

Notes from the AGCA Confidentiality & Student Records Panel Discussion

10:00am to 12:00pm Friday, November 15, 2013, Dodd 161

Panel comprised of:

Brenda Moore – UCLA Registrar's Office
Susan Smith – UCLA Graduate Division
Valery Holtom – UCLA Office of the Dean of Students

Panel moderated by AGCA (Barrett Korerat - School of Theater, Film, & Television)

Notes by Alexis Sexauer, Lisa Lee, & Barrett Korerat

Notes are organized by topics of discussion and keywords highlighted in bold text

ADMISSIONS & FUNDING

Issues covered in this section:

1. Resources for confidential review of admissions materials
 2. Web access and review
 3. Confidentiality agreements and auditing of information
 4. Financial information for admissions
 5. Student requests for their admissions information (letters of rec, etc.)
- Who can view application information? (example given that some faculty reviewers had access to applications outside their department).
 - If faculty are on several admissions committee, the faculty member should focus on one group and not mingle the different groups.
 - Issues with faculty being able to see applications outside of their departments online has been fixed (Graduate Division).
 - Make sure to keep reviewer **portal passwords** confidential. In these cases, confidentiality agreements are not needed otherwise because when someone is given a secure login to an area with confidential materials - the confidentiality agreement is implicit with the login privileges.
 - If a student is on the review committee they should sign a confidentiality agreement (UCOP Policy 130).
 - Grad Division will not give access to **work study students**. If you want them to assist with admissions they should sign a confidentiality agreement.
 - Is there official policy on **faculty access to admissions records** and privacy of student records as it relates to downloads/pdf of applications by faculty, something we can cite when discussing with our admissions committees?
 - At the upcoming Graduate Division Admissions Chairs meeting (11/21/13), there will be information of all confidentiality policies.
 - IT security speaks to the group regarding safety of application data

- Faculty should not download and save applications to their computers, do not print them either. They should only access applications by logging into the review portal.
 - Because the application process is electronic, there are concerns. These documents should be treated as documents and should not be downloaded onto personal computers. As long as the professor is logging in and viewing the data and not saving it, there should be fewer issues.
 - It would be best to have an **intranet or Moodle** so the information is there and does not go beyond the site. Contact your MSO and system administrator to establish an intranet.
 - Faculty that are downloading and saving files onto devices should **clear the cache**. Please remind faculty.
- Are **confidentiality agreements** required for anyone that has access for admissions files or just the admissions committee members?
 - UCOP (PACAOS) **Policy 130** (on Go.Grad or on IT services) is the policy that addresses confidentiality.
 - It would be a good idea if all admissions committee members sign a confidentiality agreement and are informed of policy, but in general, confidentiality agreements should be signed by anyone with access to these records.
 - Student employees and work study employees should be informed and given the confidentiality information.
 - Confidentiality agreements should be signed by admissions committee or anyone with access. Student employees and work study should be informed and given the confidentiality information.
 - For online review, make sure to keep reviewer portal passwords confidential. In these cases, confidentiality agreements are not needed otherwise because when someone is given a secure login to an area with confidential materials - **the confidentiality agreement is implicit with the login privileges**.
- According to the *Guidelines for the Graduate Admissions Process and Codification of the Policies and Procedures Governing Graduate Admissions (aka “Codification”)*, it states that records should be retained (for a minimum of three years) for periodic **audits**. Who conducts these audits?
 - *Codification* states that records should be kept confidential. There can be an audit. Policy goes back a long way and there has not been any audits recently. The Office of Civil Rights has audited before or Graduate Division can audit.
 - While audits are not a regular occurrence they can happen (much like with the IRS) and they are looking at consistency, integrity & retention of files.
- International Students and their **financial information**, should it be kept with admissions records or filed separately from the student’s academic record? Should these be destroyed

before being sent to remote storage (Iron Mountain)? Sometimes chairs, vice chairs, deans (professional schools) will request a review of a student's file, should this financial information be redacted/removed before their review?

- International students must have this additional documentation, but Graduate Division no longer requires financial information from international students. That information is given directly to the **Dashew Center** (who maintains those records) and is *only required for visa issues*.
 - Departments should not be receiving the financial information from students. Redacting that information would be a good idea.
- Students often request copies of **letters of recommendation** from their admissions files to be used in funding applications. What is the protocol for this (in regards to the waiver forms)? Should the recommender be consulted first? Should copies be sealed in envelopes?
 - If applicants sign the **waiver of access**, they waive the access to the letters once they become students. Students that did not waive access may view them.
 - When students ask for letters of recommendations, it would not be a bad idea to consult first with the recommender.
 - This can be an issue because not all recommendation letters are favorable.
- If they applied previously but were not accepted to a program, sometimes applicants ask to forward letters from the previous application. What kind of information can be given in this regard about the letters and if an applicant asks why they were not accepted to a program?
 - Don't divulge information from unfavorable letters, but suggest that the application would be stronger if they refreshed their letters or obtained them from people they had good working relationships with.
 - When applicants ask why he/she was not admitted, departments should be as general as possible. Response should be framed- "here's what you can do to bolster your application in the future," or "This year's pool was very competitive."

FERPA, DISCLOSURE, and ACCESS TO STUDENT INFORMATION

Issues covered in this section:

1. FERPA & Directory restrictions
 2. Outside requests for information
 3. Requests from police or other authorities
 4. Faculty/Staff Requests for information
 5. Contacting students
 6. Sharing student information (websites, grades)
- Post graduation, a former student asks for a **degree confirmation letter**. Do we refer them to the Registrar, who then refers them to the clearing house?
 - If a student needs a letter confirming their degree after they have graduated, send them to the Registrar's Office.
 - The Registrar (or you) can refer people to the clearing house .

- The degree confirmation letter goes to the student. The Registrar's office does not send letters to different institutions.
- A student has a **directory restriction** on their account. What is the best practice when someone calls to ask about them? What is the best place to determine what type of directory restriction the student has placed on their record?
 - All students and their information are federally protected under **FERPA (Family Educational Rights and Privacy Act)**. FERPA was designed to keep information as close to us as we can.
 - If someone calls for student information, look up UID on **OASIS (SAD)** or **SRWeb** to see if there is a directory restriction. UID in red will show the restrictions.
 - If a FERPA restriction exists, we must say, *"we have no information on the person you are inquiring about."* (say "person", don't say "student", as it implies that the person in question is in fact a registered, confirming information you did not intend to).
 - If there is a directory restriction, we can say, *"we cannot give out information on that person,"* or, *"records on that person are closed."*
- Sometimes **landlords or rental offices** will call to verify a student's status. If the student hasn't notified me in advance, what is the protocol for answering these questions?
 - You can refer them to the Registrar or directly to the **national student clearing house** (www.studentclearinghouse.org). It is an online procedure that will cost about \$25.
 - If the student is employed by your department and **proof of employment** is required, direct **the student** to www.atyourservice.ucop.edu where they can print their proof of employment. They can also obtain this from the Payroll Office.
- If an undercover **police officer** attended a course to ask the instructor about a possible student, what kind of information could the instructor provide, or is there a protocol to follow?
 - If a student has any directory/FERPA restrictions, staff cannot give any information. Any other information requests should be directed to the **Office of the Dean of Students** or UCPD.
 - If someone requests information beyond the public information, refer them to the Dean of Students (i.e. a federal person doing a background check).
 - If a police officer is looking for a student send them to UCPD (or direct them to the Registrar who will do the same).
 - **We as counselors do not talk to outside agencies.**
 - Staff and faculty should not talk to outside agents about the student (try to inform faculty about these policies).
 - UCPD is part of campus health & safety and can deal with these issues properly. If law enforcement comes and asks where a student is in an urgent emergency, 99% of the

time it is a UCPD officer asking. Confirm if it's a UCPD officer, if yes, then information can be shared.

- If **federal investigators** doing background checks would like information, staff can only give public information (dates of attendance, dates of degree, major, etc.) – refer then to the Office of the Dean of Students.
- Definitions of “public information” can be found in UCLA Policy 220
- Is there any policy regarding confidentiality and **TA evaluations**? I recently had an incident where evaluations were requested for an exception to policy and the department in which my student was a TA would not release her evaluations to me. Is there some sort of policy governing who can access a particular department's evaluation forms?
 - Regarding **sharing information between departments**, the other department has access to same information on OASIS. Therefore, record information sharing is okay. Think about what the role of the individual you are talking with is and think about how the information will be used and in what context.
- Requests for information and FERPA regulations: Are there any limits (or specific recommendations) on **student records disclosures** to Faculty members/ campus officials?
 - SAOs need to hold their ground with faculty when it comes to confidentiality and student records. If they have a problem with your stance, refer them to the Deans of the Graduate Division.
 - **Graduate Division deans** are assigned to departments. Faculty can be referred to the GD deans as resources. Staff can let GD staff know as well.
 - Faculty are not given student records unless they are the chair or on an advisory committee.
 - Staff should assess what role faculty has regarding the student and situation (Policy 220 states “**legitimate educational interest**”).
 - If faculty request a student's personal information, staff can contact the student and let the student decide to contact faculty.
 - If staff does give faculty a student's information, staff should have record of why the faculty is requesting the information (this is also written in policy).
- How do we inform/educate our faculty and TA's about confidentiality and FERPA?
 - Staff can better educate faculty by sending letters/memos to all faculty. We can remind them that FERPA is a federal regulation.
 - Faculty should know they do not need to respond and should not respond directly to requests for student information.
- **Other related information on FERPA and Student Information**

- Departments with student information on **departmental websites** should ask students with FERPA or directory restrictions to submit a waiver if they want their information on the website (i.e., *“you have permission to post a, b, and c about me on the dept. website despite my FERPA or directory restriction”*).
 - The department is responsible for student information posted on their website unless the student posted the information themselves.
 - If departments allow students access to update their website info on their own, the department is no longer liable. Refer to your web manager or IT group to learn how to give students this access.
 - When problems with websites arise, the Dean of Students office reminds students of this public information so the obligation for this information goes to the student as well.

- FERPA considers **alumni** as students. Departments can't give their information to anyone, including development offices, if they have restrictions.
 - URSA is available to alumni.

- Departments need permission from FERPA students to list their names in the **commencement booklet**.

- **Registrar's Service Request (RSR)** can give departments information about which students have a FERPA restrictions. Currently this is at no cost to the inquiring department.

- **If parents of students call**, staff cannot release any information without student's permission, no matter what age the student is (even under age 18) or what type of information they might request.

- Policy 220 has affected contact information on the **UCLA Directory**. Students can go into URSA and change contact information settings.

- If there are questions on how to respond to police or other emergency authorities, or in cases of an emergency regarding student/faculty/staff, you can refer to the **Emergency Coordinator** in your building.
 - There should be an Emergency Coordinator in every building. Please locate who the contact person is. Refer to your MSO if an Emergency Coordinator cannot be identified.

- **GRADES** – Faculty should not give grade information to students via email. Students can be referred to staff or be told to check URSA.

POLICIES/EXCEPTIONS REGARDING CONFIDENTIALITY

Issues covered in this section:

1. Distressed & distressing students
 2. Emergencies
 3. Student information not on record
- If a distressing student gives you very personal information about themselves that pertains to their distressing status, how much of this can you share and with who?
 - Staff/Faculty should only receive as much information as they are comfortable with, express boundaries and explain *“I’m not the best person to talk to”* and direct the student to other resources (counselor, CAPS, CARE team, etc.).
 - If staff hears about an issue from a third party, please still report and do what get the entities aware and connected.
 - Please show affirmation for FERPA by not continuing **email trails** but instead announce what will be happening.
 - If forwarding information via email to CAPS, or responding to inquiring faculty, **end the chain of “Reply All”** and delete all previously emailed information from your reply.
 - If you are not sure who to contact in a situation where a student’s safety is a concern, the best advice is to share with one of the entities on the Red folder-Faculty & Staff 911 Guide.
 - If there is immediate threat to one’s self or to others, call 911 immediately. It is always better to have UCPD on the way and turn them away in case of emergency.
 - Report any instances or communication of criminal activity to the UCPD.
 - If a student is being mistreated and student conduct/behavior is a factor, refer them to the Office of the Dean of Students
 - If student is emotional and has thoughts of harming themselves, refer them to **CAPS (Counseling & Psychological Services)**. If you refer them you are then allowed to share information with the CAPS (or other Consultation & Response Team office).
 - Tell the student you are obligated to report their situation if they tell you something distressing. To ease any potential anxiety about it (or foster any mistrust from the student) explain to student, *“because I have concern for you, I am going to share the info with CAPS,”* or, *“I hear what you are saying, do you mind if I make a quick call to CAPS”*
 - Emphasize that CAPS is a professional counseling office on campus that prioritizes the student’s confidentiality.
 - If student asks for confidence, we have a responsibility to share and must tell that to student. Staff is reporting because we care for student.

- Call CAPS and they will follow up with the student (and you if the issue calls for it). If you feel comfortable walking the student to CAPS, you may, but you do not have to.
 - Keep in mind that you only have to notify the student if you are sharing information with CAPS (not UCPD).
- Once staff hears any distressing information, please take action. Once reported to one of the agencies, the information will get centralized. The agencies will reach out to each other and coordinate.
 - If the student discloses something and you don't mention it to CAPS, it's difficult for CAPS to make a record of or consider it.
 - CARE team – CAPS, CRT, UCPD and the Office of the Dean of Students form a network to respond to students in crisis. Their centralized information network helps to respond and to keep a record of all issues of concern as a preventative measure.
 - All entities meet once a week
 - **Clery Act** – Requires colleges and universities across the US to disclose information about crime on and around their campuses.
 - *Reporting by Clery* - involves filling out an anonymous form. If we report to UCPD or CARE Team, they will fill out the Clery form.
- We are ALL Campus Security Authorities.
 - Keep this in mind when reporting dangerous situations.
- If a student is a victim of physical or sexual assault, domestic violence, stalking, and they do not know what to do, refer them to CARE (Campus Assault Resources & Education) or CRT (Consultation & Response Team), both located at Wooden Center West.
 - **Title IX requires that any act of sexual harassment must be reported.**
 - CARE provides a safe environment to support survivors of sexual assault, dating violence, and stalking. There are three CARE counselors who can help students and give them access to response and prevention services.
 - CRT is a behavior intervention team, networked with CAPS & UCPD, and Student Care Managers are available on the phone to consult with during regular business hours (otherwise call the CAPS 24-hour access line).
 - CAPS & CRT can provide direction to faculty & staff to guide them in a course of action when a student's safety is a concern.
- FERPA and HIPPA
 - Only CAPS and the Ashe Center are protected by HIPPA so they cannot discuss freely, but does give general recommendations.

- As a counselor your actions are protected by FERPA. You are not bound by HIPPA.

Emergency Resource contact information

- Counseling & Psychological Services (CAPS) – <http://www.counseling.ucla.edu/>, (310) 825-0768 (24-hour access to counselors by phone)
 - Consultation & Response Team (CRT) - <http://www.studentincrisis.ucla.edu/>, (310) 825-7291 or (310) 825-0628, or email CRTeam@ucla.edu
 - Campus Assault Resources & Education (CARE) - <http://www.counseling.ucla.edu/care/default.htm>, (310) 825-0768
 - UCPD - <http://map.ais.ucla.edu/go/police>, (310) 825-1491, or 911 (24-hour dispatch)
 - UCLA Sexual Harassment Prevention (Title IX) Office - <http://www.sexualharassment.ucla.edu/>, (310) 206-3417, or contact Cathy Bell at (310)206-3464
 - Los Angeles Suicide Prevention Center (310) 391-1253 (24-hour Crisis Hotline)
- If a student contacts you via **personal email**, or gives you a phone number **not on file** on URSA/SRS, can this be shared with staff/faculty if requested?
 - If a student shares personal information with you it becomes part of the student's record.
 - All student info on UCLA Directory is restricted unless student un-restricts it on URSA. Even if the student un-restricts their info, UCLA can only release the public information (refer to Policy 220 for what is included in public information).
 - Best practice is to contact the student to obtain permission to share information not on file in SRS or the UCLA Directory. Keep a record of their response.
 - If they prefer communication via email/phone not on file, **have them log onto URSA to update their contact information and privacy settings.**
 - Staff can only disclose contact information to faculty if it is for an educational purpose. Safest way to avoid problems is to ask the student if it's OK to pass their info to a faculty member.
 - **All offices/counselors should keep a keep record of the disclosure and the reasons for disclosure (as per Policy 220)**

RECORDS RETENTION

1. The UCOP Records Retention Schedule - <http://recordsretention.ucop.edu/>
- If there is **medical information or financial statements** in a student's records, are these to be retained for the same amount of time with the rest of their file?

- Anything added to the students file (medical records, financial documents, etc.) becomes part of their academic record. If student shares doctor's notes, it becomes part of the student's record. It would be good to put a **confidential stamp** on it.
- Please note that any medical accommodations should be made with **OSD (Office of Students with Disabilities)**. Please discourage faculty and students making their own accommodations.
- Some student records have **counseling notes** and printouts of emails from staff and faculty that the student has never seen. Should these be kept or destroyed before files are sent to Iron Mountain?
 - Students have the right access to see own files. Any file that has student's name on it is considered to be student records. FERPA allows for students to see paper and electronic files. If student sees incorrect information, they can request to amend. They are able to write a disclaimer that would go into the file (this is all in Policy 220)
 - Do not keep anything in a student file that you don't want them to see. Students have a right to their files. If you want to keep "notes" on a student you need to keep it in a personal file (Sole Possession) that is not marked with the student names.
 - **Sole Possession** – if staff have their own personal files (unmarked) that are in a secure location and not accessible or reviewed by anyone other than that staff person, they have "sole possession" of that file and documents in that file do not need to be included in a student's file.
- If something alumni requested is in **offsite long-term storage** and it costs the department to retrieve it, is it okay to have the alumni cover the cost? We get requests for really old syllabi from nurses seeking licensure in a new state (question from School of Nursing).
 - This is for each department/school to establish for themselves. There is no policy that says a department cannot charge for such services. If they write a policy for it, it becomes record in their own department/school and is for them to govern, not the Registrar or Graduate Division.
- I know we are supposed to keep records 10 years for alumni grads students, can we **PDF** them before (or after 10 years) and get an **electronic copy instead of a hard copy**?
 - Refer to the Records Retention Schedule (via UCOP) for the appropriate length of time.
 - You can PDF historical documents instead of keeping paper files.
 - Physical storage or electronic storage is to be used (and paid for) at the discretion of each individual department.
- **Admissions records retention** – How long should we keep admissions materials (i.e. hard copies of GRE's TOEFL, transcripts) of non-admitted applicants?

- Generally, paper files should be kept at the department level from 0-5 years. It depends on what the document/file is. Graduate Division admissions records policy is retain 3 years as stated in the Guidelines for the *Graduate Admissions Process and Codification of the Policies and Procedures Governing Graduate Admissions* (per the UCLA Graduate Council). Refer to the Records Retention Schedule for other files.
- During audits, Graduate Division would like paper files and not electronic.
- Non-admitted (non-matriculated) applicant files should be kept for 3 years. All applicants sign when they apply that all things submitted are the property of the university.
- **Records retention for different types of records** (financial, admission, academic, travel grant, funding, academic petitions, etc. Also alumni) – How long do we keep each type?
 - Matriculated students will have their admissions files as part of their Student Record/File.
 - **Alumni files** should be treated as regular student records for matriculated students.
 - All documents included in a student’s file are considered part of the student record. Follow the Records Retention Schedule and proceed accordingly.
- How long do we have to keep masters comprehensive **exams and** PhD written qualification exam? **Other student work?**
 - Follow the Records Retention Schedule where it may apply.
 - Generally, for other assignments, bluebooks, exams, papers, etc. departments should keep for at least one quarter and notify the student that they will be destroyed after a specific date. Best to send reminders beforehand.
 - It’s up to the department to establish protocol for graduate exams.

SAFEGUARDING STUDENT RECORDS

- Departmental procedures – Best practices
 - There is no authority or policy that directly states where and how student and admissions records should be stored.
 - Ideally, **files and file cabinets are not located in high traffic and communal office areas.**
 - If a department can keep files separately in a locked room, even better.
 - Keep cabinets locked and keep track of who has access to file areas.
 - Electronic files should be treated the same (lock hard drives during campus closures, etc.)
 - Coordinate with your IT group or system administrator to review who has access to shared drives and folders in those drives.
 - Confidentiality agreements would be a good idea for all those who have access to student files.
 - Remember, **UCLA Policy 220 requires a record of all disclosures and reasons for those disclosures.** Any access to a student’s file could be deemed a disclosure. In that sense, be very aware of who has access and who information has been given to.