Safe Technology Use at Home

- Have your child work in a common area of the home. This is an easy way to keep an eye on them and ensure they are staying on task.
- Remind them to keep private information private. They should never be using their real names, where they go to school, where they hang out, where they live, or any other identifying information with anyone they don't know.
- The devices that are rented from the district will have the Internet filtered with the same strong protection we use at school. If your child is using their own device, be sure to take advantage of filtering software. There are many options when looking for a solution to filter Internet content. Below are just a few suggestions.
  - OpenDNS has a good solution, but requires a bit of technical knowledge to set up.
  - Norton Family is a good service and has a free 30-day trial.
  - Net Nanny is a popular option and simple to set up. It also has a 30-day trial.
  - Circle - We heard great things about this product from parents when we held the BYOD informational meetings.
- Keep an open line of communication and let them know that it's alright to come to you if they see something online that made them feel uncomfortable.
- Have them get permission from you before posting anything to a website that is not operated by the school system.
- Remind them often that they should treat their friends with the same respect when interacting online as they do when they are face-to-face.
- They should NEVER be sharing their passwords with anyone, including teachers. Parents should be the only people they share their password with. If they forget their password, the technology department at WWS will be able to reset it for them.
- Check their browser history every so often. This is a great way to be proactive and know what your child's online activities have been. If you know which browser they use, a quick Google search will tell you how to do this.
- Remind them to never respond to ads or click on unfamiliar links. Hackers are getting smarter in the way they trick people into giving access to their computer. A good rule of thumb is to stick to reliable sites and never click on a link in any email that is from an unknown sender.
- Talk to your kids about the persistence of anything they post online. They may have deleted that embarrassing story they posted, but it is never truly gone. They should never write anything in an email, message board, or private message that they wouldn't want the entire world to read.