Guidance for Students Securing Information in the Cloud

Overview
There has been a major shift toward storing information over the Internet. Cloud services are not only becoming popular with big corporations, but also with individuals who like the convenience of having access to all their files from virtually any device. Popular ones include iCloud, Dropbox, Facebook and Google Cloud Storage.

Security Concerns

- **Ownership of data:** Many cloud services include fine print outlining their rights to the files stored on their servers. The term “dual ownership” is used to explain that the customer still OWNS their data, but the company may claim possession and rights to use that data for their own benefit.
- **Loss of control:** Customers have no control over how secure the servers are that store their data. There is a great deal of trust put into the cloud service provider’s ability to protect against hackers and data loss.

Recommendations

- **Set limits:** This is by far the best way to safeguard sensitive information. Limit what is saved in the cloud. Save those English papers and Math notes to Dropbox, but refrain from storing bank information, valuable research and those embarrassing photos in the cloud.
- **Backup Data:** Since consumers who use cloud storage have no control over what happens if the provider loses all their data, having files backed up to an external physical drive (i.e. a thumbdrive) is a great way to ensure nothing will be completely lost.
- **Encrypt Data:** Files can be encrypted with password protection. The IT@UC Office of Information Security gives a step-by-step explanation on how to do this: [encrypting office documents](https://kb.uc.edu/kbarticles/ucbox-landing.aspx).
- **Use Box@UC:** All UC students, faculty and staff automatically receive a Box@UC account with unlimited storage. Review the other services it provides, and the policy on their usage [https://kb.uc.edu/kbarticles/ucbox-landing.aspx](https://kb.uc.edu/kbarticles/ucbox-landing.aspx).
- **Research vendors:** If a cloud service is necessary, research the various options available. Look into ownership rights; how the providers backup their servers; and any security measures (if any) they take to safeguard the information stored.