A. Welcome and Introductions  
Jim Davis (5 minutes)

B. New Operational Framework for the Board  
Jim Davis, Kent Wada (15 minutes)  
   1. CPO announcement  
   2. Transition proposals for AY2012-13  
   3. Overview of meeting agendas for AY2012-13

C. Revisiting the UCLA Statement on Privacy and Data Protection  
Kent Wada (40 minutes)  
   1. Status of UC privacy and information security initiative  
   2. UCLA and UC value statements and principles

D. Opus Faculty Information System (continued)  
Carole Goldberg, Vice Chancellor, Academic Personnel (60 minutes)  
Fred Zimmerman, Chair, Opus Committee and Professor and Chair, Health Services, School of Public Health  
Meg Buzzi, Opus Project Director  
   1. Update and discussion of Opus issues related to privacy.

Marti Arvin, Chief Compliance Officer, UCLA Health System and the David Geffen School of Medicine  
Stuart Biegel, Education Faculty & Law Faculty  
Amy Blum, Senior Campus Counsel  
Ross Bollens, Chief Information Security Officer, Information Technology Services  
Christine Borgman, Professor and Presidential Chair, Information Studies  
Alfonso Cardenas, Professor, Computer Science  
Dana Cuff, Professor and Vice Chair, Architecture and Urban Planning  
Michael Curry, Professor, Geography  
Jim Davis, Vice Provost, Information Technology and Chief Academic Technology Officer (chair)  
Sharon Friend, Director, Office of Human Research Protection Program  
Maryann Jacobi Gray, Assistant Provost, Office of the Executive Vice Chancellor and Provost  
Lubbe Levin, Associate Vice Chancellor, Campus Human Resources  
Leah Lievrouw, Professor, Information Studies  
Rafail Ostrovsky, Professor, Computer Science  
Edwin Pierce, Director, Audit & Advisory Services  
Dinesh Shadrach, Graduate Student Representative, Anderson School  
Gary Strong, University Librarian  
Burton Swanson, Professor, Anderson School  
Frank Wada, University Registrar  
Kent Wada, Director, Strategic IT Policy and Chief Privacy Officer, Office of Information Technology  
TBD – Undergraduate Student Representative
UCLA Board on Privacy and Data Protection | Proposed Agenda AY 2012-2013

For each meeting (typically):
(a) present a landscape topic and
(b) invite a few privacy-related guests

**Fall 2012: 1st Meeting**
CPO Announcement
Transition Proposals for AY 2012-13
Overview of Meeting Agendas for AY 2012-13 (20)
Status of UC Privacy and Information Security Initiative
UCLA and UC Value Statements and Principles (40)
Opus Faculty Information System (60)

**Fall 2012: 2nd Meeting**
Adoption of Values and Principles
Opus Update
Landscape: Photo/Film Project (Anne Pautler)
Public Records Act Draft Statement (Amy Blum)
Action: How Do You Educate/Create Awareness?
Guests

**Winter 2013: 1st Meeting**
PISI Update
Landscape: Online Polling Tools OPT (Rose Rocchio)
Front Door Software Guidelines
Guests

**Winter 2013: 2nd Meeting**
Landscape: BYOD
Guests

**Spring 2013: 1st Meeting**
Privacy Day: Guest Speaker(s), Workshops, etc.
Guests

**Spring 2013: 2nd Meeting**
Landscape: TBD
Guests

**Possible Landscape Topics**
- California Public Records Act Requests: UCLA Stance and Community Awareness
- Privacy in Photo and Film Used for Promotion
- BYOD: Policies and Practice
- How Much Data Is Out There About Us?
- Online Polling Tools OPT (Mobile Polling Tool)
October 9, 2012

Deans, Directors, Department Chairs and Administrative Officers:

I am pleased to announce the designation of Kent Wada in the newly formed role of Chief Privacy Officer (CPO) for UCLA. In an age of proliferating information and interaction both digitally and in person, addressing privacy in its different forms has become important to the mission of the University. Privacy is critical to our values of academic and intellectual freedom and to the well being of our culture and community, even as the University’s compliance obligations with privacy legislation and commitment to transparency in the administration of a public institution escalate.

In connection with this responsibility, Kent’s current role is formally extended to Director of Strategic IT Policy and CPO. The CPO is the point of contact on matters concerning the privacy of individuals and of their information, and will be working closely with the many campus offices that have compliance or operational responsibilities for privacy; and with the Chief Compliance Officer of the UCLA Health System and the David Geffen School of Medicine. The UCLA Board on Privacy and Data Protection, whose chair is jointly appointed by the Academic Senate and the Executive Vice Chancellor and Provost, will provide oversight to the CPO role in guiding and balancing the University’s values with its legal, policy, administrative, security and privacy responsibilities.

As the Director of Strategic IT Policy and CPO, Kent will continue to help craft the campus-wide agenda for technology and privacy policy issues of strategic importance to the institution, and collaborate broadly across the campus and with its IT governance groups, across the UC system and nationally. Kent was involved with founding the UCLA Board on Privacy and Data Protection in 2005, and currently chairs the working group of the UC Privacy and Information Security Initiative charged by UC President Yudof to recommend a framework for considering privacy and information security issues within the University.

Please join me in welcoming Kent into this new role. We look forward to having an experienced, thoughtful leader advocating and addressing the pressing privacy and data protection issues facing our institution.

Sincerely,

Jim Davis
Vice Provost, Information Technology
UCLA Board on Privacy and Data Protection

OPERATIONAL FRAMEWORK

A. Authority
Executive Vice Chancellor and Provost; faculty Chair appointed jointly by Provost and Academic Senate; Academic Senate Chair-elect member; oversight and support through the Office of Information Technology

B. Membership
Because privacy is essential to academic freedom and to the conduct of teaching and research, the Academic Senate must play a vital role in the governance of privacy and data protection for the academy. The Board is therefore organized in structure and process to reflect the faculty voice.

The Board maintains a balanced number of faculty and administration, plus one graduate and one undergraduate student representative. Faculty appointments should ensure social, cultural, technical and management aspects of privacy and data protection. Administrative appointments should have direct involvement with institutional management of privacy matters.

Members are recommended by the Board’s Executive Committee, in consultation with the full Board, and require a majority vote to be confirmed. The Executive Committee is responsible for managing the recommendation process.

Voting Membership
Faculty
Faculty members equal to the number of administrative voting members† (staggered three-year terms). The Chair-Elect of the Academic Senate shall be included and counted as one of these members.

Students
1. One undergraduate student designated by the Undergraduate Students Association Council (one year term)
2. One graduate student designated by the Graduate Students Association (one year term)

Administration
1. University Librarian
2. Vice Provost, Information Technology
3. Designee from the Office of the Campus Counsel
4. Chief Compliance Officer of the UCLA Health System and the David Geffen School of Medicine
5. University Registrar
6. Director, Office of the Human Research Protection Program
7. Designee from Campus Human Resources

† Must be adjusted as the administrative membership changes in number.
Non-Voting Membership
1. UCLA Chief Privacy Officer
2. UCLA Chief Information Security Officer
3. Designee of the Executive Vice Chancellor and Provost
4. Designee from Audit & Advisory Services

C. Executive Structure

Faculty Chair (two-year term)
The Chair must be a voting faculty Board member, ladder faculty and appointed by both the Executive Vice Chancellor and Provost and the Academic Senate.

Administration Vice Chair (two-year term)
The Vice Chair must be a voting administrative Board member.

Executive Committee
The Executive Committee comprises the Chair, Vice Chair and UCLA Chief Privacy Officer. It acts on behalf of the Board to ensure responsiveness with regard to operations and agendas.

D. Representation to Oversight Committee
The Chair and/or the Vice Provost-IT represent the Board on interactions with the Oversight Committee on Audit, IT Governance, Compliance and Accountability as appropriate to the privacy topic.

E. Meetings
Meetings are generally held at least once per academic quarter.

Meetings are open to UCLA visitors with prior notice unless called otherwise by the Chair. Non-UCLA visitors attend at the discretion of the Chair. All visitors will be introduced.

Closed sessions
In consultation with legal counsel, the Board may go into closed session for certain agenda items at the direction of the Chair, with only voting members present. The attendance of non-voting or other individuals during such sessions is at the direction of the Chair. Student members may be excluded from closed sessions where deemed appropriate by the Chair.

F. Web site
The Board will maintain a web site for publishing meeting materials, meeting summaries and any relevant documentation used by the Board. Materials will be assumed open to the campus and public unless declared confidential, privileged or otherwise limited by the Chair or legal counsel.

G. Support
Support to the Board is provided by the Office of the UCLA Chief Privacy Officer and the Office of Information Technology.
UCLA Board on Privacy and Data Protection
Transition Proposals for AY 2012-2013

Note: The Board’s new operational framework is currently in review by the UCLA Academic Senate. This proposal provides transition options toward full implementation of the structure by start of AY 2013-2014 (pending review from the Academic Senate).

EXECUTIVE COMMITTEE
The Executive Committee comprises the Chair, Vice Chair and UCLA Chief Privacy Officer. It acts on behalf of the Board to ensure responsiveness with regard to operations and agendas.

FACULTY CHAIR FOR AY 2012-13
The Chair must be a voting faculty Board member, ladder faculty and appointed by both the Executive Vice Chancellor and Provost and the Academic Senate.

Proposal: Jim Davis continues to serve as Chair during this transition year. Meanwhile, the Board should identify options to suggest to the Executive Vice Chancellor and Provost and the Academic Senate for consideration of the two-year Chair appointment for AY 2013-2015.

ADMINISTRATION VICE CHAIR
The Vice Chair must be a voting administrative Board member.

Proposal: Board to define selection process.

FACULTY MEMBERS
Faculty members will be selected to ensure social, cultural, technical and management aspects of privacy and data protection. The new framework calls for staggered three-year terms for faculty, which allows for continuity, institutional memory and development of expertise on the Board. Members are recommended by the Board’s Executive Committee, in consultation with the full Board, and require a majority vote to be confirmed. The Executive Committee is responsible for managing the recommendation process.

PROPOSAL FOR FACULTY ROTATION
The Board is comprised of faculty members equal to the number of administrative voting members. The Chair Elect of the Academic Senate shall be one of the faculty members.

Proposal: Begin rotation with two members in September 2013, three members rotating out in September 2014, and three members rotating out in September 2015. The Board should consider teaching, research and sabbatical schedules in an effort to best accommodate everyone’s plans. Board members to identify potential new members.

ADMINISTRATIVE MEMBERS
Administrative members should have direct involvement with institutional management of privacy matters. In restructuring the Board, several administrative offices have been identified for voting and non-voting positions.

Proposal: The board has filled its administrative positions.

STUDENT MEMBERS
Each year the Undergraduate Students Association Council (USAC) and the Graduate Students Association (GSA) will be asked to designate one undergraduate and one graduate student for a one-year term respectively.

Proposal: We have requested the assistance of both USAC and GSA to fill these positions for AY 2012-13. Dinesh Shadrach has expressed interest in continuing as the graduate student representative for AY 2012-13. He is currently working with the GSA and the Office of Information Technology to process his appointment. The undergraduate position remains open and will be filled as soon as an interested student has been named by USAC.
# UCLA BOARD ON PRIVACY AND DATA PROTECTION | TRANSITION DOCUMENT AY 2012-13
(Under Senate Discussion)

## EXECUTIVE COMMITTEE

1. **CHAIR | JIM DAVIS**, Interim AY 2012-13  
   Faculty 2-Yr Term, Dual Appointment Academic Senate & EVC/Provost

2. **VICE-CHAIR | TBD**  
   Admin 2-Yr Term, Voting Administrative Member

3. **CHIEF PRIVACY OFFICER | KENT WADA**

### FACULTY MEMBERSHIP (VOTING)

1. Chair Elect of the Academic Senate
2. Current Faculty Members, Rotation TBD
3. rotation TBD
4.  
5.  
6.  
7.  

### ADMINISTRATIVE MEMBERSHIP (VOTING)

1. University Librarian | Gary Strong
2. VP Info Technology | Jim Davis
3. Designee Campus Counsel | Amy Blum
4. CCO, Med Center | Marti Arvin
5. University Registrar | Frank Wada
6. Director, HRPP | Sharon Friend
7. Designee, Campus HR | Lubbe Levin

### STUDENT MEMBERSHIP (VOTING)

1. Dinesh Shadrach | Grad Student
2. Undergraduate Student

### NON-VOTING MEMBERSHIP

1. CPO | Kent Wada
2. CISO | Ross Bollens
3. Designee, EVC & Provost | Maryann Gray
People

Contact the Board:

Kent Wada
email: kent@ucla.edu
phone: x63874

Chair:
Jim Davis
Vice Provost, Information Technology

Current Members:
Marti Arvin *
Chief Compliance Officer, UCLA Health Sciences
Stuart Biegel
Education Faculty & Law Faculty
Amy Blum *
Senior Campus Counsel
Christine Borgman
Professor, Information Studies
Alfonso Cardenas
Professor, Computer Science
Dana Cuff
Professor & Vice Chair, Architecture and Urban Planning
Michael Curry
Professor, Geography
Sharon Friend *
Director, Office of Human Research Protection Program
Maryann Gray *
Assistant Provost
David Harmon*
Director, Financial Management Programs
Leah Lievrouw
Professor, Information Studies
Rafail Ostrovsky
Professor, Computer Science
Gary Strong *
University Librarian
Burton Swanson
Professor, Anderson School
TBD
Faculty
Kent Wada *
Director, Strategic IT & Privacy Policy
* Ex-Officio

Student Representative:
TBD
Undergraduate Student Representative
Dinesh Shadrach
Graduate Student Representative

Resources:
Ross Bollens
Director, IT Security
Claudia Luther
Senior Media Relations Representative, University Communications
Prelude
The Advisory Board on Privacy and Data Protection is an advisory board to the Executive Vice Chancellor and Provost. It is charged with articulating an institutional position reflecting the campus’s values and cultural expectations to address the challenging issues of balancing privacy and data protection faced by the campus community.

This Statement articulates principles and provides guidance for attaining the principles when complying with University and campus policy on privacy and data protection. However, the Statement is not policy itself and does not confer nor abrogate any rights or privileges.

Table of Contents
Statement .................................................................................................................... 2
Principles of Fair Information Practices ................................................................ 3
Appendix A. Guidance for Attainment ................................................................. 5
Privacy of Electronic Communications .................................................................. 5
Protection of Confidential Information ................................................................. 6
Legally Required Disclosures ............................................................................... 7
Considerations for Individuals .............................................................................. 8
Appendix B. Scenarios ......................................................................................... 9

---

1 The Board would like to express its appreciation to Chris Jay Hoofnagle, now with the Berkeley Center for Law & Technology, for his work in framing this statement.
2 This Statement does not speak to whistleblower policies or issues.
Statement

Academic and intellectual freedom are values of the academy that help further the mission of the University. These freedoms are most vibrant where individuals have autonomy: where their inquiry is free because it is given adequate space for experimentation and their ability to speak and participate in discourse within the academy is possible without intimidation. Privacy is a condition that makes these values possible and is strongly supported by UCLA.

UCLA recognizes that there is a constellation of values and of legal, policy, and administrative obligations that are always in play. Privacy is an important condition threaded throughout this constellation:

- ensuring an appropriate level of privacy through its policies and practices, even as interpretations of privacy change over time;
- nurturing an environment of openness and creativity for teaching and research;
- honoring its obligation as a public institution to remain transparent, accountable and operationally effective; and
- safeguarding confidential information and assets for which it is a steward.

The Advisory Board on Privacy and Data Protection is the campus nexus for the ongoing discussion about appropriate balance in the context of an ever-evolving societal, legal and technological climate.

---

Principles of Fair Information Practices

The following principles, drawn from the Organisation for Economic Co-operation and Development\(^4\), help uphold privacy rights. They seek to balance the rights and responsibilities of data collectors and individuals by establishing a code of fair information practices. UCLA strives to align with these principles in its policies and implement these practices in its information systems\(^5\).

1. **Transparency.** Transparency promotes accountability, informs individuals of their rights and responsibilities and allows individuals to make more enlightened decisions when disclosing or using data. In furtherance of its educational role, the campus should inform individuals of the personal information collected and how that information is used to perform official functions. Where possible, and without creating undue bureaucracy, the campus should strive to disclose the following aspects of personal information systems:
   - Information sought
     - What information is being collected.
     - For what purpose it is being collected and the resulting benefit.
     - Whether the collection is mandatory or voluntary.
     - How long the information is kept.
     - In what form it is kept, including documentation.
     - The purpose(s) for which the information can be used.
   - Stewardship
     - Who is the steward of the data and has responsibility for addressing questions or complaints concerning the system or its content.
     - Who has access to the information and by what means.\(^6\)
     - What security safeguards are in place to protect the information.\(^7\)

2. **Privacy-Friendly Design.** The campus should encourage the development of information systems that deliver services or perform functions without the collection of personal information. Where possible, the campus should allow individuals to decide whether to enroll in systems that collect personal information. Information systems should be designed consciously to avoid creating opportunities for information to be reused for purposes incompatible with the purpose of its collection, to avoid creating new surveillance opportunities, and to avoid the persistent maintenance of personal information.

3. **Accountability and Fairness.** There must be processes in place to ensure fairness where important decisions are made based on personal data. There should be a

---

\(^4\) http://oecd.org/

\(^5\) Examples of information systems include Registrar, BruinCard, library records and personnel records.

\(^6\) Only in general terms, without reference to specifics that could help an ill-intentioned individual inappropriately gain access to information.

\(^7\) Again, only in general terms, without reference to specifics that could help an ill-intentioned individual inappropriately gain access to information.
mechanism for recourse for individuals who desire to challenge a determination based on personal information.

4. *Sustainability and Operational Necessity.* The campus performs myriad functions in addition to education and research, including providing housing, health care, communications and transportation. Many of these functions require the collection of personal information. These principles should be applied in a reasonable manner so as to promote operational effectiveness (including appropriate security safeguards) while striving to design systems that are sensitive to privacy risks.
Appendix A. Guidance for Attainment

The following sections give guidance for attaining the principles and for achieving an appropriate balance between privacy and compliance with applicable policies.

Privacy of Electronic Communications

This section is primarily applicable to the administration of networks, email servers and systems.

The University of California is governed by its Electronic Communications Policy (ECP) with respect to privacy of electronic communications. It articulates a bright-line threshold for protecting individual privacy: “The University does not examine or disclose electronic communications records without the holder’s consent.”

A high bar is set for overriding this protection (“non-consensual access procedure”), which can occur only in specified circumstances and which requires a multi-level review, including high-level review through the approval of the appropriate administrator at the minimum level of Vice Chancellor.

Security, privacy, and other values and obligations must be appropriately balanced as articulated in the Statement. The following guidance can be applied to help resolve conflicts between values and/or varying interests.

1. Employ standard technical practices to ensure the security, reliability and integrity of electronic information systems, services and data. These practices include the routine monitoring of the network by automated means.

2. Do not allow security practices to be used for surveillance, or the monitoring of individual behavior. If surveillance is required, appropriate guidance shall be sought and either the provisions for non-consensual access in the ECP followed or other legal requirements satisfied.

3. Do not “lock down” access so tightly that security becomes a barrier to collaboration or productivity. The appropriate balance between security risk and functionality must be considered.

4. Consistent with the ECP, do not intentionally search electronic communications for violations of law or policy. Do act to assure that

---

10 UC ECP, Section IV.B Access Without Consent: “(i) when required by and consistent with law; (ii) when there is substantiated reason; (iii) when there are compelling circumstances; or (iv) under time-dependent, critical operational circumstances.” http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20PRIVACY
12 However, also refer to the text on audit trails and other means for effecting due diligence in complying with legal or regulatory requirements in the section Protection of Confidential Information.
suspected, inadvertently discovered and reported violations are promptly and properly handled. If non-consensual access is required to do so, the ECP’s procedure for such access must be followed.11

5. Avoid making judgments based on value of content (e.g., whether access to certain web sites is appropriate), as most a priori prohibitions on access to content are considered censorship.

6. Consult with the appropriate campus official(s) when conflicts arise between privacy and other policies or legal obligations (e.g., sexual harassment policies or human subjects protection).

7. Situations requiring emergency access should follow the specific procedure defined in the ECP for this purpose.13

Protection of Confidential Information

This section is primarily applicable to data stewards and to those administering or developing databases or other information systems and networks.

The University is the steward for the confidential information it requires to fulfill its missions and operations. To safeguard such information, the University employs practices that ensure confidentiality, foster clear accountability, increase the effectiveness of data administration and minimize legal exposure and liability.14,15

In order to effect due diligence in complying with legal requirements and to be good stewards of the public trust, appropriate controls must be implemented in systems and services containing confidential information. For research and clinical trials involving human subjects, approval by the Institutional Review Board16 is Federally mandated. More generally, controls can take many forms, including administrative (e.g., background checks), physical (e.g., access to devices) or technical.

Technical controls include:

- Use of encryption technology17 as generally required for Personal Information18.
- Limiting access to specific data, systems or network content to only those who legitimately require access.

---

13 UC ECP, Section IV.B.2. Emergency Circumstances.  
http://ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20PRIVACY

http://www.ucop.edu/ucophome/policies/bfb/is3.pdf

15 UCLA Policy 404, Protection of Electronically Stored Personal Information.  
http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=404

16 http://oprs.ucla.edu/human/about-IRBs

17 UCLA Policy 404, Protection of Electronically Stored Personal Information, Section IV.A Campuswide Standards for Electronically Storing Personal Information.  
http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=404

18 Defined by UCLA Policy 404 as an individual’s first name or first initial, and last name, in combination with any one or more of the following: (1) Social Security number, (2) driver’s license number or California identification card number, (3) 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, (4) medical information, and (5) health insurance information.
• The maintenance of an audit trail logging access to specific data, systems or network content (e.g., a clinical patient system) in order to permit the identification of potential wrongdoers.19

• Limiting access to network content or services not required for the intended purpose of the network, system or unit to minimize risk (e.g., prohibiting peer-to-peer protocols on a payroll network where there is no business or academic need for such tools — at present).

Use of controls such as audit trails and the limitation on access to specific network content or services can be necessary to effect due diligence in complying with legal or regulatory requirements.20 Unless stipulated by law, however, such controls should be carefully considered so as to avoid violating the UC Electronic Communications Policy. Regardless, the ECP does require a minimization approach: only as much intrusive security as is appropriate in any given circumstance should be used and no more.21

Use of these technical controls does not abrogate other provisions of the ECP. For example, logging access to a specific system containing personally identifiable information does not mean a supervisor can look at an employee’s email without his or her consent; or absent consent, going through the Policy’s non-consensual access procedure.11

Legally Required Disclosures
The University is often required to disclose information it may not routinely make public: for example, when in receipt of a subpoena, during litigation or when a California Public Records Act (PRA) request is made. UCLA has existing policies and procedures that speak to these circumstances.22,23,24 There are also requests made under the aegis of national security, which should always be referred to Campus or University Counsel.

It is important to be mindful that much information held or created by the University is subject to disclosure under the PRA to help ensure transparency and accountability for public institutions. For example, current salaries (as employees of a public institution) and routine email communications generally fall under this provision, though most personally identifiable information does not.

---

21 UC ECP, Section V.B, Security Practices: “Network traffic may be inspected to confirm malicious or unauthorized activity that may harm the campus network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation.” http://www.ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#B%20SECURITY
Specific computer security sensitive information – information that could directly assist malicious individuals in attacking UCLA applications, systems and networks – is not subject to an express statutory exemption, but is protected under a balance of interest rule. Thus when information relating directly to the security of systems is communicated, it should be identified as such with the label “Confidential: Computer Security Sensitive Information”. This flags material for careful examination by campus attorneys when a PRA covers such information. It also makes it clear to anyone else seeing such information that extra care expected. Only the truly sensitive information should be so labeled.

Considerations for Individuals

An important rule of thumb is to avoid putting in an email anything you would prefer not end up as a headline in the newspaper. While incidental personal use of electronic resources is permitted, any individual concerned about individual privacy unrelated to University activities should use a separate commercial account for non-University related electronic records and communications.

Conversely, the convenience of free or low-cost external email accounts or other “cloud” services that store data outside of University control (and for which there is no institutional contract or agreement with the University) should be carefully weighed against the increased security, privacy and business risk in using such services. Each individual must take responsibility when making decisions about when it is and is not acceptable to use these free/low cost services.

All legal and University policy requirements apply to all University records, whether on UC or non-UC systems.

Under no circumstances should confidential or restricted data be used with services for which UC has not negotiated an agreement through the regular campus or University process.

---

25 UC ECP, Section III.D.8, Personal Use.
http://ucop.edu/ucophome/policies/ec/html/pp081805ecp.html#D%20ALLOW

26 Guidance on making informed decisions in this area is being developed. In the interim, such guidance from the University of California, Santa Cruz, provides excellent information on the use of free cloud services: http://its.ucsc.edu/security/policies/free.php.

27 UC BFB IS-2 Inventory, Classification, and Release of University Electronic Information, Appendix A, Definitions.
http://ucop.edu/ucophome/policies/bfb/is2.pdf
Appendix B. Scenarios