Important FERPA Reminders in an E-Learning or Virtual Environment

The Family Educational Rights and Privacy Act, a federal law, protects the privacy of student education records and gives parents certain rights with respect to their children's education records.

With certain exceptions, FERPA requires that Lexington County School District One obtain the written consent of a parent or, if the student is over 18 years of age, the written consent of the student, prior to the disclosure of personally identifiable information from a child's education records. Disclosure of a child's PII without the proper consent could constitute a violation of FERPA.

Even though what we are all experiencing is unprecedented, the laws and district policies regarding FERPA and/or confidentiality do not change.

Directory Information

Directory information deals with personally identifiable information in each child's educational records and information that the district maintains through PowerSchool, for instance.

This is information that schools use as part of the daily educational process (such as grades, home address, telephone numbers) and for internal use in honor rolls, annuals, height and weight for basketball, football or wrestling programs, recognition lists, newsletters, playbills, programs (including graduation and athletic programs), etc.

The release of directory information does not require prior consent. However, if parents do not want the district to release some or all of their child's directory information without prior written consent, they must notify the district in writing by completing the Directory Information Form.

Anything that directly identifies or could potentially identify a student, staff member, or their families may be a violation of the district's confidentiality policies.

Student Media Consent and Release

Over the years, the district realized that the press/media's use of newer forms of communication were blurring the lines of parent/guardian consent and making it more difficult to communicate to parents what they were consenting to release. As newspapers and television stations began to use social media (Twitter, Facebook, Instagram) and their own websites to communicate news, it became important to be more specific when we asked for parent permission.

The Student Media Consent and Release Form allows us to determine whether parents want their children to appear in any form of social media or media that has the potential to be public such as the district's own social media posts, television or newspaper stories and photographs, internal or external videos, radio interviews, newsletters, publications, etc.

At the beginning of the year, each student's parent or legal guardian is asked, through the Student Media Consent and Release Form, to give Lexington District One and its employees, representatives and authorized media organizations permission to print, photograph and record their child for use in audio, video, film or any other electronic, digital or printed media.

Confidential Information Tips

- Don't talk about individual students, their programs or their progress with others.
- Don't use student names in conversations about your work.
- Don't get drawn into conversations or questions about your work at ball games, grocery stores, restaurants, parties or any other community setting.
- Even at school, keep your conversations about students confidential. Not everyone at the school has a "need to know," an important part of FERPA.

E-learning, Virtual Classroom Tips

- Only Lexington District One students and staff should be allowed to join Zoom meetings. This helps prevent the accidental sharing of sensitive information, limits disruptions and helps protect their privacy.
- No videoconference or Zoom information should be posted online.
- You should not post anything related to students in your classrooms, whether face to face or virtual, on social media (Facebook, Instagram, Twitter, etc.) without specific permission for each post or photograph, as all of these could identify students either directly or indirectly. If all your students' parents/legal guardians gave permission for social media postings through the annual Student Media Consent and Release Form, you should still be very careful about what you post.
- As you go about teaching and learning in the virtual environment, do not share documents, information, lists, etc. that include personal information such as date of birth, Social Security Number, South Carolina Department of Education State ID, health conditions, etc.
- Be careful in your conversations with others. For instance, you should not say "a girl in my fourth block with diabetes" or "I heard that one of my second graders' families has been quarantined." Any unnecessary communications, such as verbal conversations and text messages, about a student's illness or potential illness may violate FERPA's nondisclosure provisions.
- Schools need to consider if and how they will store videos that capture students' voices and faces. If you record live-streamed classes and keep video files that contain student information, these files may become "education records" as defined by FERPA. Education records cannot be shared without parental permission.
- For the purposes of Schoology, any lesson recorded is considered instruction and possibly an educational record. Recorded lessons on Schoology or other learning platforms cannot be shared outside of those platforms, on any social media, or with anyone other than students and teachers in that classroom.
- Set community norms and rules around not taking screenshots or recording the session on a separate device. For instance, when students join with video, they may reveal some personal information about their lives such as what their house looks like or how many other people live there. The feed could catch children in moments they might not want to broadcast. Please take the time to explore the Active Management of the Virtual Classroom module provided by the district's Professional Learning Office for support on how to create norms with your students.
- Teachers should also encourage students to maintain and abide by the recommendations in this document.

Tips to make your virtual classroom more secure

- Teachers should take steps to secure access to their virtual classroom, so that only students can come in.
- When you are in the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up box, you will see a button that says Lock Meeting. When you lock the meeting, no new participants can join, even if they have the meeting ID and password.
- If something unexpected happens, you can put a participant back in the waiting room. This allows the teacher to let them back in the room later.
- The Remove feature eliminates unwanted participants and prevents them from entering the meeting room again. Only use Remove if you intend to never allow that participant to join the meeting room again.
- While in the Participants menu, you can mouse over a participant's name and several options will appear including Remove. Click Remove to delete a participant from the meeting. They cannot get back in if you then click Lock Meeting.
- You may also want to prevent participants from sharing their screen. In the host controls, click the arrow next to Share Screen and click Advanced Sharing Options. Under Who can share? choose Only Host and close the window.
- Teachers can turn students' video off to block unwanted, distracting or inappropriate gestures.
- Teachers can also mute and unmute individual participants or everyone to block unwanted, distracting or inappropriate noises.
- Zoom has a "Tips and Tricks: Teachers Educating on Zoom" document that has other useful information.