Cedar Park Middle School PTC Minutes
November 20, 2017

The meeting was called to order by Dr. Shannon Anderson at 7:00 pm.

In Attendance:
Board: Jana Drotzmann, Jennifer Kveton, Tonya Stevens, Karen DiPietro, Dr. Shannon Anderson
Parents/Guests: There were about 30 parents in attendance tonight.

Approval of Minutes: Approval of October minutes will be postponed until January's General Meeting.

Principal Update
- Dr. Anderson introduced the parent's to each of our guests.

Board Reports

Treasurer:
- None to report at this time.

President:
- None to report at this time.

Secretary:
- None to report at this time.

Volunteer Coordinator:
- None to report at this time.

Next Meeting
Next meeting scheduled for January 22, 2017, 7pm in the Media Center (Library). Unfortunately, we were unable to get to any actual PTC business tonight, due to our two speaker presentations. The meeting ended with our final guest asking for open questions.

Presentation: Empowerteen

Guest Speaker: Dr. Paula Pilcher
- Forbes Research Article
- Worked at Merlo Station High School
- Wellness Class at Aloha HS
- After School Class (a piece to help with early release Wednesdays)
- Data Collection
- Pre- & Post Questionnaires

- Feedback at the end of the program “how did you feel on the first day, how did you feel on the last day?”
- Video of testimonials from kids at camp. Interns helped her with these videos.
- www.empowerteen.org
- Middle School Boys Retreat this summer in THPRD catalog

Presentation: Internet and Digital Profile Safety/Dangers of Technology

Guest Speaker: Matt Cline, Cedar Park's Safety Resource Officer
Officer Kevin McDonald

There are 7 School Resource Officers’s (SRO’s) in Beaverton Police Department for 45K students in BSD (2016 stats)

Why is technology dangerous?
Unrestricted access to information.
Constantly evolving.
Millennials.
Stranger Danger??
YouTube Proxy VPN (Virtual Private Network) Jailbreak

Top 10 Cyber-Risks
Cyberbaiting, Cyberbullying, Cybermobbing, Cyberstalking, Sexting, Extortion, Outing, Impersonation, Phishing, Malware/Ransom ware. We’ll touch on a few.

- Cyberbullying is often done anonymously, causing additional stress to the victim.
- Cybermobbing is a type of bullying that involves a group sharing the same malicious mindset to harm.
- Sexting: Crimes like Harassment, Encouraging Child Sexual Abuse I & II
- What is Meta Data - embedded in pictures. Apps are built around Meta Data. Provides info like camera used, time of photo, pixels and GPS locations. Can pinpoint where a photo was taken. Your address not on the profile doesn’t mean motivated people can’t find it. FB does strip meta data on images.
- Sextortion: a form of sexual exploitation where people are extorted with a sexually explicit image, etc. Your child does not need to have had previous contact with the suspect. Think of your webcam as an open window.
- Impersonation also known as Catfishing. Common on dating websites. People creating accounts under fake names or photographs. These deceptions can lead to relationship or bullying issues. Many students have reported social media acts under their name that do not belong to them.

Malware/Ransomware: Tips for home safety.
Always use Anti-Virus Software (even on Macs)
Update iOS, Anti-Virus, Windows to newest versions of everything
Don’t use Free Wi-Fi
Turn off your Bluetooth when not using it
Change your passwords often. 16-64 characters.

Most Popular Apps:
Twitter, Instagram (Sinsta/Secret Instagram), KIK, SnapChat, Facebook, Tumblr, YouTube
Video game chat rooms: Playstation & Xbox
Less Common:

Omegal, Chat Roullete, Vine, Skype, ask.fm, Yik Yak, StreamdIn, Meetme, Whatsapp, Text Free
Chat for Omegle (Talk with Strangers)

Trending this week: Go into the app store on your phone. Hit trending…list changes all the time, with hot items at the top. VPN's are popular too.

Hidden photos in Apps, typically disguised as calculator.
Secret photos KYMS Free Hide (calculator) Flashlight App, Lock Photo, etc.

So what do you worry about
- Monitor friends of your kids. Know the way they conduct themselves.
- Monitor all accounts
- Have your kids passwords and check daily to make sure they were not changed.

When do I talk to my child about this?
- As soon as you provide your child with a phone or any way to access the internet. Once you do that know you have invited strangers into your home.

What can you do?
- Require your kids to give you their passwords
- Have fake accounts to monitor them
- No phone after 8pm
- No phone outside main living areas (not in bedrooms)
- Check their phone - let them know it is not private and you will check it and the records.
- Contact your wireless provider and put parental restrictions in place.
- Disable the camera.
- Any device that has Wi-Fi can access social media apps, call and text.

Ways to monitor accounts:
- Wireless provider parental control: MMGuardian, Baracuda, Bluecoat, Cisco, Symantec, Websense, Wavecrest, OpenDNS, NetNanny, My Mobile Watchdog, My Social Watchdog, Spector Soft, Zscaler, Lightspeed, Edgewave, McAfee, M86, Foritnet, iBoss
- Set controls on your home router.

Online Resources:

National Center for Missing and Exploited Children
www.missingkids.com 1-800-843-5678
netsmartz.org
kidsmartz.org
stopbullying.gov