QUESTIONS: Contact the Registrar at 706-446-1430 or at Registrar@augusta.edu

FERPA in a Remote or Virtual Environment

Faculty and staff have an obligation under the law to protect student information in the Education Record as defined by FERPA. FERPA-protected information (FPI) includes Personally Identifiable Information (PII), grades, graded papers, exams, transcripts, and notes from a conversation with or about a student that are placed in a student's file. PII includes things such as Name, ID Number, Social Security number, DOB, or other information which, when used alone or in a combination with other non-identifiable information may allow for identification of the student.

Official AU Guidance:

Faculty and staff should utilize only Augusta University's endorsed, licensed, and supported tools as identified in the table below when 1) providing instruction, 2) delivering course material, or 3) communicating with a student, colleague, or administrator about FERPA-protected information (FPI).

Each method and tool is listed below, with guidelines provided for their use. ***SECURE*** *indicates that the tool or feature/function can be used to communicate or store FPI.* ***NOT SECURE*** *indicates that the tool or feature CANNOT be used to communicate or store FPI.*

[NOTE: While there is much publicity about Zoom and its usage by other USG institutions, our faculty and staff should not use Zoom or any other tool beyond those listed below, as they are not licensed or supported at this time.]

Tool	Information

Teams	Teams provides a way for general collaboration, remote meetings, file and app sharing.
	• **SECURE for NON-RECORDED Video Conferencing and NON-RECORDED Screen Sharing**, **if**
	  o The student is on notice that the discussion will include FPI
	  o The student is on notice that it is their responsibility to ensure that no one on their end will be able to see the screen or hear the conversation (unless they approve).
	  o The faculty/staff member ensures that no one on their end will be able to see the screen or hear the conversation.
	  o The faculty/staff member ensures that s/he does not share FPI for other students (like an entire gradebook) when screen sharing.
	• **NOT SECURE** for file sharing through the Teams platform
	• **NOT SECURE** for chat through Teams
	
	Note: You may use the chat, file sharing, and recording functions for instruction and course delivery as long as no FPI is communicated or shared.

WebEx	WebEx is a collaboration tool providing faculty a convenient way to meet "live" with students and colleagues, conduct online office hours, and even feature guest speakers. When scheduling a meeting with a student, passwords should be so that only those authorized can enter the meeting.
	• **SECURE for NON-RECORDED Video Conferencing and NON-RECORDED Screen Sharing, if**
	  o The student is on notice that the discussion will include FPI
	  o The student is on notice that it is their responsibility to ensure that no one on their end will be able to see the screen or hear the conversation (unless they approve).
	  o The faculty/staff member ensures that no one on their end will be able to see the screen or hear the conversation.
	  o The faculty/staff member ensures that s/he does not share FPI for other students (like an entire gradebook) when screen sharing.
	  o The faculty/staff member ensures that no other users are signed into the video conference (the sign-in link may not be secure).
	• **NOT SECURE** for file sharing through the WebEx platform
	• **NOT SECURE** for chat through WebEx
	
	Note: *You may use the chat, file sharing, and recording functions for instruction and course delivery as long as no FPI is communicated or shared.*

D2L	**SECURE** – Faculty/staff can use D2L for communication and sharing of content with students.

Navigate	**NOT SECURE** for text function; **SECURE** for all other functions.
Email (D2L, Navigate)	**SECURE** - Emailing through D2L or Navigate is the safest ***email*** option for contact with students when FERPA protected information is included in the correspondence. It is strongly recommended that, as a best practice, you follow the guidelines listed below for Outlook email even when you utilize D2L and Navigate for email.
Email (Outlook)	**NOT RECOMMENDED** – Because there is a risk of sharing information you did not intend or sharing information to a person that should not receive it, sharing FPI through Outlook email is not recommended. In the case that there is no other approved method to use, FPI ***may*** be shared using Outlook email and is **considered SECURE if communication adheres to the Acceptable Use of Electronic Mail & Electronic Messaging Policy**. This policy indicates that only encrypted PII may be sent via AU's official email, and the following security measures must be followed: • Electronic messages containing PII may not be sent or received except with a device that has been secured in compliance with AU's security policies and procedures. • The Personally Identifiable Information in the email must be limited to the minimum information necessary. • AU personnel must use their official AU email account to send and receive properly encrypted PII and they may not use any other email accounts (for example, Google or Yahoo accounts) for that purpose. • PII may only be sent by encrypted email after the recipient's address has been carefully verified (for example, from a directory or a previous email) and entered correctly. • Always check any attachment you are sending to make sure you have attached the correct information.
Phone	**SECURE if** • The student is on notice that the discussion will include FPI • The student is on notice that it is their responsibility to ensure that no one on their end will be able to hear the conversation (unless they approve). • The faculty/staff member ensures that no one on their end will be able to hear the conversation. • The faculty/staff member uses reasonable methods to identify and authenticate the identity of the person the information is being disclosed to. Typically, an individual's identity is authenticated through the use of one or more factors known or possessed only by the person you are disclosing the information to. The choice of the specific authentication method may vary depending upon the level of sensitivity of the data and the type of information the person providing the information has access to validate. Contact the Registrar's Office at 706-446-1430 or at Registrar@augusta.edu for assistance if you cannot identify and authenticate the identity of a person you are working with or if you need assistance determining your specific authentication method.
Text	**NOT SECURE** (even if text is pushed from one of the above platforms)
JagTrax	**SECURE**
Box	**SECURE** – Box is the recommended solution for storing student data if retention is necessary. Please review the PowerPoint created by the Augusta University Information Security Office and reference the proper way to secure data stored in Box. Student data stored in an electronic format must be secure and available only to those entitled to access that information. • Student data should not be stored on personal computing equipment, a hard drive, a shared computer, or a portable device such as a jump drive or laptop computer. • Student data may not be stored outside of Augusta University systems maintained and protected by Information Technology. • Box is the recommended solution for storing FPI if retention is necessary. Before retaining any sensitive information consider: • Is it absolutely necessary to retain the information? • Is this information available in a secure university system I have access to rather than creating a file that will require special attention to secure?