be MINDFUL when using Google Docs

LEADERSHIP SUPPORT SERVICE

Anyone using a cloud-based solution, like Google Docs, to manage Personally Identifiable Information (PII) should be mindful in its utilization.

OWNERSHIP

It is the user's responsibility to safely utilize a cloud-based solution and maintain ownership of all data. This includes, but is not limited to:

- closely managing sharing permissions throughout a document's life cycle
- ensuring permissions are shared only with users within the same domain
- ensuring destruction after use
- ensuring utilization is in compliance with FERPA

DO NOT DUPLICATE

All activity should be done inside the working-document used in the cloud. Use extreme caution when downloading or copying this information.

MAINTAIN SECURITY

Accessing sensitive information through a cloud-based account requires a strong password on **professional** and **personal** devices at **ALL** times.

- any device accessing the account should be password protected and encrypted (including mobile devices)
- do not reuse a password attached to sensitive information with any other other account
- enable 2-factor authentication when possible

LOG OUT

Completely log out when using another computer. Never store your login credentials. Be sure to use private browsing and clear your browsing history.

SECURE NETWORK

Never access PII on an unsecure network or wifi connection. Turn VPN on whenever accessing sensitive information outside of the district network (even when you think your connection is safe).

Remember! The cloud provides space for you to store information on someone else's computer. There are always risks associated with any solution. It is the the responsibility of each person who handles PII to properly manage those risks. More often than not, it is how the tool is used that presents the greatest risk and not the tool itself.