Molalla River School District

Code: EHB-AR
Revised/Reviewed:

Staff Cybersecurity Policy

The Molalla River School District is committed to maintaining a secure digital environment that protects the confidentiality, integrity, and availability of district data, including sensitive student information. This Cybersecurity Policy outlines the responsibilities of all staff members in ensuring the safety and security of our technology resources and data, in compliance with federal and state laws and district policies, including but not limited to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet Protection Act (CIPA), and the Oregon Student Information Protection Act (OSIPA).

Roles and Responsibilities

All staff members ("Users") are responsible for adhering to this policy and related guidelines to protect district data. Specific roles with cybersecurity responsibilities include:

- **Designated Information Security Officer (ISO):** Oversees the district-wide information security program, develops and disseminates policies, coordinates training, and manages responses to security breaches. The ISO will be a senior-level employee.
- **Data Owners:** Management-level employees who oversee the lifecycle of district data, classify data sensitivity, determine access criteria, and ensure data custodians implement security controls.
- **Data Custodians:** Employees within the Information Technology Department with administrative and operational responsibility over district data, responsible for implementing security safeguards, documenting procedures, managing access, reporting risks, performing data backups, and ensuring password expiration.
- **Users (All Staff):** Employees, contractors, or third-party agents authorized to access District Information Systems and/or district data. Users are responsible for:
    - **Adhering to all policies, guidelines, and procedures related to the protection of district data.** This includes this Cybersecurity Policy, the Technology User Agreement, the AI Policy and the policy on Personally Identifiable Information (PII).
    - **Protecting password confidentiality and not sharing passwords with others** . Using another user's account or allowing such access is prohibited without supervisor approval.
    - **Reporting actual or suspected vulnerabilities or breaches in the confidentiality, integrity, or availability of district data to an administrator or the Information Technology Department immediately.**
    - **Exercising professional judgment in the use of all technology and limiting personal use so as not to interfere with the intended business purposes**. The district makes no guarantee of privacy on its systems; email and documents generated on the district's system are considered a public record and the property of the district.
    - **Safeguarding the MRSD's confidential information from disclosure**.
    - **Complying with all laws regarding student records, confidentiality, privacy, and student internet use at all times**, including FERPA, COPPA, CIPA, and OSIPA.

  - **Under no circumstances should Personally Identifiable Information (PII) be shared with any non-district approved online service or application, including generative AI applications**.

Classification of Information

All district data shall be classified based on its level of sensitivity and potential impact if disclosed, altered, or destroyed without authorization. The classification helps determine appropriate security controls.

- **Confidential Data:** Unauthorized disclosure, alteration, or destruction could cause a significant level of risk to the district or its affiliates. This includes data protected by state or federal privacy regulations and confidentiality agreements..... **Examples include student data, evaluation and disciplinary records**. The highest level of security controls applies to confidential data.
- **Sensitive Data:** Unauthorized disclosure, alteration, or destruction could result in a moderate level of risk. By default, all district data not explicitly classified as confidential or public is sensitive. **Examples include salaries and staff personal contact information**. A reasonable level of security controls applies to sensitive data.
- **Public Data:** Unauthorized disclosure, alteration, or destruction would result in little or no risk. **Examples include board minutes and policies**. While confidentiality controls are minimal, controls to prevent unauthorized modification or destruction are necessary.

Online Services and Applications

District employees are encouraged to research online services or applications to support district objectives. However, **employees are prohibited from installing or using any applications, programs, software, or online systems/websites that store, collect, or share confidential or sensitive data until the ISO approves the vendor and the software or service**. Prior to approval, the ISO (or designee) will verify compliance with all applicable laws, regulations, and board policies, ensuring appropriate protection of district data. This prior approval is required regardless of whether the software or online service is obtained or used without charge . This is particularly important in the context of AI technologies; **only AI applications approved by the district's IT Department may be used for tasks involving students or student data**.

Guidelines for Secure Practices

- **Password Management:** Create strong, unique passwords and change them regularly (at least annually, as enforced by data custodians). Do not share passwords. Implement Multi-Factor Authentication (MFA) for logins as directed by the IT Department.
- **Email Security:** Be cautious of phishing emails and suspicious links or attachments. Verify the sender's identity before providing any information or clicking on links. Follow best practices for sharing student information in emails, such as using initials or student ID numbers and including only necessary information. **Never include student names in the subject line of an email or use SSIDs in email**.
- **Device Security:** Secure district-issued devices (laptops, tablets, etc.) by locking them when unattended. Do not leave devices in unlocked locations, including vehicles, especially in

extreme temperatures. Report any lost, stolen, or damaged devices immediately to the MRSD Technology Department.

- **Software and Updates:** Do not attempt to install unauthorized software or upgrade existing software on district devices. Report any software needs to the IT Department. Ensure that operating systems and software are kept up to date with the latest security patches, which may be managed centrally by the IT Department.
- **Data Storage:** Save all work-related content to Google Drive or other network drives as designated by the district. Data saved locally on devices may not be backed up.
- **Internet Use:** Adhere to the district's Technology User Agreement. Be mindful of the websites visited and the information shared online. Be aware of CIPA regulations regarding access to offensive content on school computers.
- **Physical Security:** Secure physical access to areas where district data is stored or processed. Follow procedures for visitor access and data disposal.
- **Use of Personal Devices:** Any use of personal electronic devices for school-related activities must be in accordance with District Policy GCAB. Ensure that no photos or videos of students are kept on personal social media sites or phones without proper authorization.
- **Generative AI:** Staff must adhere to the district’s policy on Artificial Intelligence (AI). **Never share Personally Identifiable Information (PII) with any generative AI application**. Use only district-approved AI applications when engaging in activities directly involving students or student data. Evaluate AI-generated content critically for accuracy and bias.

Violations and Sanctions

Violations of this Cybersecurity Policy include, but are not limited to, unauthorized access to information, enabling unauthorized access, inappropriate disclosure, modification, or destruction of data, inadequate data protection, or ignoring the explicit requirements of data owners.
Violations of this policy will be subject to disciplinary action in accordance with district policies, collective bargaining agreements, and applicable provisions of law. Sanctions may include:

- Suspension or termination of access to district technology resources.
- Disciplinary action up to and including dismissal.
- Referral to law enforcement for violations of law.
- Staff are encouraged to report suspected violations of this administrative regulation to the ISO or the appropriate data owner. Reports of violations are considered sensitive information until otherwise designated.

This policy will be reviewed and updated periodically to reflect changes in technology and legal requirements. All staff are expected to familiarize themselves with this policy and adhere to its guidelines to ensure a secure and responsible digital environment for the Molalla River School District.