Navarro ISD

Board Report

Technology Department

February 2025

Director

Managed Methods - Updates

In early January, we proactively implemented Managed Methods, a platform designed to monitor and identify potentially sensitive data within our digital environment. After over a month of active use, the platform has revealed a significant volume of sensitive data being shared via email and Google Drive, confirming our initial concerns. This discovery underscores the need for a robust data loss prevention strategy. Specifically, Managed Methods has pinpointed several key areas of concern where sensitive information is being inadvertently or inappropriately shared. Recognizing the critical balance between security and operational efficiency, we have been diligently evaluating secure solutions that empower staff to share necessary information without imposing undue complexity or hindering recipients. Our goal is to implement a solution that seamlessly integrates with existing workflows while significantly mitigating the risk of data breaches and ensuring compliance with relevant regulations.

Virtru

Following our discovery of substantial sensitive data sharing through email and Google Drive (identified via Managed Methods), we identified and implemented Virtru as a secure email and Drive sharing solution. Virtru offers robust encryption for both email content and attachments, addressing the core security concerns highlighted by the Managed Methods platform. Beyond basic encryption, Virtru empowers the district with granular control through enforceable access policies, including the ability to limit data availability timelines and revoke access at any time, even after the recipient has received the information. Staff members with a demonstrated need for access to sensitive data have received comprehensive training on utilizing Virtru effectively.

Since implementing Virtru, Managed Methods alerts have significantly decreased, indicating a marked improvement in our data security posture. This solution provides a crucial safeguard against data breaches, even in the event of user account compromise. Virtru's security relies on cryptographic keys intricately linked to the user's password. Critically, whenever a user's password is changed (whether intentionally or due to a compromise), the associated security keys are automatically updated. This ensures that unauthorized individuals, even if they have previously downloaded emails or attachments via IMAP (Internet Message Access Protocol), a protocol allowing remote email access, will be unable to decrypt the content without re-authenticating with the updated password. This dynamic key management provides a robust layer of protection against unauthorized access to sensitive data, even after initial transmission.

Google Data Loss Protection

With the above two initiatives in place we are able to turn on Google's Data Loss Protection (DLP). This initiative strengthens our data security posture by automatically scanning emails and attachments for sensitive information, preventing unauthorized disclosure.

DLP identifies and blocks emails containing protected data, including:

- FERPA (Family Educational Rights and Privacy Act): Student education records.
- HIPAA (Health Insurance Portability and Accountability Act): Protected health information.
- PII (Personally Identifiable Information): Data that can identify an individual (e.g., names, addresses, Social Security numbers).

DLP will either flag emails containing sensitive data, prompting user review, or block the email entirely, notifying the sender. For authorized transmission of sensitive data, Virtru encryption remains the required method. This enhancement reinforces our commitment to data privacy and regulatory compliance. Further details are available upon request.

Student Passwords

Prior to the winter break, junior high and high school students were notified that they would be required to establish personalized passwords upon their return in January. This initiative directly addresses several instances of students accessing and misusing their peers' accounts, a vulnerability stemming from the previous use of simple, default passwords. To minimize disruption and maximize student productivity during this transition, librarians and/or aides at each campus were granted password reset access within Google Admin for their respective student populations. This decentralized approach empowers students to regain account access quickly, eliminating potential delays associated with waiting for IT intervention. Furthermore, to enhance security and prevent reversion to easily guessable credentials, we have disabled the reuse of old passwords for all students. This measure ensures that students cannot simply revert to the previously assigned default password, significantly strengthening the security of their individual accounts.

Systems Administrator

- The Technology Department has completed a cleanup of outdated Chromebook extensions that were previously force-installed for students and staff. This initiative will improve the initial boot times for student Chromebooks and streamline Google account loading, enhancing overall device performance.
- The ClassLink Analytics environment has been successfully set up and configured to support the Academics team. Administrative access has been granted, allowing them to monitor usage

statistics related to classes, users, and applications. This will provide valuable insights to improve instructional technology integration.
- To ensure seamless access to IXL, the allotted licensing amount has been adjusted to stay within our limit. This adjustment prevents rostering issues and allows students to be added without disruption.
- Rostering issues with Frog Street LilyPad and McGraw Hill, which previously prevented entire classes from accessing their respective platforms, have been resolved with assistance from their support teams. These fixes restore access and ensure uninterrupted learning experiences for students and teachers.
- The migration of NWEA from a manual data pull to an automatic overnight sync is in progress. This transition will enhance data accuracy and efficiency. The final phase involves resolving minor metadata issues with NWEA support, which is currently underway.

Network Administrator

1. New Intermediate School portable network equipment - Ordered and received all network equipment for the new Intermediate School portables. This will allow for network equipment installation during the spring after the portables have been delivered and be ready for the 2025-2026 school year.
2. Internet Service Provider (ISP) Virtual Redundant Router Protocol (VRRP) Switchover - Transitioned to the new ISP IP address with the VRRP features. These features will allow for the primary ISP to lose one leg of the circuit (ex. Austin to Dallas) and still provide full network connectivity (via San Antonio to Houston). The secondary WAN solution is still in place providing a load balancing solution that will provide essential network connectivity and limit downtimes in the event of an ISP outage like the one that occurred in December (both circuits experienced physical damage due to construction).
3. High School Bell System. Worked with the vendor for the High School bell system as the bells had lost time and were ringing approximately 90-120 seconds late. The root cause of this was a malfunctioned cable in the High School that was apparently chewed on by rodents (this occurred in several areas throughout the district during the below freezing temps).
4. Phishing training to Staff members. Provided valuable training to Food Service, Transportation, and High School staff members. This training was focused on how to identify and report phishing and the importance of growing Cybersecurity threats that are facing the K-12 educational space.

Technicians

- A total of 58 monitors have been replaced at the high school, providing upgraded equipment to enhance the learning environment.

- The staff device rollout at the high school is nearly complete, with the majority of devices successfully distributed and configured for use.
- Our technician team resolved 270 support tickets this month, demonstrating our continued commitment to addressing technical issues in a timely manner.