FERPA Compliant Practices for Faculty & Staff

As a **UCF employee with access to student records,** you have the responsibility to protect the confidentiality of personally identifiable information (PII) in your possession.

The following items represent some FERPA best practices:

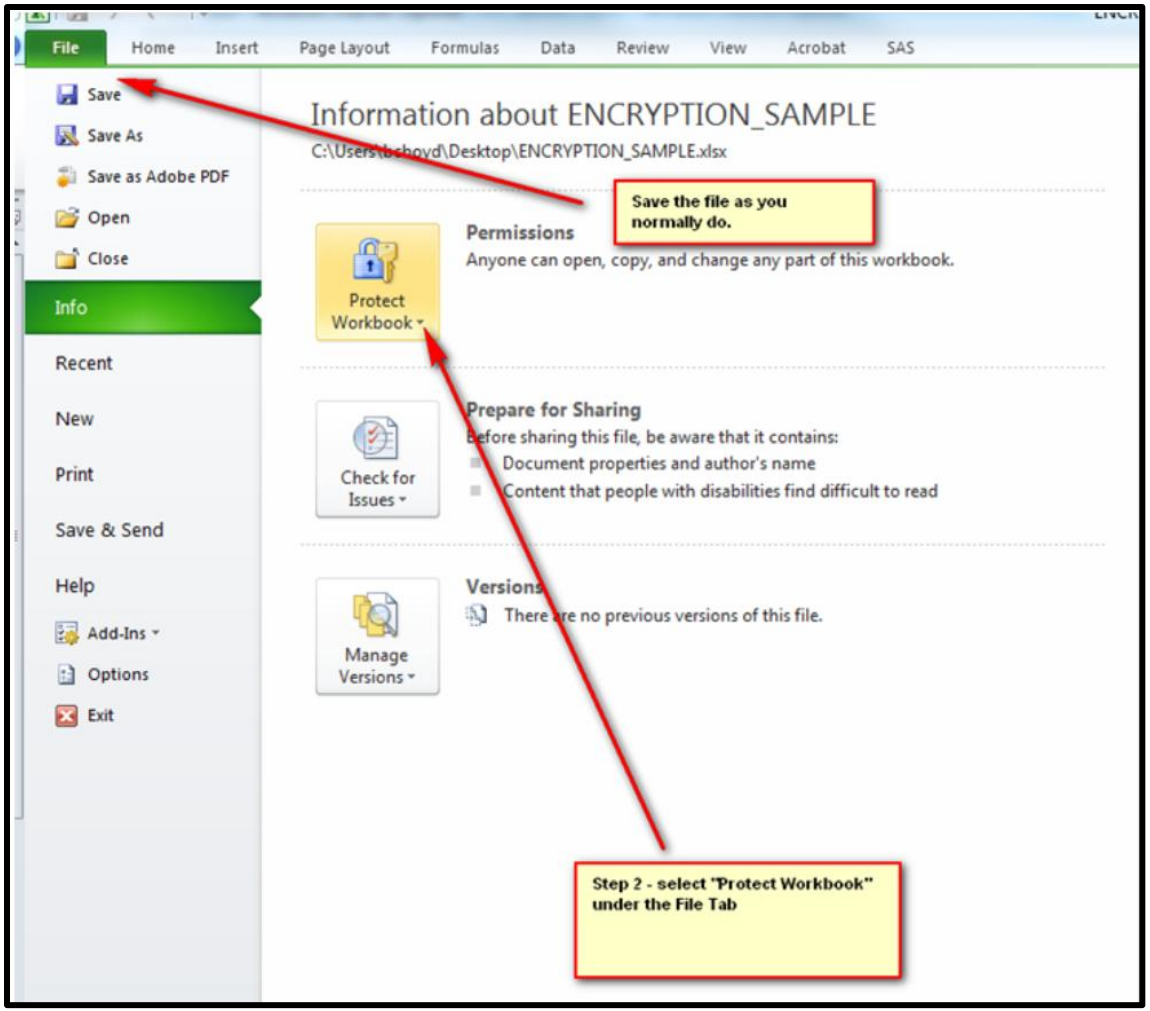
- **DO NOT** record attendance or any other student specific information by passing around the UCF class roster, which contains the student's UCFID, grades, gender, or other non-directory information.
- **DO NOT** leave graded exams, papers, or any documents containing a student's PII, unattended. Using Canvas, the university's learning management system (LMS) is the recommended vehicle for communicating grade information with your students.
- **DO NOT** discuss the progress, status or grade of any student with anyone (including parents) and do not release a student's PII without the written and signed consent of the student. Please contact your department office or the Registrar's Office if you have any questions or concerns prior to releasing any student information to third parties.
- **DO NOT** make lists of students enrolled in your class available for any commercial purpose. These requests must be routed to Analytics and Integrated Planning. https://analytics.ucf.edu/.
- **DO be careful when discussing grades or** other Personally Identifiable Information with your students via telephone or email. The identity of the recipient of those records must always be verified. Using Canvas, the university's learning management system (LMS) is the recommended vehicle for communicating grade information with your students.

How to encrypt and send sensitive data to staff or other persons with a legitimate educational interest:

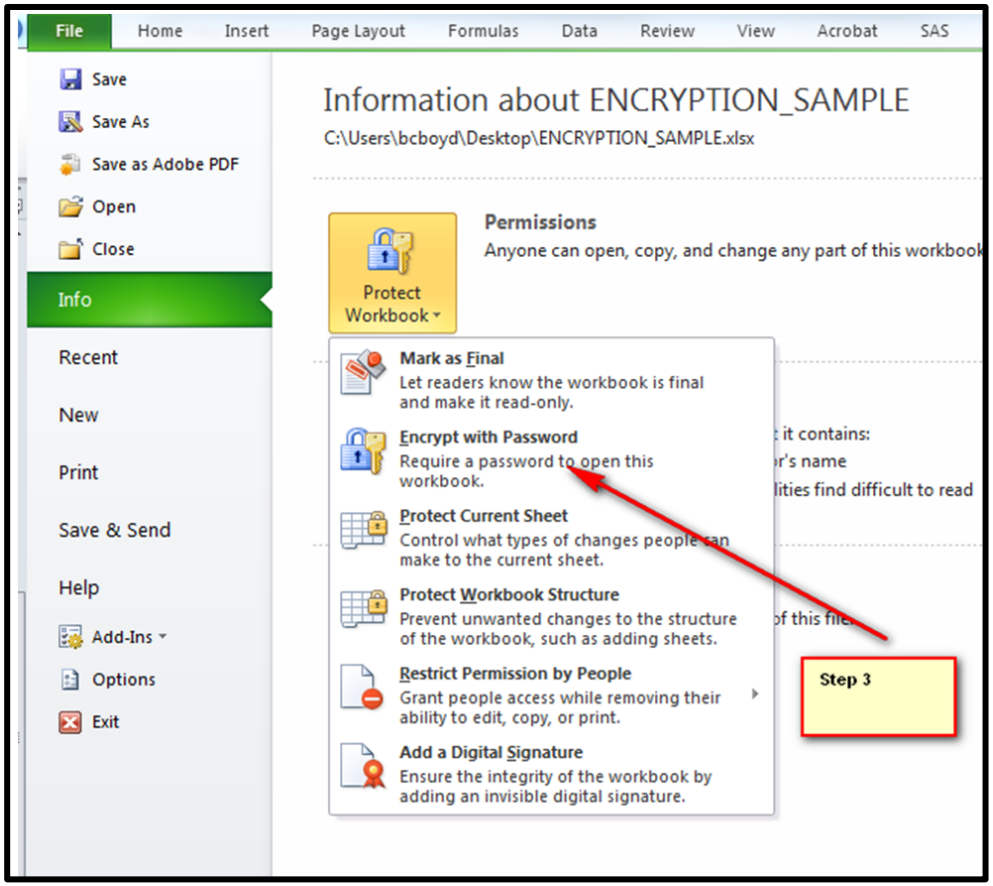
In the course of your work, sometimes it is necessary for email communications to contain sensitive data. When passing sensitive information via email to persons with a legitimate educational interest, such as a list or file that contains non-directory information, it should always be encrypted and password protected. Here are some tips on how to protect the sensitive data you are sending: You will need to save the data on a file type that can eventually be password protected. Some common examples are pdf, Word, or Excel. The following is an example illustrating an instructor passing along exam grades to a student using Excel.

Step 1 – Save and name the file as you normally do.

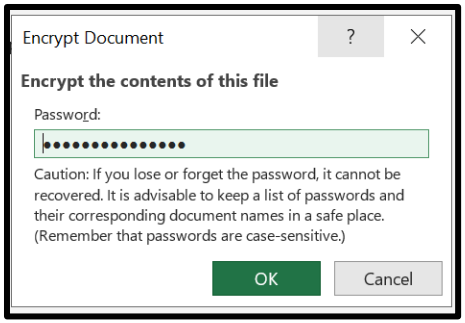
Step 2 – Select “Protect Notebook” under the Info Tab



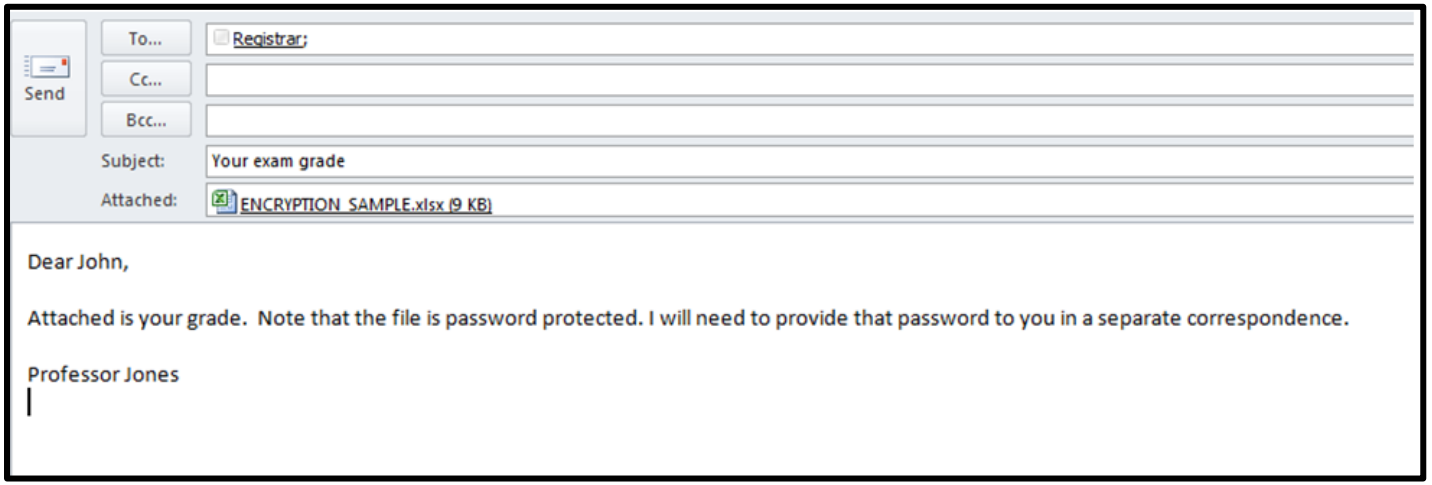
Step 3 – After clicking “Protect Notebook”, select “Encrypt with Password” from the list of options.



Step 4 – Select a password that you will need to provide to the recipient of your file. It is important that you use strong password standards when establishing a password. It is recommended that it does not contain the student's or your name that includes upper case, lower case, numbers and special characters. After setting the password, it will be necessary to save the file again.



Step 5 – If emailing the information, you will attach the encrypted file to the email. DO NOT INCLUDE THE PASSWORD IN THE EMAIL THAT CONTAINS THE ENCRYPTED FILE. Instead, you will send a separate email that contains the password OR you will call the recipient with the password. If emailing the password, it is recommended that you do not use the same subject heading as the original note that contains the note.



Second email contains the login credentials:

Note the subject heading is different. Also note that the file is not included in this email.

HOW TO SEND OUT MASS EMAILS

DO NOT send out mass e-mails to students unless you put the students' email addresses in the blind copy (BC:) box. Email is considered non-directory information at UCF. Therefore, email addresses must be concealed from view by other students and cannot be disclosed. The message in mass emails should not include any personally identifiable information. Use of Canvas for communicating with students in your class is recommended.

Please remember that **all personnel who handle and view student record information are responsible for FERPA compliance.** Any improper disclosure of FERPA-protected records is a violation of the federal law and must be reported to UCF's Information Security Office and the Registrar's Office. These violations can result in costly and time-consuming investigations and resolutions. Therefore, timely reporting is critical.

To review a list of frequently asked questions, please visit http://registrar.ucf.edu/ferpa#faq
Should you have questions about FERPA or the practices outlined here, contact the UCF Registrar's Office at 407-823-3013.