

# Privacy Best Practices for Parents

## Welcome from your session facilitators:

- Pam Davis, ACES  
Educational Technology
- Jim Moyle, ACES  
Educational Technology
- Wanda Wagner, ACES  
Educational Technology

## Guidelines for a successful session:

- Please turn off your video.
- Please mute your microphones.
- Introduce yourself in the chat area.
- Place questions in the chat area during the session.
- Click 'raise hand' to be recognized, then unmute and turn on video when speaking.



Educational Technology

# Purpose and Outline

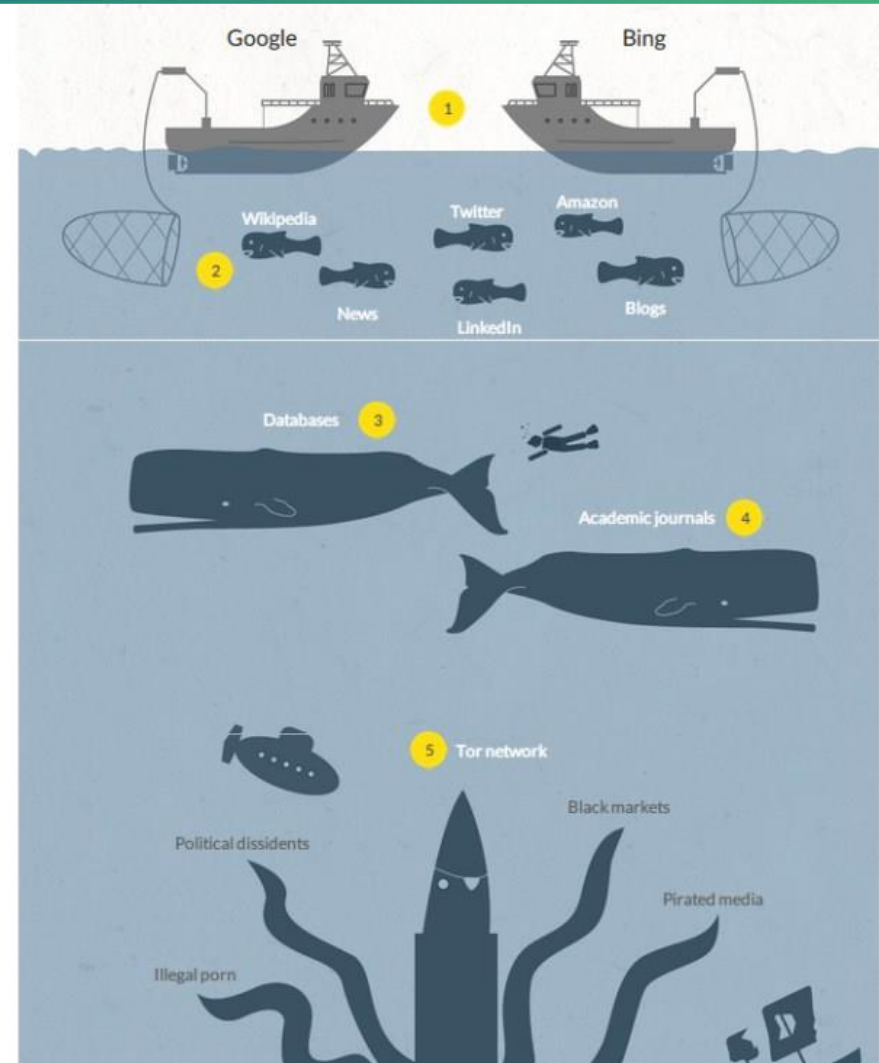
- Purpose: Review the ACES code of conduct for responsible use of technology. The code of conduct includes best practices that help protect your child's information and experiences online. Learn about how the ACES Technology Leadership Committee vets applications to be used by students with a four step process, including the CT student data privacy act and privacy contracts that each vendor must sign.
- Outline:
  - The why: Keeping students safe – ACES website resources
    - Process to vet applications – ACES Technology Leadership Committee
    - Parent guide
    - List of vetted applications
  - The how: Best practices
    - ACES code of conduct for responsible use of technology
    - Think before using email
    - Store data in secure sites
    - Login and logout
    - Watch for paper trails

# The why: Keeping students safe

Using and protecting personal and health information in secure and responsible ways is at the heart of our efforts to provide a richer, more dynamic, safer, and more personalized learning experience for all learners and staff at ACES.

# The why: Surface, dark, and deep web predators

- Layers 1 and 2 = surface web
  - 10% of the content on the web
  - Standard Google searches and web sites
  - Amazon, CNN, WebMD
- Layers 3 and 4 = deep web
  - 85% of invited or password protected sites
  - Bank of America, government resources, databases, university sites, academic journals
- Layer 5 = dark web
  - 5% of web
  - Unregulated sites that provide anonymity to users
  - Silk Road, Shadow Creak



# The why: Predator targets

Criminals on the dark web target all of the below groups. Which group is MOST targeted? (AARP, 2018)

- Senior citizens
- Elementary students
- People with their names and emails posted on websites

Answer in the online poll.



# The why: Human error

Criminals on the dark web target all of the below groups. Which group is MOST targeted?

- Senior citizens
- **Elementary students**
- People with their names and emails posted on websites

Data privacy is only as good as the end-users.

- 95% of all data breaches happen from human error



# The how: Data privacy at ACES

- Keeping students safe – [ACES resources](#) and [parent flyer](#)
  - Data privacy laws
    - Family Education Rights & Privacy Act (FERPA)
    - Children’s Online Privacy Protection Act (COPPA)
    - Children’s Internet Protection Act (CIPA)
    - Protection of Pupil Rights Amendment (PPRA)
    - CT Student Data Privacy Law
  - Process to vet applications – ACES Technology Leadership Committee
    - Stage 1: Privacy review
    - Stage 2: Curriculum review
    - Stage 3: Technology security review
    - Stage 4: Budget review
  - [List of vetted applications](#)

# The how: Best practices – RUP/AUP

ACES [code of conduct for responsible use of technology](#)



Educational use



Filtering and the internet



Respect privacy



Protect your password



Respect property



Respect your network



Be polite and kind



Communicate and collaborate online



Respect the law



Maintenance, updates and repairs

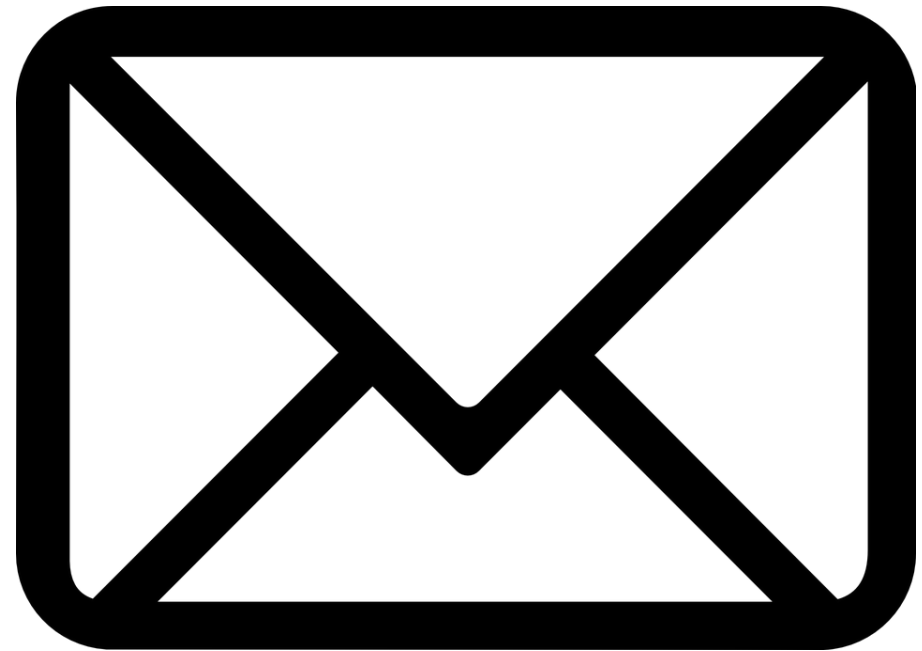


Keep personal information private



# The how: Best practices - Email

- Decide whether email is the best communication channel
- Less is more, perhaps request a phone call
- Watch out for “reply to all” and forwarding threads of conversations
- Ask permission to forward



# The how: Best practices – Save work

- Store data in secure sites
- Student work should be saved in Google Classroom and Google Drive
- FERPA compliant and backed up
- Cautions
  - Deleted files are removed every 30 days
  - Students may have collaborative, group work assignments
  - Share documents wisely
  - Cite other's work



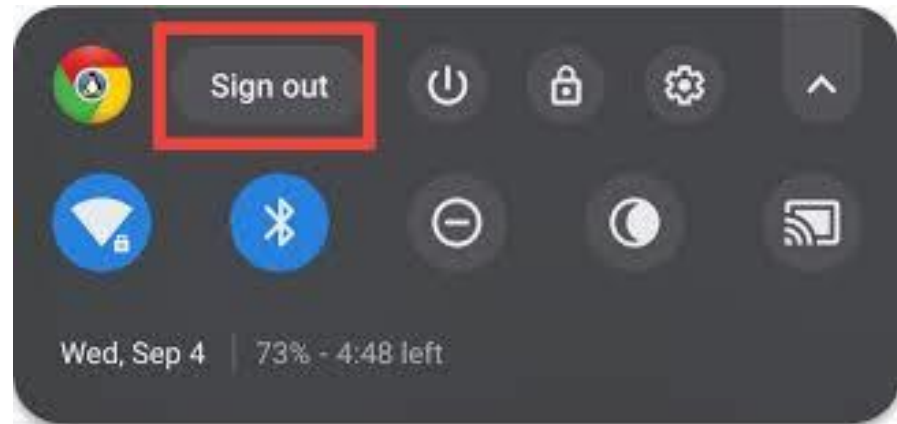
# The how: Best practices – Log ins

When not is use ...

... log out of applications

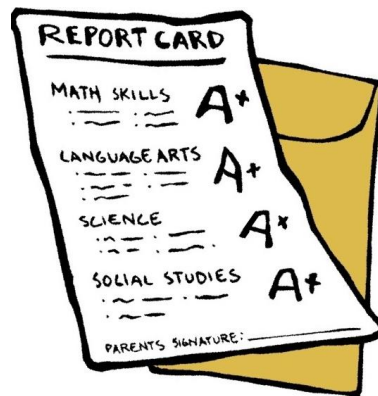
... log out of your Chromebook

... power off (helps signal upgrade installs)



# The how: Best practices – paper trail

- Watch for paper trails
- Security goes beyond electronic devices
- Secure documents with personally identifiable information
- Shred paper versus placing in the trash can
- If you must travel with confidential paper documents, use a locked, secure case



# Resource References

ACES (2020). ACES code of conduct and responsible use. Retrieved from [https://www.aces.org/uploads/application/files/2019-2020\\_aces\\_aup\\_kid-friendly\\_6-12.pdf](https://www.aces.org/uploads/application/files/2019-2020_aces_aup_kid-friendly_6-12.pdf)

ACES (2020). Data privacy practices @ ACES. Retrieved from <https://www.aces.org/schools-programs/school-based-services/educational-technology/data-privacy-practices>

ACES (2020). Our commitment to parents: Clear data privacy practices @ ACES. Retrieved from [https://www.aces.org/uploads/files/School-Based%20Services/Curriculum/Parent\\_Preliminary\\_Overview\\_to\\_Student\\_Data\\_Privacy\\_Act\\_\(1\).pdf](https://www.aces.org/uploads/files/School-Based%20Services/Curriculum/Parent_Preliminary_Overview_to_Student_Data_Privacy_Act_(1).pdf)

ACES (2020). Vetted applications used at ACES. Retrieved from <https://edprivacy.educationframework.com/Districts/main.aspx?districtid=30109>

aces

Educational Technology