Three Tips from the Director of Technology

1. Cut down on your kids' screen time: Limit casual screen time to an hour a day, and only when all homework and chores have been completed. No screens in the bedroom. That means all screens, including phones and smartphones. Late-night texting and Web surfing have been cited as two of the main reasons why today's teens are not getting enough sleep.

2. Know your Parental Controls:

- iPad: Set device restrictions on your iPad. Go to Settings > General > Restrictions and tap Enable Restrictions. Every time you do this you'll be asked to set a 4-digit passcode and enter it a second time. Apple doesn't give you the option of disabling every app on the iPad individually, though some do have that option. You can turn off Safari, YouTube, the Cameras, Facetime, even iTunes.
- Allow Content Tap Apps. This gives you the ability to restrict apps by age range. These ratings are visible in the app store and assigned by Apple. Be aware that they may not conform to your idea of what's appropriate for what age group.
- Macbook: Currently within the district network we have content filtering, so we can block specific sites and apps. However, at this time Derby Public Schools does not have a mobile device management application for Macbooks. Because the Parental Control needs the Admin password, you are not able to access it at this time.

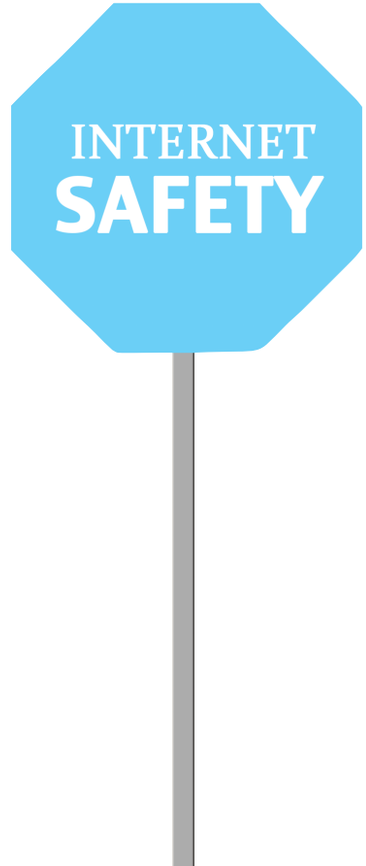
3. Network Security: A week doesn't go by without reading about some new virus that is attacking computers all over the world. Meanwhile, phishing scams, malware, worms and spam continue to be everyday threats. If you haven't already done so, then it's a good idea to protect your personal information and data by installing the latest security software.

- Create A Strong Password: Don't fall into the trap of using the same password to log in to multiple web sites; if one site gets hacked, then you are vulnerable everywhere else.
- Backup Your Data: You have heard this hundreds of times as well, but this this highly recommended! The stories of computer crashes, corrupted hard drives and data-destroying viruses are just too common to ignore.
- Network Router: Many times families don't know that their personal home router is still set to the default username and password. Many hackers try the default login before moving on to another router. If you don't know how to do this, look up the specific router and download the manual. Many routers already have parental controls that can be set for specific times of the day.

Source: Parent Guide for Apple ID for Students & www.commonsensemedia.org

Parent Guide Book

Internet Safety for Students



Learn the basics of Internet safety:

- Keep the computer in a high-traffic area of your home.
- Establish limits for which online sites children may visit and for how long.
- Remember that Internet technology can be mobile, so make sure to monitor cell phones, gaming devices, and laptops.
- Surf the Internet with your children and let them show you what they like to do online.
- Know who is connecting with your children online and set rules for social networking, instant messaging, emailing, online gaming, and using webcams.
- Continually dialogue with your children about online safety.

Source: National Center for Missing & Exploited Children

Talk to your kids

When your kids begin socializing online, you may want to talk to them about certain risks.

Inappropriate Conduct: The online world can feel anonymous. Kids sometimes forget that they are still accountable for their actions.
Inappropriate Contact: Some people online have bad intentions, including bullies, predators, hackers, and scammers.
Inappropriate Content: You may be concerned that your kids could find pornography, violence, or hate speech online.

You can reduce these risks by talking to your kids about how they communicate - online and off - and encourage them to engage in coduct they can be proud of.

Source: OnGuardOnline.gov

Social Media Safety

Check comments and images for any inappropriate posts that are illegal, such as threats, nudity, alcohol, or drugs.

Talk to your child about what's okay to post. Agree that they won't post embarrassing or hurtful comments or images about other people. Be clear that you'll delete - or if needed, report - any posts that are inappropriate, illegal, or threatening that could get them in trouble.

Review account settings. Check to see what is on their profile and who can see it.

Ask your child if they know who their friends, contacts, and followers are. These are the people who can see, share, and comment on their posts, so you want to be sure your child knows who they are. Block and report anyone who makes harassing, threatening, or inappropriate comments.

Keep an eye on third party apps. Some apps give companies access to personal information.

Don't forget about mobile devices like smartphones and tablets. Your child might be sharing their location when they make posts. Check their settings to make sure that they are sharing what you want them to.

PROTECTING YOUR KIDS ONLINE

TAKE CHARGE

Set some ground rules.
Establish basic guidelines like when your kids can go online, what sites they can visit, and how many texts they can send a month, so everyone is on the same page.

Research before you buy.
Some hand-held games can connect to the Internet and some laptops have built-in webcams. Understand what technology you have and what you might bring home.

Don't just sit there - REPORT!
If your kids are dealing with cyberbullies or potential predators, report them to the website, cell phone service, law enforcement, or www.cybertipline.com.

MONITOR

Supervise Internet Use.
If you can see what your kids are doing, they're less likely to get in trouble.

Safeguards do not equal Safe Kids.
Installing CIA-level monitoring software does not guarantee that your kids will be safe online. Technology can't replace your time and attention as a parent or guardian.

Don't go overboard.
It's smart to keep an eye on your kids' social networking profiles, but it's never cool when you post embarrassing messages or pictures to their page.

COMMUNICATE

Talk to your kids; they're not as mysterious as you think.
Your kids might not tell you everything, but that doesn't mean you shouldn't ask. Get involved so you're not the last to know.

Challenge them to a duel.
If you have kids who like to play video or computer games, ask if you can play, too. When you respect their interests, they're more likely to respect your rules.

Don't pull the plug.
Taking away your kids' Internet access because they've done something wrong doesn't solve the problem. Talk to them about protecting themselves and respecting others online.

Source: National Center for Missing & Exploited Children