BringYourOwnDevice

Device and Internet Safety

Our children have an unprecedented access to information, learning, and the world through technology, especially as we move to BYOD. While there are great benefits, there are also dangers in this access. How do we protect our children from the evil that is around us while giving them the tools they need to be successful in this technological age? Below are some tips and tools you can use. Implement them, not because you don't trust your children, but because you want a boundary between the predators of this world and your child, and because the devil works best in darkness and secrecy.

General Best Practices

Keep devices in common areas or if students study in their bedroom keep the door open. As a family we have found it best to have all devices in main areas at night.

Limit the time kids spend on electronic devices. The American Academy of Pediatrics recommends no more than 1-2 hours per day of high quality content for children and teens, stating "It is important for kids to spend time on outdoor play, reading, hobbies, and using their imaginations in free play." Sure, they need to do their homework, but they don't need to play games for hours also.

Be involved. Talk to your children about social media and texting etiquette. Make sure their privacy settings are set to "Friends Only." Be their friend on Facebook, Twitter, etc. Reserve the right to look at anything on their device at any time. Know their passwords and usernames.

Set age-appropriate restrictions on devices your children use. This includes computers, phones, ipods, etc. The information on page 2 will walk you through the process. Links can also be found at nmcs.us/student-life. **This is very important!**

Virus Protection

You **need** virus protection on your computer. Even Apple products can get viruses, it is just less likely because hackers target the most common operating system—Windows. There are many paid virus protection products out there, and they all work. There is also quality free protection. Below are some free options. Tablets and phones usually don't need virus protection since apps are downloaded only from the app store.

avast! FREE FOR EDU We use Avast for Education. For Windows or Mac. It is a good free virus protection, but you may get the occasional ad to upgrade to the paid version. Download at Avast.com/students.

Microsoft Microsoft Security Essentials offer virus and malware protection. Google and download from Microsoft.com. It comes in a pack with other programs—choose Custom Installation to choose only the programs you want.

Setting Restrictions on Devices

Setting boundaries on devices protects your child from accidently or purposefully accessing inappropriate websites. It may be overzealous at times, but you can generally manually allow websites it has blocked. This will not always block inappropriate images in searches, which is why the other "Best Practices" are recommended. These should always be implemented in addition to parental and teacher supervision.

Windows Family Safety

For Windows 7 or 8 devices. Can be downloaded at *https://familysafety.microsoft.com* . Will require you to have a user account with administrative privileges that is password protected on the device. You will create an account and create your settings for each child (can be for more than one computer). On each computer you will set up each user with the correct account (it walks you through it). You can turn on activity reporting, web filtering, time limits, app restrictions, Windows Store and game restrictions and requests. It sometimes blocks things you don't need blocked, but you can allow them with the password.

Macintosh Parental Controls

For Apple computers. Go to *support.apple.com* and search for "Set up Parental Controls." Choose the operating system on your computer (to find out what that is, click on the little apple icon in the top left corner and choose "About this Mac.") Follow the directions there. You can adjust settings for apps, web, people, time limits, and other. It may block things you don't need blocked, but you may be able to allow them with your administrative password (it does on an ipad)

To set Parental Controls on Kindle, Android, or Apple tablets and phones, see nmcs.us/student-life for links.

What NMCS Does to Keep your Child Safe

Firewall

Our firewall blocks malicious attacks and also blocks access to inappropriate websites when students are on our wifi. It does **NOT monitor devices using cellular data** (such as phones), or devices when they are not at school. That is why it is important to set restrictions.

Education

We discuss cyber safety and the appropriate and moral use of technology at all ages in computer classes, from Kindergarten through Computer 10.

Supervision

As teachers we know that the best protection is our presence. Teachers move around the room or have computers screens facing the front as students work. We reserve the right to remove technology if it is hindering education, and only use technology when it is the best way to learn. However, we can only supervise in the classroom setting is why setting restrictions is vital.

Questions or comments? Call Erin at 231-825-2492 or email eheuker@nmcs.us. Technology is a rapidly changing environment. Your input is appreciated as we work together to keep our children safe.