

Procedures for Protecting Student Privacy In Remote Environments

During Phase 1 and Phase 2 during the 2020-21 school year we will be using video livestream and recording to deliver instruction in a remote environment. There is a collection of federal and state regulations that apply and the purpose of this document is to clarify facts and provide guidance to teachers as we use digital tools in their instruction. Educators are covered under the district's malpractice insurance should a concern arise so long as district policies and procedures are followed. Parents and students should be fully informed as to the use of student information in this remote environment.

[A statement for each course syllabus and digital classroom is included below.](#)

Student Privacy Protections

In Auburn-Washburn we take student privacy seriously. Students and parents are informed about the manner in which remote instruction will include the use of online platforms, video streaming and recording. Digital safety and citizenship skills are included in each class to ensure that students know how to safely navigate the online classroom. These skills include: the ability to curate reliable information, to interact safely and lawfully online, including cyberbullying, hacking and the unauthorized disclosure, use and dissemination of personal information. Because instruction will be occurring in students' homes, parents and other household members are also notified of the following:

- a. Auburn Washburn Board Policy KGB prohibits the recording of any students, employees, surreptitiously or through the use of concealed audio and/or visual recording devices.
- b. Recorded classroom instruction and communication will be posted only on private online sites that are not publicly searchable for the purpose of making that information available to students as needed.
- c. Student information subject to protections under the Family Educational Rights and Privacy Act (FERPA) and the Health Information Portability and Accountability Act (HIPPA) will be shared with written parental consent only.
- d. Students will be educated about privacy settings that are included with District-issued technology devices and digital tools.

Student Privacy Laws

DIRECTORY INFORMATION

The USD 437 Board of Education and administration have determined that the following data will be designated “directory information”:

1. Student’s name, address, telephone number,, and date of birth.
2. Student participation in officially recognized school activities and sports.
3. The weight, height, and grade of members of athletic teams.
4. The dates of attendance.
5. Scholarships and awards received.
6. The most recent previous school district attended by the student.
7. Audio or visual recording, photograph, or image of the student.
8. Student’s school email address as provided by USD 437

**This information is considered public information which may be released by the school district without parents’ prior consent. Parents need to let each school know by September 1 if they do not want this information released.

All other student information is covered by the following regulations.

1. Family Educational Rights and Privacy Act (FERPA)

Most educators are aware of the Family Educational Rights and Privacy Act (FERPA) which requires parental consent to share a student’s identifiable information when that information is maintained by the district.

2. Health Information Portability and Accountability Act (HIPPA)

In this environment, educators need to be very mindful of the privacy protections of HIPPA. All information regarding medical, one-on-one and group counselling, or other special education related services is highly sensitive and can only be shared with parental consent.

3. Children’s Internet Protection Act (CIPA)

The implications of CIPA come into play as students use district-owned devices to access the Internet in their own homes, or if the district is providing internet access in the student’s home. In the remote learning environment it is not possible to monitor the content that may be accessed at home. Therefore it is important that the district and educators provide parents and students with information about potentially harmful material.

4. Breach of Privacy (K.S.A. 21-6101)

In Kansas, it is generally acceptable for any party to a conversation to record that conversation unless a more specific law or policy prohibits it. Our district policy does prohibit it:

Concealed Observations (See JGGA) KGB

Unless otherwise provided in this policy or policy JGGA, **individuals are prohibited from recording students, employees, and/or board members surreptitiously** or through the use of concealed audio and/or visual recording devices.

This prohibition is in effect at school, on or in district property, and at meetings and conferences held for educational or disciplinary purposes.

Guidelines for Educators for Remote Instruction

- A. Educators must be aware of any student whose parent has opted out of the sharing of directory information.
- B. Live streaming class discussions, student interactions, or direct instruction by the teacher is permitted without parental consent because we are not maintaining a record of that interaction.
- C. Recorded direct instruction by the teacher is permitted without parental consent so long as the only student information that is included in the recording is the student's name, voice and/or picture. A way to accomplish this would be to use a screen sharing setting with or without a video of the teacher displayed on the screen. If student' interaction with the course content is not displayed on the recording, the session can be recorded without parental consent.
- D. If the recording does include student information that would be personally identifiable information (such as interacting with the course content, grades on an assignment, accommodations provided under an IEP or 504 plan, etc.) **AND** the recording is digitally posted on a platform that has restricted access, **AND** only accessible to the students in that class, no parental consent is needed. This includes: a mp4 file on Google Classroom, SeeSaw, YouTube (as long as the file is marked "private") as these files are not publicly searchable.
- E. There is no legal requirement that requires an educator to record instructional sessions with students, either in a class setting or one-to-one sessions as these are regarded as classroom communications.
- F. Health related information or any information related to individual counselling or therapy (this does NOT include school counselling around school-related behavior, or academics), special education medical services (such as OT, PT, nursing), etc. should NOT be shared on online platforms, recorded or live streamed. The exception for our district is for Social Workers and Speech/Language Pathologists who have a professional Zoom license which meets HIPPA requirements.
- G. Educators should teach students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness and response, warnings regarding inappropriate matter on the internet, safely and securely using electronic mail and platforms, unauthorized access, "hacking" and other unlawful activities online, and unauthorized disclosure, and use and dissemination of personal information. A statement to this effect is provided above and educators are encouraged to include it in their course syllabus and parent communication.
- H. Educators should communicate with students and parents what tools will be used in online instruction, how those tools will be used, how material may be recorded, shared and used, and how to adjust settings on the student's device to minimize any privacy concerns. A statement to this effect is provided above and educators are encouraged to include it in their course syllabus and parent communication.