IT Resources: COVID-19 Guidance

Updated 4/6/20

Wireless Options

- Verizon Wireless: Verizon Wireless is currently under state contract, and devices are $0 cost. Service is $35/month for high utilization and $24/month for low utilization.
- T-Mobile: There is currently a $0 cost for devices and a $35/month per user for unlimited bandwidth.
- Comcast: Comcast currently has a program for low-income families to obtain internet service. This service is normally $10/month (Internet Essentials program). However, under COVID guidelines, Comcast is waiving the cost for two (2) months. This does not provide super high-speed internet, but does provide basic access. Information related to this is provided below.

Device Options

- The department is currently working with Dell, Microsoft, and SHI as a reseller to provide low-cost options across manufacturers.
- Comcast also has devices under their Internet Essentials program. More information can be found at: https://corporate.comcast.com/press/releases/internet-essentials-low-income-broadband-coronavirus-pandemic.
- The average cost for devices will be between $100- $149 per device.
- Options for lease are limited due to financing conditions and no guarantee on equipment quality on return.

IT Supports for Learning

- Working with Microsoft, the department can provision Microsoft Teams to enable virtual classrooms for learning. This virtual classroom model is active in a number of states and can be structured to meet the needs of districts.
- The department can auto-create the Teacher/Student relationships into a Microsoft "Class." This functionality can be created inside of the Teams application using EIS, so that the platform creates "classrooms" inside of "schools." This feature will give teachers access to the tools available, including assignment creation, grading, teacher / student communications via text and video chat capabilities within the application.
- Microsoft Teams also allows for monitoring of student activity within the virtual classroom to ensure students are participating and actively working on their assignments.

Internet Safety Tips: **(Updated 4/6/2020)**

As we extend from the physical classroom to the virtual classroom, internet safety is as important as school safety. The Tennessee Bureau of Investigation (TBI) has released information indicating that there has been a sharp uptick in digital child exploitation cases. TBI Special Agents are asking that parents and guardians reconsider the ways their children use Internet connected devices such as computers, mobile phones, gaming consoles, and tablets. TBI has released a webinar via their Facebook page (link below) addressing this issue as well as some online safety tips.

- **Keep computers in common areas.** Any computers, including laptops, should remain in the main living areas of a home.
- **Take advantage of content controls.** Many software providers and Internet service providers (ISPs) offer technology that helps block inappropriate sites.

- **Never share personal information online.** Don't post, e-mail or in any way provide personal information to strangers in chat rooms or elsewhere online. Details off limits include: full name, address, phone number, school name or photos.
- **Protect your online identity.** Don't use e-mail logins, screen names or passwords that reveal personal information, such as name, age or gender.
- **Never, ever meet a stranger offline.** Under no circumstances should a child or young adult meet in person with anyone they've met on the Internet.
- **Monitor Internet activities.** Learn how to check Web history and maintain access to e-mail passwords to review online communication.
- **Understand social networking trends.** Popular social media sites are popular with young people, but have become hunting grounds for Internet predators. Explore privacy settings.
- **Talk openly about Internet safety.** Parents and kids should spend time together online and check out information resources. Communication is the key.
- **Speak up.** If a child or young adult feels uncomfortable about anything seen on a computer, he or she should feel safe telling a parent, teacher or another trusted adult.

Finally, don't forget: To report cases of child sexual exploitation - including child pornography and cyber-enticement - use the national CyberTipline (https://report.cybertip.org/). Reports can be made online or by calling (800) 843-5678.

Resource Links

There are numerous resources available on these subject for students, parents/guardians, teachers, and other school staff.

- Tennessee Bureau of Investigation Facebook Page: www.facebook.com/TBInvestigation
- National Center for Missing and Exploited Children (NCMEC): www.missingkids.org
    - Are Your Kids Home and Online? How to Keep them Safer
    - Protecting Kids Online
    - NetSmartz: This link contains educational games, tip sheets, presentations, and curriculum.
- Tennessee Association of Chiefs of Police, Delete Online Predators: www.deletepredators.com
- Common Sense Media: www.commonsensemedia.org
- Internet Crimes Against Children: www.icactaskforce.org
    - Internet Safety Resources Page

EIS Reporting **(Updated 4/6/2020)**

- For specific information about EIS Coding Guidance, please see the EIS Coding FAQ's document.