

## **Technology Update - School Committee**

### **December 14, 2017**

#### Network Security Audit

As part of last summer's network upgrade, a security audit was performed to evaluate our network and our current security practices. Overall, the results of the audit were positive, indicating that our risk of a security breach is fairly low. Some suggestions that came out of the audit include:

- For those users that have PC computers, it is recommended that we remove administrator privileges so that users cannot accidentally download/install malware on their devices.
- Staff and student network passwords should be reset on a periodic basis. Currently, passwords do not expire.
- Identify and apply missing updates and/or software patches.
- Identify and/or de-activate dormant users and/or computers.
- Create a monthly maintenance schedule that includes items such as account user maintenance tasks, software updates, password security audits, etc...

Additionally, the network upgrade performed over the summer and finalized this fall comes with a number of inherent security upgrades. For example, all staff and students are required to register their school issued device and personal device with our wireless network. This provides a much higher level of accountability and allows us to more easily identify potential security threats. Our Guest network requires authentication and has a limit to the number of sessions available to users in any given 2-week period. On the wired side, we now have the capability to monitor and manage devices that have been connected directly to our network data ports. These forms of *network access control*, for both our wireless and wired networks, have greatly increased our ability to mitigate threats to our network.

#### Student Data Privacy Initiative

In an era where online teaching and learning resources are commonplace, districts are struggling to identify and implement best practice safeguards around the issue of student data privacy. In response to member district needs in this area, The Education Cooperative (TEC) has created the **TEC Student Data Privacy Alliance (TEC SDPA)**. This alliance will provide members with shared access to targeted training, experienced administrative support, and expert legal counsel as well as to leverage the TEC Collaborative's collective influence with vendors. It should be noted that TEC has allocated significant funds to establish this alliance.

The TEC SDPA will have access to the Massachusetts Student Privacy Alliance (MSPA) website, tools, and expertise. MSPA is an established alliance, led by Steve Smith of the Cambridge Public Schools, that is nationally recognized for its pioneering work in the area of student data privacy.

Westwood is one of 20 founding members of this alliance and will be entitled to the following benefits:

1. Participation in monthly member networking meetings.
2. Support of an experienced Administrative Specialist who will be our point of contact to research, review and submit the MSPA contract to our vendors on our behalf.
3. Access to expert legal counsel to provide us with guidance and support when needed.
4. Participation in targeted data privacy Professional Development workshops, webinars, and events
5. Legal Issues Workshop Series - Topics include: Anatomy of a Vendor Contract, Must Haves vs. Nice to Have, Red Flags