COEIT Recommended Procedures for Collecting and/or Storing Data on Personal Devices

Introduction

The files, recordings, and data you collect as a University of Oregon student should be considered a valuable asset in your academic career. You should also be aware that some of the data you collect may have personally identifiable information (PII) or FERPA data relating to fellow students, to yourself, and to co-workers. Collecting, handling, and storing data is frequently part of course work, clinical work, teaching practica, volunteer opportunities or student employment at the UO. In many cases students, faculty and staff will collect and store data on their personally owned devices such as computers, tablets, phones, external hard drives or “thumb” drives.

Recommendations from the College of Education Information Technology Group (COEIT)

The College of Education strongly recommends that students take reasonable and feasible data security precautions when collecting, transmitting, and/or storing data collected as part course work, clinical work, teaching practica, volunteer opportunities or student employment at the UO.

1. Make sure that all your personal devices (phones, tablets, computers) require a sufficiently secure access code or passphrase to use them. Set a reasonable duration for an automatic screen lock (depending on the device, this can be from 5 minutes to 20 minutes)
2. Use standard encryption protocols such as HTTPS, SFTP or SCP when transmitting data between devices over a network.
3. Use “whole disk encryption” technologies such as FileVault (MacOS), BitLocker (Windows OS) or VeraCrypt (Multi-platform) in order to encrypt all local (non-removable) drives on your computer (Make sure to keep your encryption keys or passphrases in a safe and separate location)
4. When storing data on external storage devices, such as external hard drives or “thumb” drives, use similar encryption technologies (FileVault, BitLocker, VeraCrypt)
5. Make regular back-ups of your data and store them on an encrypted device or use an encrypted backup service (e.g., CrashPlan, BackBlaze). Keep back-ups in a safe place away from your work computer
6. If you are backing up or storing your data to Internet hosted or “Cloud” services (e.g., Microsoft OneDrive, Google Docs, etc.), try to use services that use similar encryption for transmitting and storing your data.
7. Review any user permissions relating to your data files and folders to make sure you are only sharing data with those who need to gain access to it

If you have any questions about securing your devices or what encryption technologies are available, please contact COEIT at coe-support@ithelp.uoregon.edu or in the HEDCO Learning Commons (110 HEDCO).

Updated: January 12, 2018