

## **5-Recommendations**

### **Monitor Student Use**

- Schools must allow students to access and utilize technology in the age that we live in.
- To be competitive global citizens, students must become comfortable and proficient with various technologies.
- Access and use of technology by students are increasingly important to allow for familiarity, comfort, and proficiency.
- However, greater access and use of technology by students can increase the risk of students having the ability to bring viruses into a network, harming others and themselves.
- It is important that students are allowed to use technology with effective monitoring. Verses, limiting their use of technology in the classroom. (Robinson, Brown, & Green 2010)

### **Training teachers**

- To improve students monitoring in the classroom, teachers must be trained to know what to look for.
- Teachers that are trained on types of social networks, websites, wearable devices, and other devices that commonly cause viruses, will be armed with the technological knowledge to have a more vigilant eye when monitoring students. Thereby, impacting pedagogical component of technology use.

### **Use Secure Passwords**

- Another common mistake many internal users make is using passwords that are easy for individuals or automated tools to figure out. (Robinson, Brown, & Green 2010)
- Once user's password is compromised a network can be accessed and thereby compromised.
- Using longer more complex passwords are recommended to improve internal security and protect a computer network within a school.
- Using special characters, numbers, and capital letters can strengthen passwords and network security.

### **Balance Instructional Needs with Network Security**

- Overall, a network must be protected to allow users to function and schools, and businesses alike, to operate more effectively.
- Network administrators, principals, and teachers should work diligently and take logical approaches to balance both computer network access and security to promote use and safety. (Robinson, Brown, & Green 2010)
- Too much security and less access, halts productivity.
- While too much access and less security increase the possibility of computer network attacks, viruses, and ultimately inoperable educational technologies.

## **Reference**

Robinson, L., Brown, A., & Green, T. (2010). Network Security Versus Access. In Security vs. access balancing safety and productivity in the digital school. Eugene, Or.: International Society for Technology in Education.