New email, calendar and collaboration services have arrived at UC Davis!

The new services, intended for all faculty and staff in both administrative and academic units, are being closely reviewed by Dean's offices and department teams to select the best option, transition timeframe, and roll-out approach for their group. Departments and units have a choice between Office 365, Google (DavisMail), and the current uConnect Exchange service.

Privacy Compliance of Email and Collaboration Services at UC Davis.

The 2 new options are cloud based and therefore the data is vendor hosted. The compliance of these services with various privacy considerations is indicated in the below table. For further explanation of these privacy considerations, see the Notes section on page 2.

	Google Apps for Education (DavisMail)	Microsoft Office 365 (uConnect Cloud)	Microsoft Exchange (uConnect Local)
US Located Data	Not Guaranteed	Yes	Yes
Data Mining	Yes[1,2]	No[2]	No
Advertisements	No[3]	No	No
HIPAA	No	Yes	No
FISMA	No[4]	Yes	No
Notification Triggering Data (CA Civ. Code §1798.29)	No	Yes	No
FERPA[5]			
• FERPA **Directory Information**	Yes[6]	Yes	Yes
• FERPA **Personally Identifiable Information (PII)**	No	No if A2[6] Yes if A3[7]	No
• **Student Education Record** (excluding data elements that meet the criteria of FERPA PII)	No	No if A2[6] Yes if A3	Yes
ITAR	No	No	No

[1] Google has admitted to [data mining student emails in their free education apps](.).
[2] UC Davis cannot guarantee that any cloud provider will not mine data.
[3] Information on Google's use of mined data can be found [here](.).
[4] Google Premier is FISMA certified, not the free Google Apps for Education.
[5] Data for students who have exercised their right to opt out of data disclosure should be treated accordingly. Department business processes should consider a student's opt out status before placing data in a cloud service.
[6] UC Davis users receive the Office 365 A2 license by default. An upgraded Office 365 A3 license will be available to campus Fall 2014.
[7] Including PII in emails is not advisable. Info can be found at: [UC Davis Cyber-Safety Program: Personal Information](.)

Resources

- [UC Davis Cloud Service Storage and Use Guidelines](.)
- [ECS Project Web Site](.)

- [Microsoft Office 365 Trust Center](.)
- [Google's Privacy Policy](.)
- [Google's Term of Service](.)

PROJECT MANAGER: Mark Thonen, mthonen@ucdavis.edu

Our thanks to the campus advisory committees (Campus Council for Information Technology, Technology Infrastructure Forum, Deans' Technology Council), as well as the Academic Senate Committee on Information Technology, and the project's advisory committees who advised the team throughout this initiative.

Notes

- **Data Mining** – the ability of the vendor to capture information from user accounts.
- **Advertisements** –vendor shows targeted and/or untargeted advertisements in the user's UC Davis account.
- **FERPA Compliance** – FERPA defines "Education Record" to include those records that are:
  - Directly related to a student; and
  - Maintained by the University or by a party acting for the University.
    - This definition is not limited to academic records. It also includes housing records, disciplinary records, financial aid records, and all other records directly related to a student (unless expressly carved out as an exception, discussed below).
    - The term "maintained" is not defined, but should be interpreted broadly to include all records in the possession, custody, or control of any employee or agent of the University.
  - **FERPA Directory Information** – means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.
  - **FERPA Personally Identifiable Information (PII)** – Data elements within the student education record that should be protected from improper disclosure includes, but is not limited to:
    - The student's name;
    - The name of the student's parent or other family members;
    - The address of the student or student's family;
    - A personal identifier, such as the student's social security number, student number, or biometric record;
    - Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
    - Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
    - Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates (known as a Targeted Request).
  - **Student Education Record** - The term means those records that are (1) directly related to a student; and (2) maintained by an educational agency, institution, or a party acting for the agency or institution. This includes outcome data such as GPA, LSAT score, etc.
- **Notification Triggering Data Under CA Law** (CA Civil Code § 1798.29) – California law requires notification to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a security breach. Notification triggering information is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  - Social Security Number
  - Driver's license number or California Identification Card number
  - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
  - Medical information
  - Health Insurance Information
- **FISMA Compliance** – vendor has acquired a federal agency FISMA certification.
- **HIPAA Compliance** – vendor has signed a HIPAA Business Associate Agreement with UCOP.
- **ITAR Compliance** - service has been granted ITAR authority to operate (ATO) from a federal agency and the ATO applies to the UC Davis service.