices must be configured to automatically

logoff users according to the procedure EHA-R (Automatic Logoff) (For example, any website that contains student data has HTTPS in the web address.)

7. PROTECTION FROM MALICIOUS SOFTWARE (MALWARE)

Protection from Malicious Software refers to procedures for guarding against, detecting, and reporting Malware. The District's IT department will ensure all operating systems are up to date and running all supported versions which would ensure that the systems are running the latest malware protection from the vendors.

The District will provide security training that will include information on:

- Potential harm that can be caused by malicious software
- Prevention of malicious software such as viruses
- Steps to take if a malicious software such as a virus is detected

8. REMOTE ACCESS

Remote Access refers to implementing security measures sufficient to reduce risks and vulnerabilities of remote access connections to the School District's enterprise infrastructure.

The School District remote access infrastructure follows these guidelines:

- It is the responsibility of School District employees, contractors, vendors and agents with remote access privileges to the School District's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the School District.
- Secure remote access must be strictly controlled. Control will be enforced by using strong passwords.
- At no time should any School District employee provide his or her remote access login or password to anyone.
- All hosts that are connected to School District internal networks via remote access technologies must use the most up-to-date software.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the School District production network must obtain prior approval from the Director of Technology.

9. SECURITY AWARENESS AND TRAINING

School district employees will be trained how to identify, report, and prevent potential security incidents. Periodic security reminders will keep school district employees up to date with new threats, such as computer viruses or "scams" to watch out for. The Technology Director will determine the frequency of these reminders.

10. TERMINATION PROCEDURE

Termination Procedure refers to implementing procedures for quickly, securely and appropriately terminating access to sensitive information when the employment of a school district employee ends.

Upon termination, the District will ensure:

- Password access is immediately revoked
- Access to all systems and applications is revoked (including email)
- The school district employee is removed from any systems or applications that processed sensitive information
- Any keys and IDs provided to the school district employee during their employment are returned
- The school district employee is not provided any access to their desk or office. Any such access, if provided, must be limited and carefully supervised.

11. WIRELESS SECURITY

Wireless Security refers to implementing security measures sufficient to reduce risks and vulnerabilities of the School District's wireless infrastructure.

School District wireless infrastructure must follow these guidelines: Design

- Ensure that 128-bit or higher encryption is used for all wireless communication
- Fully test and deploy software patches and updates on a regular basis
- Deploy Intrusion Protection Systems (IPS) on the wireless network to report suspected activities

Access Points (AP*)*

- Place APs in secured areas to prevent unauthorized physical access and user manipulation
- Ensure that all APs have strong administrative passwords
- Enable user authentication mechanisms for the management interfaces of the AP
- Use SNMPv3 and/or SSL/TLS for Web-based management of APs
- Turn on audit capabilities on AP; review log files on a regular basis

12. WORKSTATION SECURITY

Workstation Security refers to implementing physical safeguards for all workstations that access sensitive information and to restrict access to authorized users. Physical safeguards will be implemented for all workstations that access sensitive information to restrict access to authorized users only.

All workstations must be operated in a manner that ensures:

• Confidentiality of sensitive information

• Employment of a password protected screen saver and/or workstation locking mechanism when the workstation is unattended

• Proper log off or shut down of workstations at the end of the business day

• Routine back up of all critical data

• Only approved software may be used on School District's systems

• Workstations and said software is used in accordance with contract agreements and copyright laws

SECTION C: Privacy and Security Compliance

1. Information Classification 2. Risk Management

1. INFORMATION CLASSIFICATION

Information Classification is intended to assist employees of the District make decisions regarding what information may and may not be released to the public or disclosed to any individual outside of the organization. All School District information will be organized into two main classes. These classes are "Public" and "Confidential."
Public information is information that can be shared freely with anyone inside or outside of the organization without the possibility of negative consequences. Public information includes, but is not necessarily limited to:

• General information about School District such as the mission statement

• Most marketing information

Confidential information includes all other information, such as sensitive information, (information that, when shared or disclosed, could possibly have a negative consequence). It is understood that there are varying levels of sensitive information, and the lengths employees should go to protect the information depends on the sensitivity.

The School District will rely on the professional judgment of the individual on a daily basis when using and disclosing confidential information. If an individual is unsure of the relative sensitivity of a piece of information, they should contact their supervisor.

Confidential information includes, but is not necessarily limited to:

• Business information

• Financial information

• Operational information

• Most personnel information

• Student Data

If the sensitivity of the information is not readily apparent, the creator of the document may mark the document as “School District Confidential” in a prominent location.

2. RISK MANAGEMENT POLICY

Risk Management refers to implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce the risk to an acceptable level. Risk management related activities are essential to help identify critical resources needed to support School District and the likely threat to all such resources. The principal goal of the School District’s risk management procedure is to protect the organization, especially its sensitive information, and its ability to perform its mission.

Risk management consists of three phases:

- Phase I: Risk Assessment
- Phase II: Risk Mitigation
- Phase III: Evaluation and Assessment (Residual Risk)

The activities that the School District will conduct in each phase are as follows:

Phase I: Risk Assessment

- System characterization
- Threat identification
- Vulnerability identification
- Safeguard analysis
- Likelihood determination
- Impact analysis
- Risk Determination
- Safeguard recommendations
- Results documentation

Phase II: Risk Mitigation

- Prioritize actions
- Evaluate recommended safeguard options
- Conduct cost-benefit analysis
- Select safeguards
- Assign responsibility
- Develop safeguard implementation plan
- Implement selected safeguards

Phase III: Evaluation and Assessment (Residual Risk)

- Evaluate safeguards deployed
- Evaluate security policies

SECTION D: Processes for Identification of and Response to Data Security Incidents, Including Breach Notification and Mitigation Procedures

1. Applications and data criticality analysis 2. Contingency operations 3. Contingency Plan 4. Data Breach Management 5. Response and Reporting 6. Security Incident Procedures

1. APPLICATIONS AND DATA CRITICALITY ANALYSIS

Applications and data criticality analysis refers to assessing the relative criticality of specific applications and data in support of other contingency plan components.

The School District should assess the "critical" areas of the business, which would include:

- Critical business functions
- Critical infrastructure
- Critical sensitive information or records

The specific components of applications and data criticality analysis must include:

- Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers and system interdependencies
- Identification and analysis of critical business processes surrounding sensitive information
- Identification and analysis of key applications and systems used to support critical business processes
- Adequate redundancies within the network infrastructure to reduce or eliminate single points of failure
- Mitigating controls or work-around procedures in place and tested for single points of failure that are unable to be eliminated

2. CONTINGENCY OPERATIONS

Contingency operations refers to establishing and implementing procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

The School District will develop a contingency operation plan to address emergency response. These procedures will include:

- Notification

• Evacuation
• Equipment tests
• Training
• System shutdown

For example, the area of emergency notification procedures would include activities such as:
• Contacting the Emergency Response Team (ERT) Leader
• Contacting Administrators
• Evacuate the building if required
• Conduct a damage assessment
• Create damage assessment report and communicate to senior management
• Determine if the damaged site can be repaired and used
• Establish time objectives for activities

3. CONTINGENCY PLAN

Contingency plan refers to establishing and implementing procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain sensitive information.

A contingency plan is a routinely updated plan for responding to a system emergency that includes performing backups, preparing critical facilities, and appropriately detailed migration plans that can be used to facilitate continuity of operations in the event of an emergency and recovering from a disaster.

The District will develop contingency plan documents to identify core activities in the areas of Data Backup Plan, Disaster Recovery Plan, Emergency Mode Operation Plan, Testing and Revision, and Applications and Data Criticality Analysis.

The District will develop and implement a contingency plan to ensure the confidentiality, integrity, and availability of sensitive information during and after an emergency.

The core objectives of contingency planning include the capability to:
• Restore operations at an alternate site (if necessary)
• Recover operations using alternate equipment (if necessary)
• Perform some or all of the affected business processes using other means

The contingency plan will be developed for the entire enterprise. The contingency plan must address IT system components such as:
• Local, wide area and wireless networks including Internet access (if critical to the operation of the business)
• Server systems such as file, application, print and database

• Web sites
• Security systems such as firewalls, authentication servers, and intrusion detection

4. DATA BREACH MANAGEMENT

Data Breach Management is intended to assist employees responsible for managing breach related activities of the School District when making decisions after a data breach has been identified. This procedure is designed to minimize the loss and destruction of data, mitigate the weakness that was exploited and restore all computing and other impacted services to the School District.
If a data breach is discovered at the School District, the following steps will be followed in order to prevent further damage, assess the severity of the breach, and manage all associated breach related activities.

• Once a breach has been identified, the Technology department will review the breach details and develop an appropriate response.

• The Technology Director will keep the District leadership apprised of the situation.

• Priorities of the Technology Department: ○ Stopping the data leakage ○ Mitigation of the weakness that was exploited ○ Restoration of normal business ○ Notification of persons and businesses impacted as deemed appropriate

• The Technology Director will work with the District legal counsel to determine applicable state and federal laws that may be applicable to the incident; including but not limited to FERPA and state breach notification laws.

• If any form of protected information is at risk then the Technology Director is to enact the Breach Response and Reporting procedure.

• Forensic analysis of the breach is to begin immediately upon determination of the breach, unless law enforcement deems a delay is appropriate, or additional forensic support is required beyond the School District IT Team.

• All meeting minutes, technical documentation, and hand written notes of the breach are to be compiled by the Technology Director or designee within 72 hours of the closure of the breach.

• Any systems that were compromised or targeted as part of an incident resulting in an investigation may be quarantined as determined by the Technology Director and Superintendent.

• Based upon the scope of the perceived threat the Technology Director or Superintendent will notify local law enforcement, including local police, sheriff's office and regional FBI office.

5. RESPONSE AND REPORTING

Response and Reporting is intended to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the School District; and document security incidents and their outcome.

The District will develop and implement a contingency plan to ensure the confidentiality,

integrity, and availability of sensitive information during and after an emergency that includes response and reporting procedures.

The Technology Director is responsible for determining the appropriate level of response to a security incident. All such response must be in accordance with established policies and procedures. At a minimum, the Technology Director and department must immediately consider a response that includes:

• Disconnecting the affected system from the network (should not remove power from the system)

• Determining if the incident is accidental or intentional

• Identifying all system-related information such as: ○ Hardware address ○ System name ○ IP address ○ Sensitive data processed by the system ○ Location of the system

District employees will immediately report any and all suspected violations of information security to their supervisor.

All incident reporting and response activities must be conducted strictly on a need-to-know basis.

The Technology Director will provide a security incident report containing the following:

• Contact information of the person reporting the incident (name, phone, address, email)

• Date and time of the incident

• Detailed description of the incident

• Any further information, such as unusual activities or individuals associated with the incident

6. SECURITY INCIDENT

The District will maintain procedures for identifying security incidents. A security incident is any breach of security policy, or any activity that could potentially put sensitive information, especially sensitive information, at risk of unauthorized use, disclosure, or modification.

A breach is defined as the unauthorized acquisition, access, use, or disclosure of protected information as defined below, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. If a breach has occurred, employees must immediately follow the instructions of the District's data breach procedure.

Incidents will be classified as "serious" or "non-serious." Non-serious incidents generally have the following characteristics:

• It is determined that there was no malicious intent (or the attack was not directed

specifically at the School District associated with the incident) and

• It is determined that no sensitive information was used, disclosed, or damaged in an unauthorized manner

Serious incidents generally have the following characteristics:

• It is determined that there was malicious intent and/or an attack was directed specifically at the School District

• It is determined that sensitive information, may have been used, disclosed, or damaged in an unauthorized manner or that this incident may be construed as a data breach

All school district employees will immediately report any security incident to their supervisor.

The District will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature. Incidents characterized as serious by the Technology Director will be responded to immediately and reported to the Superintendent.

The District will attempt to mitigate any harmful effects, when possible, where a security incident affects customer information.

SECTION E: Standards for Retention and Verified Destruction of Student Data

1. Data Backup and Storage 2. Disposal 3. Media Re-use

1. DATA BACKUP AND STORAGE

Data Backup and Storage refers to creating a retrievable, exact copy of sensitive information, when needed, before the movement of equipment. The School District will determine when backups are needed and this will be done prior to the movement of any required systems. The School District will make an exact, retrievable copy of the data. The School District will test the copy of the data to make sure the copy of the data is exact and retrievable. The School District will store the backed up data in a secure location and ensure that the appropriate access controls are implemented to only allow authorized access to all such data.

2. DISPOSAL

Disposal refers to implementation of procedures to address the final disposition of sensitive information and/or the hardware or electronic media on which it is stored. The District will ensure that the master inventory list is appropriately updated upon the disposal of components containing sensitive information. The District will retain School District records and/or public information for the period required by the State records retention policy and rules to the extent applicable. The School District will ensure that prior to disposal either the data will be securely overwritten or physically destroyed and that such steps taken will be documented.

3. MEDIA RE-USE

Media Re-use refers to implementing procedures for removal of sensitive information from electronic media before the media are made available for re-use. The School District will ensure the master inventory list is appropriately updated upon the re-use of media components containing sensitive information. The School District will ensure that prior to re-use that the media is securely overwritten and that such action is verified and documented.

Adopted
:

Lincoln County School District #2,
Wyoming