

Information Technology Advisory Committee

February 10, 2020 4:30 – 6:00 p.m.

Room 2750, John Stanford Center

2445 3rd Avenue South, Seattle, WA 98134



Meeting Notes

Call to Order

Mr. Carlos Del Valle called the meeting to order at 4:41 p.m. Roll call is as follows:

- Committee Members Present: Nina Arens, Christine Billroth, Carla Rogers, Peter Lee. Avery Wager, James Wager, TuesD Chambers, Ms. Elizabeth Ebersole.
- Committee Members Absent: Tu Dang, Molly Meck, Josh Caldwell, Marcello Benati. Brian Vance, Charnjit Dhoot, Jacob Marzynbski, Roy Zimmerman, Pauline Amell Nash (co-chair).
- Other Staff Present: Executive Director of Technology Carlos Del Valle (chair), Director of Enterprise Applications and Data Services Nancy Petersen, Information Security Manager April Mardock, Executive Assistant Tim Hall, Stephanie Shek.

Committee members introduced themselves during roll call.

Ms. Ebersole move to accept the proposed agenda, Mr. Peter Lee seconded. This item passed unanimously.

Ms. Ebersole move to accept the minutes from the December meeting, Ms. Carla Rogers seconded. This item passed unanimously.

Review of DoTS Budget

Mr. Del Valle discussed classroom technology budgets and Information Support Specialist in response to the questions from December raised by Mr. Lee.

Special Attention Items

Staff member April Mardock provided a presentation regarding district cybersecurity. Ms. Mardock explained there is a team of Cybersecurity specialists that includes a .5 Network Analyst and one Full-Time Employee (FTE) Systems Engineer Senior.

Ms. Mardock shared that the district has taken steps for data privacy. Policy 6501 started as a plan to protect staff members and has since been modified to include protecting student data as well. Superintendent Procedure 6501 also reflects data privacy as well.

Ms. Mardock walked through the various items that the Cybersecurity team does to ensure safety. Vendors that hold or host student information have data sharing agreements (DSA). Ms. Mardock goes into details regarding the parameters of DSA clauses. The Cybersecurity team is active in all software procurement and requests for proposals (RFP) and conducts audits all applications are single accounts.

Ms. Mardock spoke about the ATP (Microsoft's Advanced Threat Protection) that keeps a log of anything that attempts to access the network. There have been students who have attempted to access the internal network. Ms. Mardock clarified that the Department of Technology Services (DoTS) does not handle any disciplinary action but will inform and provide a log to the school principal and parents for next steps. Other threats are addressed case by case basis and will involve law enforcement agencies as needed.

In collaboration with the Seattle Education Association (SEA) Union, all staff are required to use a multi-factor authentication (MFA) when using district accounts on personal devices. Staff members may choose to opt-out but will not have ability to have the access.

Ms. Mardock shared that there is a third-party vendor that monitors district networks during the weekends and long holidays as these have been targeted timeframes for attacks.

Ms. Mardock also discussed firewalls that protects specific data centers and networks. Schools are restricted from sharing networks and files to eliminate the potential spread of viruses. New Microsoft technology also helps support active cybersecurity such as checking and flagging suspicious emails before they reach a user's inbox

Ms. Ebersole brought up the occurrence of donated technology or outside products that cannot be supported by the district. Committee members also supported explicit dissuading usage of old technology equipment due to limited support of old devices and easy targets.

There was a follow up question from Ms. Arens regarding the Bring-Your-Own-Devices for the 1:1 student device deployment and steps for cybersecurity. Ms. Mardock answered that the student account is hosted on the cloud Microsoft 365 OneDrive and they are not accessing the district drive.

Ms. Mardock discussed cybersecurity external feedback conducted by an outside party that included formalizing incident response plan has many layers, IT security policy, password policies, cloud security, and monitoring network health.

Ms. Mardock answered questions from Committee Members regarding adding additional training that would have to be discussed in the next Collective Bargaining Agreement and how to leverage safe technology practices, and business continuity success. Ms. Mardock concluded the presentation.

Mr. Del Valle asked Committee Members for their comment on TEAMS and how it works for users. Ms. Chambers shared feedback regarding TEAMS and issues that have come up. Mr. James Wager shared that only one TEAMS account per time and messaging may be missed if another account is logged into the device account.

Open Comments

REA team – Ms. Ebersole wanted to learn how REA impacts board policies.

Public Comments

There were no public comments.

Adjourn

Ms. Ebersole motioned for the meeting to adjourn. Ms. Arens seconded.
The meeting adjourned at 5:55 p.m.

Next Meeting

Monday, May 18, 2020