Instructions for encrypting and sending sensitive personally identifiable information via email

Sending sensitive personally identifiable information directly through email is against College policy. Any sensitive information must be placed in a password protected document if it must be shared via email.

Unfortunately Google Drive and GMail do not offer a native way to add encryption to files. Google does provide encryption during transit and at rest within its environment but any files or messages will not be encrypted if the recipient forwards the message to another system or downloads the file to their own storage location.

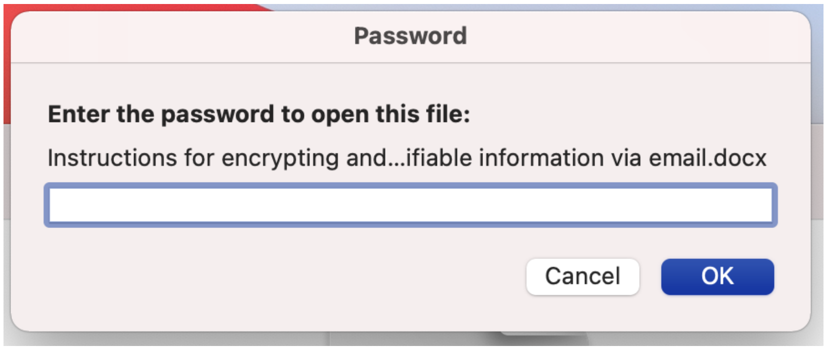
If you need to send sensitive or personally identifiable information and using our preferred method through Google Drive is not an option, **you must use the following instructions to secure the information when sending via email**.

1. Follow the Microsoft Support instructions for the type of office document you are using : https://support.microsoft.com/en-us/office/protect-a-document-with-a-password-05084cc3-300d-4c1a-8416-38d3e37d6826

2. When you set the password for opening/reading the file be sure to make the password something that is easy for you to remember and hard for others to guess because you will not be able to access the file if you forget the password.

3. Once you have saved the password protected file, create your message and attach the password protected file to the email and send to the recipient
4. Create a separate email with a different subject line and put the password you created in step 2 above in the body of the message and send it to the recipient.

The recipient will be prompted to enter the password you provided when they try to read the attachment.



Enter the password to open this file:

Instructions for encrypting and...ifiable information via email.docx

Note: You can use a similar process for password protecting Adobe PDF files. Here are Abobe's instructions: https://www.adobe.com/acrobat/how-to/pdf-file-password-permissions.html