UCLA Data Use Policy for Cloud Storage Services

Faculty and staff use[*] of cloud storage services offered by UCLA must comply with applicable University and campus policies, notably policies relating to the protection of University data and the UC Electronic Communications Policy. This includes observing the data use requirements in the table below, which are based on the UCLA Data Classification Standard and University-negotiated agreements established to help safeguard information about individuals and other confidential information for which the campus is a steward. Always employ due care when processing, storing, or communicating sensitive information. Violation of these data use requirements or other campus policies may result in disciplinary action up to and including termination.

Contact **IT Services Client Support at clientsupport@it.ucla.edu or (310-82)5-8000** to open a ticket to discuss the particulars of your situation if the data you have is listed in middle (yellow) column below, if you have data that does not appear in the table, or if you have any other questions about using these services.

Table 1. Data use requirements for UCLA cloud storage services

	Permitted	Open a ticket with Client Support	Prohibited
Box	• Any information already publicly available • Student records not related to health • Personnel records	• Data relating to human subjects or animal research • Export controlled data • Use of 3rd-party Box apps • Sensitive information not about individuals	• Logon credentials (account and password) • Credit card data • Individuals' health information[†] • Social Security numbers • Drivers license and CA identification numbers
Dropbox	• None		• All

---

[*] Including students in any employee role.
[†] A Business Associate Agreement (BAA) is required in order to permit storage of protected health information (PHI). A BAA for Box at UCLA is currently under review. Contact IT Services Client Support and open a ticket to request current status.