Digital Classrooms in the time of COVID – Records, Recordings, and Privacy

Best Practices to protect educators and students

The COVID crisis has caused a shift to online and remote learning. The platforms and systems used to deliver instruction provide solutions to bringing learning to students but, also bring with them challenges and possible risks (privacy, security, and legal). Many of these risks and challenges are complex and will require understanding of rights provided by both by privacy laws (federal and state) and collective bargaining agreements.

This document primarily focuses on suggested best practices for implementing digital remote learning models to protect both students and staff in the virtual classroom.

Best Practices for Educators Using "Ed Tech" and Digital Communication

1. Know What Protections and Rights Exist under the Collective Bargaining Agreement
   - Many CBA include some privacy protections for educators, such as prohibiting the use of video recordings for evaluative or disciplinary purposes. Determine whether these protections would also apply to a virtual learning model.

2. Know and Follow District Policies Related to Use Technology
   - District email policies may require educators to use encryption software or other technology to safely transmit education records electronically.
   - Districts are best positioned to vet security and privacy features, check for a pre-approved list of technology providers and applications before using.
     - If the district does not have approved list, educators should seek district assistance before using products.
   - Be aware of district policies around student and staff use of technology and how it may relate to the current remote learning model.

3. Use District-Provided Technology and District-Approved Platforms Whenever Possible
   - The use of personal cell phones, computers or other electronic devices could subject those devices to search by the District in response to a request under the state's Public Records Act.
   - If a district will not provide educators with district-owned cell phones, there are apps and other products available to allow an educator to text or communicate with students and families without divulging the educator's personal cell phone number.
   - Applications or products specifically created for educational purposes are more likely to account for student privacy laws.

4. Employ Reasonable Safeguards to Prevent Unauthorized Disclosure of Student Records
   - If possible, student education records should be kept in a secure, locked cabinet.
   - Strong passwords should be used to protect work accounts and should not be shared with anyone, including members of the educator's household.
   - To the extent possible, live interactions with students that could result in the disclosure of PII should be conducted in private areas where members of the educator's household cannot overhear. If it is not possible to conduct such interactions in private, obtain proper parental consent for any inadvertent disclosures.

5. Learn About Technology Features and Privacy Settings
    - Even district-approved or district-provided products could create privacy issues depending on how they are used, so understanding the product and its settings can help prevent inadvertent disclosure.

6. Supervision of student to student interactions: Virtual breakout rooms – Private chats
    - Just like in a brick and mortar classroom, there may be times when students engage with each other without direct supervision of the teacher for group work or discussions.
        - Virtual breakout rooms - The use of these rooms does not place a legal liability onto the teacher. However, best practice would be to provide some form of adult supervision to the group by visiting each breakout room or assigning a paraeducator to supervise.
        - Private Chat – Consider changing the settings to limit private interactions between students. In addition, saving a record of the chat to a district cloud may be advised to document any interaction that may have taken place.
    - Know how the security features work in the platform you are using in these situations.

7. Meeting with student one on one.
    - It is not advised to meet one on one as a regular occurrence.
    - When it is necessary to meet with an individual student due to the conversation being protected by FERPA, it is advised that the educator consider requesting support of another adult in the meeting.
        - This might be a paraeducator, administrator, student's parent, or another educator.
    - When having another adult present is not an option, the educator should consider notifying the building administer that the meeting is taking place and then taking steps to record the meeting following district policies and procedures.

8. When in Doubt, Obtain (and Document) Parental Consent
    - The potential for different laws to apply in different context makes it wise to err on the side of obtaining consent even where doing so is not clearly required.
    - Note: Consent usually must meet certain requirements such as specifying the information to be collected/disclosed. The Department of Education has provided sample consent forms for districts to use and/or adapt.

Links and Resources:
USDOE: https://studentprivacy.ed.gov

- UDOE FERPA & COVID-19 FAQs:
  https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf
- UDOE FERPA & Virtual Learning Resource List
  https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20%20Virtual%20Learning%20032020_FINAL.pdf

- UDOE FAQs on Photos and Videos under FERPA
  https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa