TECH-Knowledge-y Newsletter

May 2020: The Remote Edition 2.0

Your Ed-Tech Specialists:

James Doyle

jdoyle@oceanschools.org

Make an appointment Jamie . . .

Kristin McKenna

kmckenna@oceanschools.org

Make an appointment Kristin . . .

Website

Elementary

PDF to Digital Activity

With access to TpT, teachers accumulate a ton of PDF's that would be useful to print out, but now with remote learning how can we make them digital? The *snipping tool* is a helpful tool that allows you to take just a page of a PDF and then make it digital. Instead of inserting the entire PDF into your Google Classroom, the snipping takes a screenshot of the area you need and then saves that image to your computer. From there all you need to do is set it as a background in Google Slides and add text boxes. Your PDF has now become a digital activity you can post in your classroom for your students. Check out this video on the snipping tool.

Technology Ed-Camps

The technology department will be running a series of Ed-Camps as a chance for teachers to share the ways they are using technology during the remote teaching process. If you are doing something new and think it would be helpful to your colleagues, reach out to Pat O'Neill (poneill@oceanschools.org) so you can be a part of our next PD session. There are so many amazing things the teachers in our district are doing, and why not learning from the best. Check out our first event. Thank you to Traci O'Neill, Ryan Pringle, and Karolanne Konefal for presenting.

Your Ed-Tech Specialist:

Derek Tranchina

dtranchina@oceanschools.org

Your Media Specialist:

Mike Huston

jhuston@oceanschools.org

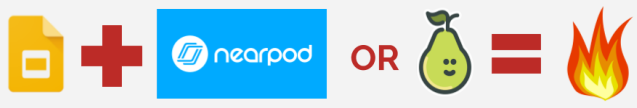
Make an appointment . . .

Website

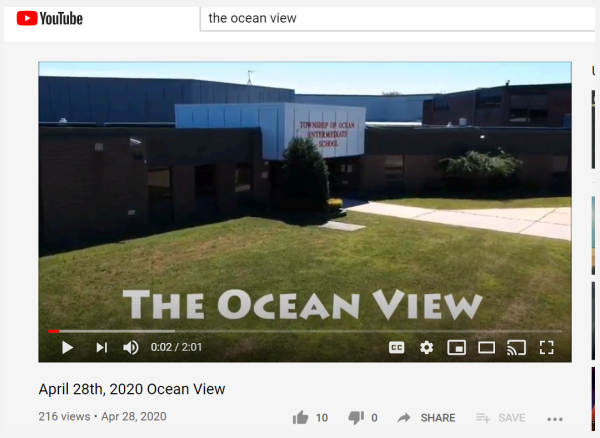
TOIS

Fun with Google Slides

Want to take your Virtual Lessons to the next level? Consider using Google Slides to create engaging, collaborative activities for students. These could also work for ongoing, interactive "digital notebooks." Feel free to use these Interactive Slide Templates *(file > make a copy)* or go above and beyond with Peardeck or Nearpod.



The Ocean View Is Back



For the latest in remote learning from TOIS subscribe to our morning YouTube show which is airing Tuesdays and Thursdays during school building closures. Also, please share pictures and videos of you and your family during remote learning and we'll air them on the show. Don't forget to subscribe and like our videos!

Your Ed-Tech Specialist:

Tim Spaeth

spartanlegacy@oceanschools.org

Make an appointment . . .

Website

OTHS

Coming Soon: Virtual Ed-Camps

Stay tuned for upcoming Virtual Ed-Camp Meeting sessions in which teachers will share some successful, innovative lessons they have put together during this remote learning period. If you have a particular lesson that has been successful and could be useful to others, please reach out to me (tspaeth@oceanschools.org) to discuss. The Zoom session will be open to all staff and will feature 2-3 teachers for 8-10 minute sessions followed by some Q & A. This will be a great way to share new ideas to keep students engaged throughout remote learning. Hope to see you there!

Security Settings

To ensure safety and privacy, consider the following safety features in Zoom:

- **Enable Waiting Room:** allows you to approve everyone before they can enter the meeting
- **Turn OFF "Participants can Rename Themselves:"** keeps participants' names the same as their Google Account
- **Lock Meeting:** keep new participants from joining the meeting (in-meeting feature)
- **NEVER SHARE ZOOM LINKS OR PASSWORDS PUBLICLY!**

Follow us on Social Media

@OT_James_Doyle

@OT_KMcKenna

@DerekTranchina

@OtisMediaCenter

YouTube The Ocean View

@OTSpartanLegacy

@OTSpartanLegacy

@OTSpartanLegacy

YouTube Spartan Legacy

Network Security Notice

Brought to you by Mike Hall

Phishing Scams

- COVID-19 has not only brought a pandemic but it has also presented an opportunity for scammers and criminals to capitalize on people's fears, medical needs, curiosity, and interests, at the same time
- Look before you click: While phishing emails have become quite sophisticated, be wary of emails that have bad grammar, misspellings, unfamiliar greetings, and those claiming immediate action or attention. Refrain from clicking on links, opening attachments, or downloading files unless they are from a known sender.
- Google has seen more than 18 million daily malware and phishing emails related to COVID-19 alone within the last couple of weeks. There has been many more types including

Related Links:

- https://www.comodo.com/resources/home/what-are-phishing-scams.php
- https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620
- https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email
- https://www.bankrate.com/personal-finance/common-coronavirus-scams-to-watch-out-for/
- https://www.computerworld.com/article/3538470/how-to-protect-against-apple-phishing-scams.html

Secure Your Passwords

Create A Strong, Long Passphrase

- Strong passwords make it significantly more difficult for hackers to crack and break into systems. Strong passwords are considered over eight characters in length and made up of both upper and lowercase letters, numbers, and symbols. Create long passphrases that are easy to remember and difficult to crack. A best practice is to generate passwords of up to 64 characters, including spaces.

Once you've created a strong password, you should follow these guidelines to keep it secure:

Implement Two-Factor Authentication

- Two-factor authentication has fast become a standard for managing access to organizational resources. In addition to traditional credentials like username and password, users have to confirm their identity with a one-time code sent to their mobile device or using a personalized USB token. The idea is that with two-factor (or multi-factor) authentication, guessing or cracking the password alone is not enough for an attacker to gain access.
    - https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en

- Don't share a Password
- Don't share a password with anyone. Not even a friend or family member.
- Never Send a Password
- Never send a password by email, instant message, or any other means of communication that is not reliably secure.
- Avoid Storing Passwords
- Avoid storing passwords either digitally or on paper, as this information can be stolen by those with malicious motives.
- Use Different Passwords for Every Account
    - Otherwise, if one account is breached, other accounts with the same credentials can easily by compromised

Secure Your Mobile Phone

- Mobile phones are now commonly used to conduct business, shop, and more, but bring with them many security concerns. Protect your phone and other mobile devices from hackers by securing your phone with a strong password, fingerprint, or facial recognition passwords.
- Related Links:
    - https://www.fbi.gov/video-repository/protected-voices-passphrases-and-mfa-102319.mp4/view
    - https://support.microsoft.com/en-us/help/4091450