**Remote Working – FERPA Guidelines**

As institutions around the world change the way they are instructing classes in response to COVID-19, it is important to recognize that there are some individuals that will use these unique circumstances to try to gain access to information they should not have. Below are some general guidelines that will help you ensure that we keep our student’s private information secure.

**Discussion of Class Material**

Discussion of class materials is not part of the protected student record. The majority of your lecture will likely be conducted as usual, just through online mechanisms.

**Be Mindful of Technology**

Sharing your screen can be a great educational aid, but it may inadvertently share protected information. Take steps to ensure that any documents or applications showing protected information are closed before sharing your screen.

**Discussion of Protected Student Information**

*E-mail* Utilization of official University of Kentucky e-mail accounts is the *preferred way* to discuss any   
protected information as it resides behind a protected login.

*Video* Echo360, Skype, or Zoom are great ways to setup one-on-one meetings with students; both   
parties being able to see one another in real-time helps ensure the student’s identity. However, should protected information be discussed both parties will need to meet from private locations.

*Phone* Communication by phone is the least secure method and poses the most risks. Discussions   
occurring over the phone or via audio-only conferencing should be limited to topics that do not rely on sharing protected information.

**Management of Student Data**

When working with student data, limit yourself to using official University of Kentucky applications such as myUK, Canvas, and SAP. Refrain from downloading, printing, or otherwise removing data from UK systems if possible. Doing so increases the risks of protected information being disclosed inadvertently.

**Other Resources**

UK Faculty & Staff FERPA Information   
<https://www.uky.edu/registrar/content/facultystaff-ferpa-privacy>

Use of Technology Resources  
<https://www.uky.edu/regs/sites/www.uky.edu.regs/files/files/ar/ar10-1_2018_final.pdf>

Mobile Device Security  
<https://www.uky.edu/internalaudit/blog/mobile-device-security>

DOE Student Privacy and Policy Office March 2020 Guidance <https://content.govdelivery.com/attachments/USED/2020/03/20/file_attachments/1407008/FERPA%20&%20Virtual%20Learning%20032020.pdf>

FERPA guidelines require verification of identity within a reasonable standard when communicating with students. During this time when all interaction with students is remote, an option for advisors and faculty to be more secure in communicating with students via phone is to send to the student’s UKY email address a unique passphrase or PIN. The student would then call the advisor/faculty and provide the passphrase or PIN, confirming they were able to access it through University of Kentucky email.