UCLA Allowable Data Use – Google Apps

Faculty and staff use of Google Apps must comply with applicable University policies, notably policies relating to the protection of University data and the UC Electronic Communications Policy. This includes the data use requirements in the table below, which are based on the 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, transmitting, or storing sensitive information. Violation of these data use requirements or other campus policies may result in disciplinary action up to and including termination.

Contact the **IT Support Center at help@it.ucla.edu or (310) 267-HELP (4357)** if the data you have is listed in the middle (yellow) column below, if you have data that does not appear in the table, or if you have any other data use questions.

Table 1. Data use requirements for UCLA Google Apps services

	Permitted	Contact the IT Support Center	Prohibited
Google Apps	• Any information already publicly available • Student records not related to health • Personnel records	• Data relating to human subjects or animal research • Sensitive information not about individuals • Storage of all other logon passwords (other than those listed in the "Prohibited" column)	• Storage of UCLA Logon, OASIS Logon, passwords • Credit card data • Social Security numbers • Drivers license and CA identification numbers • Individuals' health information • Export controlled data