To: Faculty Senate
From: Susannah Hannaford and David Latimer, fall and spring chairs of the LMIS committee, respectively; Jane Carlin, Kate Cohn, Jeremy Cucco, Andrew Gomez, Quentin Hubbard, Janet Marcavage, Kaity Peake, Lori Ricigliano, Adam Smith
Re: End of year report from the LMIS committee, 2018-2019
Date: May 9, 2019

Dear Colleagues:

This report contains a summary the LMIS committee's work on the charges laid out by the Faculty Senate for the 2018 academic year. For further information, please consult the LMIS committee meeting minutes archived on the university's website. In what follows, we will first address the Senate's two exceptional charges, then discuss progress on the committee's standing charges.

Charge 5: *Circulate the draft of "Best Practices for Managing Sensitive Documents" to the Professional Standards Committee; the Institutional Review Board; Counseling, Health, and Wellness Services; the Center for Writing, Learning, and Teaching; Data Standards; Student Accessibility and Accommodation; Registrar's Office; Student Conduct; Title IX; and Human Resources for feedback in the expectation that in AY 2019-2020 the committee with finalize the document for approval and campus use.*

We note that, per a request by the LMIS committee, the Senate agreed to revise this charge by limiting the draft circulation to faculty committees. Given this, the LMIS sought input on the "Best Practices" working document from the PSC, FAC, IRB, and ASC. Feedback from the committees was varied but some common themes emerged.[1] We will briefly reflect on other committees' responses to our working document.

First, interfacing with the committees brought our audience more sharply into focus: the LMIS "Best Practices" document concerns an *individual faculty member's* handling and management of sensitive information. The different standing committees have security needs that are specific to their particular role and function within the university, and the LMIS cannot fully anticipate each committees' needs. In light of the LMIS "Best Practices" document for faculty, standing committees might wish to craft an analogous document outlining processes regarding sensitive materials that reflect their particular practices and materials.

Second, the committee responses highlighted the need for the "Best Practices" document to address how faculty should handle security issues when working collaboratively on electronic documents (even outside standing committees). At the moment, the university has several electronic platforms on which groups can work collaboratively (e.g., Moodle, Canvas, SoundNet, and now the Google drives). The user interface and function of these platforms differ widely, so

[1] We include in an Appendix the feedback received from these four committees.

the “Best Practices” can only speak generally about security issues associated with collaborative work.

Third, the committee feedback brought to light a likely recurrent issue when crafting a specific “Best Practices” document, namely, the ever-changing technology landscape. As an example, when the LMIS committee first took up the charge to create this document, the use of Google docs was discouraged for both legal and security issues, but now that we are a Google university, the use of the Google Suite is perfectly acceptable, if not encouraged. We imagine in the near future that the Google Suite will be the preferred platform for collaborative work across formal and informal working groups, while platforms like SoundNet will fall out of favor (and eventually be eliminated).

Finally, the question of enforcement arose from a couple of committees. In our document, we emphasize that faculty, at a minimum, must be compliant with FERPA (and if applicable HIPAA) regulations. But, aside from these legal requirements, the documents just suggests best practices. The aim is to promote responsible document management in which faculty are mindful of maintaining others’ privacy.

In response to comments from these standing committees, the LMIS committee thought it best to split the original “Best Practices” document into two separate documents. The first prose document is meant to be relatively timeless with regards to technology changes. It has been streamlined, and its aim is to communicate a spirit of mindfulness in dealing with sensitive information. We provide enough specific examples so that one can identify the document’s relevance to one’s own practices, but it is not so exhaustive as to be overwhelming. The second document is in tabular form. It contains examples of how faculty should manage specific documents and, as such, will need to be periodically updated to reflect the campus’s current technology (though in reality the first document will likely need to be periodically updated). CIO Jeremy Cucco has agreed to have a TS staff member update the documents on a semi-annual basis.

The LMIS committee is currently finalizing the “Best Practices” documents and will include a copy in the final report to the Senate.

Charge 6: *Clarify and publicize to faculty and academic staff the general policies and processes related to making changes in library and information systems as applies to the academic program.*

LMIS considered how best to approach this charge. The first of the committee’s standing charges is to “*develop general policies, procedures and plans in collaboration with the Library Director and the Chief Technology Officer”* and, as such, simply carrying out normal LMIS business and disseminating this work by posting meeting minutes should at least partially address the charge. However, the committee also recognized that over the past few years many

LMIS meetings focused on the processes and policies associated with the adoption of PeopleSoft and more recently with the development of the "*Best Practices for Managing Sensitive Documents"* guidelines. The committee realized that this work probably has limited work on other policies, particularly relating to the library. Finally, LMIS recognized that this charge stems from concerns that some recent decisions related to the library and information systems (i.e., the library shift) seem to have been made without consultation with LMIS or other faculty entities.

In order to understand the decision-making process behind recent changes in the library and TS realms, the LMIS committee decided to focus on specific case studies. Our rationale was that by looking in-depth at the decision-making process in recent and current changes, we might gain an understanding of both the normal (idealized?) decision making process as well as how and why this process is not always possible. The committee also hoped that this approach would help us avoid rehashing unpopular decisions and to move forward with issues currently affecting the university. For the Library, the first exemplar dealt with the reorganization of the archives and the special collections in the library and the second case study focused on streaming videos on campus. In the TS realm, the committee looked at two future decisions: the possible implementation of multi-factor authentication and the updating of multimedia capabilities of university classrooms.

Library case studies

In the fall semester (10/23/18) Library Director Jane Carlin briefed the committee about the ongoing Library shift and discard project, prompted by the move of TS into the lower level of Collins. A thorough summary of this brief is provided as an appendix to this report. This case study illustrates some of the problems in implementing changes to the library. For example, the short time between the announcement of the decision impaired planning. LMIS was not consulted in advance. Similarly, Library and TS staff had little warning. One consequence is that roll out of the impact of the Welcome Center on the library was not sensitive to the demands on faculty and staff at one of the busiest points in the academic year.

The library shift and discard case study also provides insights into the strengths of how the Library involves faculty and academic staff in decision making. For example, the Library has a system of liasons to reach out to faculty, so there was an existing avenue allowing faculty and library staff to work together to mitigate the impact of the decision. In addition, the Library's website is well-maintained, serving as a good resource. Members of the university community were able to get updates on this shift and discard project http://research.pugetsound.edu/Summer2018. More generally, each year the library publishes a summary report (available in hardcopy and also online: https://www.pugetsound.edu/files/resources/web-version_library-report-2017-18.pdf). In addition, the Library staff have worked over the last academic year to develop a Strategic Directions document that is in alignment with the Leadership for a Changing World Strategic Plan. The document is designed to provide a broad overview of major directions for the Library over the course of the next five years and will provide faculty and other stakeholders with a clear understanding of priorities, concerns, and strategies. It should be available for review prior to the end of the academic year.

In the spring semester, LMIS looked at a second case study, involving how to deal with the legal requirements, availability, and cost of streaming videos. Library Director Carlin, Peggy Firman (Associate Director of Collections), and Associate Dean Julie Christoph briefed the LMIS committee about the topic at the April 4, 2019 meeting, and a more thorough summary is provided in the meeting minutes. In brief, this case study illustrates one of the challenges facing Collins LIbrary: while the library still holds many physical products (e.g., books, DVDs) there is an increasing reliance on electronic resources. In recent years, the Library had piloted the use of *Kanopy* streaming service, but in 2018 recognized that we couldn't sustain the financial model of unlimited streaming of the entire *Kanopy* video library. The library and TS staff, along with Dean Christoph have been reaching out -- especially to faculty who use streaming videos in their classes -- to come up with a sustainable solution.

TS case studies

CIO Jeremy Cucco led the LMIS committee through the decision making process behind the implementation of a new potential security protocol: multi-factor authentication. Before changes in campus technology are made, TS attempts to meet with the relevant stakeholders to discuss their needs and concerns. With this in mind, TS evaluates the products on the market that also meet the technical requirements of campus. Then TS reaches out to vendors either formally or informally in order to pilot test the product. If the pilot study satisfies TS and campus needs, then the new technology is adopted and implemented on campus.

Jeremy Cucco also discussed the ongoing update of the multimedia capabilities of campus classrooms. As with the previous example, software and hardware options must meet the technical requirements of campus; in this case, requirements narrow the choices considerably. With the software/hardware decisions made, TS then must determine which classrooms should be upgraded first. Though there are roughly 130 classrooms on campus, TS can only upgrade a dozen per year. To develop an upgrade schedule, TS is analyzing the data from TS request tickets and consulting with faculty who schedule courses in the highest-ticketed classrooms. Through targeted communication with a small body of faculty, TS is attempting to prioritize the most problematic classrooms first. Once these upgrades have been made, TS staff will provide training on how to use the new classroom technology for those who teach in that particular space.

General comments

- The library and TS are more tightly linked to teaching than many other divisions on campus (facilities, student life, admissions). Thus, before making a major change to the library or TS, it would be advisable to consult with faculty. LMIS is the committee where major announcements and issues associated with policy should come (if timing allows) and perhaps LMIS might also support short updates of key issues at all faculty meetings.

- Many decisions by TS and the library are driven by budget and by legal requirements. As long as the reasons for decisions are clear (transparency) most faculty will understand the need to make changes.

- As a result of LMIS discussions about communication, TS has now implemented monthly updates about activities and issues that are sent to the campus community. The Library has been doing this through faculty coms with the Collins Library Links and direct communication with departments on a routine basis for years.

- And finally, as a group, faculty are not very forthcoming when proactively asked for input. Both Technology Services and library open forums are often poorly attended by faculty, and emails from TS and the library providing information about updates get only a handful of responses. We should probably do better, if only to establish good relationships we can draw on when there is a tough situation. We do feel that the library's model of assigning Library Liaisons to departments assists in the flow of communication between the faculty and library staff.

The standing charges laid out in the Faculty Bylaws are:

1: *To develop general policies, procedures and plans in collaboration with the Library Director and the Chief Technology Officer.*

2: *To provide recommendations and advice to all parts of the University community on the role of the library, media and information systems in support of the academic program.*

3: *To review periodically the mission and objectives of the library and information systems and to recommend such changes as are needed.*

4: *To review periodically the collection development plan for the library to ensure that a balanced collection is maintained for effective support of the academic program*.

During the 2018 academic year, the LMIS committee acted on these charges as follows. On 9/26/18, Jane Carlin began a discussion on the long-term sustainability of the Makerspace; questions remain on how to staff the space and how the space should be used. We expect to follow up with this earlier discussion in one of our remaining meetings. On 2/1/2019, the committee discussed with Jeremy Cucco recent phishing attempts at the university, and Cucco spoke about a new mandatory, online training course designed to bring faculty up to date about such risks. At the same meeting, Cucco also mentioned that he will send out a monthly email update on TS activities so that there will be greater transparency about what TS is doing. On 3/1/2019, Cucco briefly discussed the excessive amount of printing on campus. The Print Green initiative is relevant only for students, but faculty are responsible for well over half of the printed pages on campus. For the remainder of 3/1/2019 meeting, Educational Technologist Kaity

Peake gave a presentation of the functionality of Google's G Suite. This overview was particularly useful in light of the "Best Practices" document.

Looking ahead:

With an eye to next year's work for the LMIS committee, we would like to roll out the "Best Practices" document to the faculty. Though floor time at a faculty meeting is at a premium, particularly given the important work of the CTF, we feel the information might be most effectively communicated by briefly advertising the document at a faculty meeting early in the semester. Additionally, we recommend that a discussion of best practices for handling sensitive documents should be included in new faculty orientation. Also, a yearly email from the Provost about the management of sensitive documents will help remind continuing faculty of this important issue. Finally, a sensible repository for the document should be found on the university's website, perhaps under the Policies heading of of the Faculty and Staff page (https://www.pugetsound.edu/gateways/faculty-staff/).

Additionally, as mentioned above, the library's holdings are shifting to match the modern reliance upon digital resources. As an example, the library increasingly subscribes to the electronic, rather than print, version of academic journals. The ongoing trend of access vs. ownership will continue to play a significant role in decisions the library makes associated with resource management. We suggest to the Senate that the LMIS committee engage in a discussion about journal pricing and bundling with the hopes of sparking a campus-wide conversation about the issue.

In light of a probable curriculum shift, the LMIS committee briefly discussed how the changes might impact the library and technology services. Though the outcome is uncertain, it is likely that the new curriculum will emphasize high-impact practices that may be catalogued electronically (in e-portfolios, for instance). Jane Carlin suggests that the LMIS committee might wish to consider the long term preservation of those projects (e.g., what platforms the library can support, how we develop the discovery layer to find those in the future). The senate might wish to charge the LMIS committee to explore the long-term storage of documents relating to student high-impact practices.

BEST PRACTICES FOR MANAGING SENSITIVE DOCUMENTS

INTRODUCTION

This document is intended to provide guidance in the management of confidential and potentially sensitive documents that faculty might retain either as electronic documents or hard copies. At a bare minimum, faculty, like all university members, must comply with federal law as outlined in the Family Educational Rights and Privacy Act (FERPA); a summary of the university policies and procedures designed to protect the privacy of student education records can be found at the following link: https://www.pugetsound.edu/academics/advising-registrar/know-educational-rights/. However, faculty typically retain sensitive documents such as student emails, CVs, grade spreadsheets, graded work, recommendation letters, and related documents which may not legally be a part of the student's official education record but nonetheless contain sensitive information about the student. Additionally, faculty often retain both confidential and sensitive documents which do not fall under the purview of FERPA but nonetheless contain sensitive information that should remain confidential. Such documents could include evaluation letters of colleagues (including off-campus personnel), job-search materials, research or clinical materials, and service related documents from committees on and off campus.

CONTEXT

Questions continue to arise about how long to retain documents, where to store them, and whether or not retaining documentation that is linked to an individual puts the university at risk (e.g., a student transcript or disability disclosure). At the request of the Faculty Senate, the LMIS Committee addressed this topic over the 2017-2019 academic years. As we reviewed existing documentation, current protocol, and legal requirements, we recognized that document retention is a complex issue. This document seeks to provide general recommendations and guidance for faculty in a practical manner. Because technology and technological platforms continually change, specific advice on document storage can be found in an updated accompanying table. We found the Student Affairs

Policy for Document and Data Retention and Destruction from the University of California, Santa Barbara, very useful in compiling our recommendations and acknowledge its use with permission. It should be noted that this document is not intended to be a policy, rather guiding practices that when applied with critical thinking, make safeguarding private information more feasible.

RECOMMENDATIONS

We recommend that each faculty member be aware of the location of all sensitive documents in their possession, both in electronic and hard-copy form, and develop a plan to organize, store, and annually eliminate these documents. Electronic documents are most secure on each respective faculty member's university provided personal network drive: stafffiles.pugetsound.edu/username. Information about accessing one's personal network drive can be found at https://www.pugetsound.edu/files/resources/mapping-to-a-network-share-2.pdf.

University-issued personal computers are generally more secure than personally-owned computers, because of the more stringent password policies, required antivirus and automatic system updates, and because they are encrypted. As such, it is preferable to store university-related data on university-issued computers.

There is no need to retain official university correspondence such as a student transcript or grades. If sensitive documents are required as working documents, follow the guidelines listed below in Electronic Records. If you need copies for letters of recommendation or review, these can be supplied by the student and should be deleted once consulted. Below we provide guidelines specific to electronic and hard-copy formats.

We end this document with some suggested guidelines regarding the destruction of less-sensitive documents. The costs and risks associated with the long-term electronic storage of documents are not trivial, and we encourage faculty and departments to develop practices that recognize this fact.

ELECTRONIC RECORDS

Faculty should follow the procedures below when considering electronic records. Technology Services can provide guidance and assistance; send requests and questions to the Technology Service Desk (servicedesk@pugetsound.edu).

1. Email: Emails containing sensitive information should be marked as such. For example, use "confidential" in the subject line of emails, and for documents, use the watermark feature to identify them as confidential documents. Delete appropriate messages from folders and then empty the Deleted Items folder in your email client. Legally, information transmitted by email is not considered confidential.

   (a) In terms of communication with students, we should treat emails as if they were protected under the FERPA statutes. Note that even prospective students are protected by FERPA.

   (b) Email should not be archived on your personal network drive.

2. Collaborative work: Faculty often work collaboratively across many technological platforms (e.g., Canvas, Google Drive, Digication, Network File Shares). Faculty evaluations, collaborative research, and committee work often require that sensitive documents be shared on a common drive. When stored on university supported platforms, sensitive documents are secure; however, faculty must be mindful that if they download such documents to their university-issued personal computer then these documents should be deleted once they are no longer needed. For files on Network File Shares, once files are deleted from this platform, they will be purged from the system and not included in future backups. The university keeps these deleted files locally for 8 weeks, remotely for an additional 8 weeks, and in cold storage for up to one year per our Data Retention Policy (https://www.pugetsound.edu/about/offices-services/technology-services/policies/backup-and-data-retention/).

3. Personal Network Drives: University data (e.g., material for classes, research, etc.) that is stored in personal network drives is subject to the same retention and elimination policies and files past their retention periods should be deleted in the same manner as those on other network file shares.

4. Local Hard Drives: University data should not be kept on users' local hard drives because it can be lost if the device is stolen or when the drive fails. If university data exists on these drives, it should be moved to the appropriate location on a network file share or Google Drive so that it can be backed up and secured.

5. University Data: Contact Technology Services for assistance in eliminating all records that are past retention if you are unsure of how to properly permanently delete files. Staff may be able to help set up automated mechanisms for review and/or elimination of records when retention periods are reached.

6. Acceptable Incidental Personal Use: Personal files stored locally on a university computer as part of acceptable incidental personal use of campus electronic resources should be stored on a short-term basis. Long-term storage should be on a personally owned flash drive. Files stored on university owned equipment may be subject to search in the case of legal action and may also be accessible to other people using the computer. Personal non-university related files (e.g., photos, videos, music, etc.) should never be stored on Personal Network Drives, because the university incurs the cost of storing and backing up these files.

HARD COPY RECORDS

When hard copy records and documents are to be destroyed, faculty should follow the procedures below:

1. All files with confidential information must be shredded, either manually in the office or through the university's contracted document destruction service:

https://www.pugetsound.edu/about/offices-services/office-of-finance/procurement/furniture-shredding-toner/#shredding,

2. Confidential documents and records requiring shredding may not be taken off campus for personal destruction (e.g., an employee owns a paper shredder and offers to shred the documents at home–this is not allowed).

3. Non-confidential documents or records may be destroyed through disposal in departmental or university-controlled recycling bins.

GUIDELINES FOR LESS SENSITIVE INFORMATION

Some records are not sensitive in nature, but still should be given consideration from time to time to make sure that academic departments are most efficiently using resources. The following are discussion points that each department could consider, perhaps on an annual basis:

- How are members of the department doing collaborative work? Do they utilize the share/network drive? Does each department have a network drive (if not, Technology Services can assist). Or, are they using university provided Google Drives? Programs like Dropbox should be discouraged, especially in cases where projects are distinctly tied to the university, for reasons of licensing and data protection.
- Documents and files that take up a significant file size should be evaluated. Departments could host a "clean-up day" where an audit guides work to minimize and remove unneeded files. For example, if pictures have been taken at a university event, do they all need to be saved? Or, if someone utilized a revision process, which resulted in several Word documents, all with similar content, with various revision dates on each of the files, do they all need to be saved, or perhaps only the final product?

APPENDIX: GUIDELINES FOR DOCUMENTS OF LASTING AND PERMANENT VALUE TO THE UNIVERSITY

While this document primarily focuses on the management of personal documentation, please keep in mind that some resources generated by you or your department may be appropriate for the University Archives. Many documents are important to retain as part of the lasting and permanent record of academic life at the University of Puget Sound. Academic departments are encouraged to establish guidelines for the retention of materials associated with their work. The Archivist & Special Collections Librarian is available to work with your department to establish a records retention program. Recommended guidelines for the retention of academic department records, developed by the Archives & Special Collections, can be found at the following link: https://www.pugetsound.edu/academics/academic-resources/collins-memorial-library/archives/acad-dept-rec-guidelines/. Materials of enduring historical value such as course syllabi, reports and planning documents, department histories, newsletters and other publications as well as records documenting major events may be appropriate for transfer to the Archives & Special Collections. Please contact archives@pugetsound.edu.

GLOSSARY:

1. **Encryption** – Encryption can refer to the encryption of data in motion or the encryption of data at rest. The encryption of data in motion is most often seen when visiting a website where the address is preceded by https versus the unsecure http. Encryption of data at rest is encryption when the data stored on a hard drive is protected using mathematical algorithms designed to obfuscate it. Data on an encrypted hard drive cannot be read by anyone who does not have access to the appropriate key or password. Encryption methods differ depending on if you want to encrypt a Mac or PC or a mobile device. Technology Services has information on how to encrypt your personal devices: https://www.pugetsound.edu/about/offices-services/technology-services/help-support/data-encryption/.

2. **External hard drive** – An external hard drive is a portable storage device that can be attached to a computer through a USB or other external means. External hard drives typically have high storage capacities and are often used to back up computers or serve as added file storage for large files such as video and audio files.

3. **FERPA** – The Family Educational Rights and Privacy Act is a federal law that protects the privacy of student education records. Detailed information can be found at the following link: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. The university's current FERPA Guidance can be found here: https://www.pugetsound.edu/academics/advising-registrar/know-educational-rights/

4. **HIPAA** – The Health Insurance Portability and Accountability Act sets the standard for protecting sensitive patient data. Any company that deals with protected health information must ensure that all the required physical, network, and process security measures are in place and followed.

5. **Personal Network Drives** – A personal network drive, often referred to as a “home directory” or “personal share,” refers to the network file share where a user’s files can be backed up or stored. Your home directory at Puget Sound is located at stafffiles.pugetsound.edu/username.

6. **IRB** – The Institutional Research Board serves as an objective third party, an oversight committee, governed by federal regulations with the purpose of protecting and managing risk to human participants involved in research.

7. **Network File Share** – A network file share is server storage space accessible on a network with different levels of access privileges. Individuals or groups may have access to specific file shares. File shares can be mapped from a user’s computer, creating a shortcut link to access that specific file share.

8. **University data** – University data includes digital data contained on the Learning Management System (LMS), e-portfolio system, the streaming media server, and other university provided academic software systems. Any data created while performing work associated with the university is data that is technically owned by the institution and thus referred to as university data. This also includes all emails and documentation relevant to university business.

Recommended Document Storage Guidelines

Legally Protected Documents

FERPA Protected | Highly Confidential | 3–5 Years Minimum Retention

Includes:

Student records (official and unofficial).

All admission application documents including: formal and informal information linked to individual students, financial information, interview data. All personal contact information of students and their families. Student grades and grade sheets. All materials collected as part of student disciplinary actions, complaints, or hearing boards. All communication with students about grades, performance, disciplinary action, or any graded material or work product.

Health, academic, or personal data from CHWS, Office of Student Accommodations, Dean of Students, Residence Halls, e.g. communications about student status, progress, disposition of hearing boards, petitions, conduct boards, other adjudications, communications about academic accommodations, illnesses, or leaves of absence.

Confidentiality:

Not shared without signed informed consent, and release. Release includes specified time frame, and purpose. Must conform to FERPA guidelines. For specific guidance, contact the Registrar, the university's official FERPA privacy officer. Retention and review of permissions and releases should be addressed at an administrative level and in departments and committees.

Storage:

Store in: Digital documents should be stored on University Share Drive, university Google drives with appropriate sharing, or encrypted drive. Drives not in use should be stored in locked secure cabinets. Use locked file cabinet for paper records.

Do not store in: Email files, non-encrypted computer, external drive or internet-based storage, cloud storage other than those specifically designated by the university, cell phone. Do not store on personal computer or laptop.

Retention and Purge Recommendations:

Minimum Recommended Retention is 3-5 years unless likely usage clearly extends longer. Materials that can be accessed easily in the future should be purged when there is no indication of future use. Purge methods: shredding of hard copies via locked commercial containers, full erasure of digital including email, cloud, external and computer drives.

Resources for Further Information; Web Links:

Note: Student Healthcare documents collected on campus are covered by FERPA, unless collected by OT/PT clinics or as part of research program that falls under HIPAA guidelines (per grant or professional licensing of those conducting the research).

When in doubt, faculty, students, and staff should follow HIPAA and FERPA guidelines, until specific protocol is identified.

Community research samples are not covered by FERPA. Data from non-students should be handled in accordance with HIPPA.

HIPAA Protected | Highly Confidential | Use HIPAA Retention Guidelines

Includes:

All health data collected by the university for staff, faculty or the community should be handled in accordance with HIPAA guidelines, regardless of whether or not the data is technically HIPAA protected. This includes physical health, mental health, and also education or work-related accommodation information). All health research data on non-students collected (or stored on campus) by faculty, students or staff should be handled in accordance with HIPAA guidelines.

Note: The schools of OT and PT are the only programs required to follow HIPAA guidelines on campus, as they are HIPAA entities.

Confidentiality:

Not shared without signed informed consent, and release. Release includes specified time frame, and purpose. Must conform to HIPAA guidelines. For specific guidance, contact the Registrar, the university's official HIPAA privacy officer. Retention and review of permissions and releases should be addressed at an administrative level and in departments and committees.

Storage:

Process and Store HIPAA documents: on encrypted drives, or within a 3 rd party, HIPAA-certified solution (such as those now in use by the University, i.e. MyClientsPlus, WebPT, Jituzu, and Point-N-Click).

Do not process or store: No HIPAA documentation should ever be stored on the university shared drives. Do not process on non-encrypted drives or personal computers.

Retention/Purge: Follow HIPAA guidelines for retention of Healthcare Data

Note: Professor Ann Wilson is the university's official HIPAA Privacy Officer and thus the campus contact for HIPAA regulations.

IRB Protected | Highly Confidential | Use IRB Retention Guidelines

Includes:

All student and faculty research data governed by IRB protocols, including participant information collected during recruitment or participant selection procedures.

Confidentiality:

Not shared without signed informed consent, and release. Release includes specified time frame, and purpose. Must conform to IRB guidelines. For specific guidance, contact the Registrar, the university's official IRB privacy officer. Retention and review of permissions and releases should be addressed at an administrative level and in departments and committees.

Storage:

Process and Store IRB documents: on encrypted drives, or within a third party, HIPAA-certified solution (such as those now in use by the University, i.e. MyClientsPlus, WebPT, Jituzu, and Point-N-Click).

Do not process or store: No IRB documentation should ever be stored on the university shared drives. Do not process on non-encrypted drives or personal computers.

Retention/Purge: Follow IRB guidelines for retention of Healthcare Data.

Note: Contact Chair of Institutional Review Board and/or department or school representative.

Sensitive Documents

Student Documents | Moderately Confidential | 3–5 Years Retention; 1–2 Years Student Work

Includes:

Letters of Recommendation, student papers and other academic related products, emails from students containing personal information or documents. Specifically, student documents that do not meet the criteria of being a "Student Record" and therefore meeting the criteria above under "FERPA Protected."

Moderate Confidentiality:

Shared with permission and limited usage. Permission specifies level of confidentiality, time frame of permission, and recommended storage guidelines.

Storage: May vary depending on the nature of the document and permissions received to distribute or share

Retention: Recommended 3-5 year retention, with extension based on immediate or long-term needs

Student Work retained for 1-2 years

Contact: Academic Standards Committee; Dean of Students Office; Professional Standards; Individual Department Guidelines

Faculty & Staff Professional Docs | Moderate–High Confidentiality | 3–5 Yrs Retention

Includes:

Faculty Evaluation Letters, Letters from Evaluation Committees, Committee notes from review or disciplinary boards or petition committees. Materials used for recruitment of potential employees and faculty (often includes CVs and letters of recommendation)

Moderate to High Confidentiality:

Shared with permission and limited usage. Permission specifies level of confidentiality, time frame of permission, and recommended storage guidelines.

Storage: Letters of Evaluation and disciplinary actions should be treated with the highest level of confidentiality, stored in locked filing cabinets and encrypted drives.

Retention: Recommended 3-5 year retention, with extension based on immediate or long-term needs.

Contact: Professional Standards Committee Office of the University Provost

Other Professional Docs (Outside Univ. Roles) | Variable Confidentiality | 3–5 Yrs Retention

Includes:

Letters of recommendation or evaluation for colleagues outside the university; correspondence for reviewing academic articles, books, or grant proposals; correspondence and documents related to positions in professional organizations; professional financial documents such as book contracts; Letters for colleagues outside the university.

Variable Levels of Confidentiality:
May be confidential, depending on the type of document, purpose, or organization.

Storage: May vary depending on the document type. If stored on UPS systems (digital or paper), review annually.

Remove if no longer needed or can be stored securely elsewhere. Faculty may use "University Storage" for some of these materials Faculty may use "University Storage" for some of these materials.

Retention: Recommended 3-5 year retention, with extension based on immediate or long-term needs

Resources: Professional Standards Committee Faculty may also consult with professional organizations or ethics committees for best practices and standards in their field.

Personal Docs of Faculty and Staff | Variable Confidentiality | Retention determined by owner

Confidentiality varies depending on the type of document, and purpose.

Storage: varies depending on the type of document, and purpose.

Do not store: on University share drive, university computers, or in the university email system. The University share drive, computers, and email are engineered and managed to address FERPA concerns. The University cannot be responsible for the personal financial information of faculty and staff stored on University resources.

Any personal information stored on university-owned equipment or services has the potential to be accessed by others.

Retention is determined by individual faculty/staff.

Notes: Professional Standards and Tech Services Policies may need to clarify further.

Policies where this is covered include: Privacy and Appropriate Use of Resources Policy, Email, Voice Mail and Network Access Policy.

Documents of University Archival Interest | Consult with Librarians

Includes:
Materials (proposals, brochures, photos, historical records, letters) associated with university traditions, events, initiatives, artistic and intellectual performances, student organizations, portfolios etc.

Confidentiality varies depending on the type of document and purpose, but in most cases low.

Storage: Retain in original form if possible and contact librarian for guidance on sharing, storage, retention time, and location.

Retention: Please consult with University Librarian or Archivist for guidance.

Contact: Jane Carlin, University Librarian

Other Contacts: Library Archivist (Adriana Flores) or Assistant Archivist (Laura Edgar)

LMIS feeback from the PSC

Sue Hannaford

Mon 11/19/2018 10:20 AM

To:Sue Hannaford <shannaford@pugetsound.edu>; Janet Marcavage <jmarcavage@pugetsound.edu>; Andrew Gomez <andrewgomez@pugetsound.edu>; David C Latimer <dlatimer@pugetsound.edu>; Adam A Smith <aasmith@pugetsound.edu>; Jeremy L Cucco <jcucco@pugetsound.edu>; Kate Cohn <kcohn@pugetsound.edu>; Lori M Ricigliano <ricigliano@pugetsound.edu>; Lisa F Wood <lwood@pugetsound.edu>; Quentin T Hubbard <qhubbard@pugetsound.edu>;

Please see the response from the Professional Standards Committee regarding our best practices document. (Forwarded email from Andreas Madlung, PSC chair below)

Sue

From: Andreas Madlung
Sent: Monday, November 19, 2018 10:01 AM
To: Sue Hannaford
Subject: Re: Checking in Re: LMIS request for ASC and PSC

Hi Sue,
Below, please find the copied PSC minutes pertinent to your LMIS inquiry. Let me know if you need any clarifications.
Cheers,
Andreas

Chair Madlung led us in responding to Sue Hannaford's request for PSC to review the document drafted by LMIS called *Standards and Best Practices for Handling Sensitive and Confidential Documents* and to respond to four questions listed below, along with our responses*.*

PSC members want to thank the LMIS for their good work in drafting the document and acknowledge that it represents substantial work.

1. **Within the Committee, have you discussed how you handle and manage confidential information?**

Provost Bartanen said that the PSC has worked to have the minutes be informative while maintaining confidentiality. The minutes reference the discussion while maintaining confidentiality.

The PSC is guided by the *Faculty Code* with respect to the minutes of appeals or grievances. If something comes to PSC that requires such confidentiality, chapter 3 (for evaluation appeals) and chapter 6 (for grievances) of the *Code* are clear. The recording of the discussion and the document summarizing the discussion goes into the locked archives behind a locked door, where such faculty records are kept for six years.

2. Do you or are you planning to have documentation associated with your Committee processes and procedures that address handling and management of confidential information? If so please share it with us.

The PSC handles and manages confidentiality according to the *Faculty Code*. The PSC has minutes from last year and the prior two years about the taking of minutes. For a couple of meetings, there were two sets of minutes, the published minutes those that maintained confidentiality, and the more functional and detailed minutes for the PSC.

Provost Bartanen suggested that the PSC could create a document that says how the PSC handles the meeting minutes.

A Mifflin suggested a Faculty Senate handbook for how things work for committees, which would be especially useful to new members of the committees, as well as new chairs. Several PSC members agreed with this idea.

3. As you review the LMIS document, what parts of the guidelines and best practices are helpful? Unclear? Do you have suggestions for improving the document?

As you (LMIS) continue to work on this, what is the status of this document? Do you view this document as providing guidelines, or requirements? Are there policy implications that PSC should review?

Is LMIS working with legal counsel with respect to the consequences if there is a data breach?

We as faculty and PSC members share a common interest with LMIS, that we want confidential information to be secure. Faculty want an easy way to go back and forth from the office and home. The Cloud makes it easy. However, according to the LMIS document, Dropbox and Google Drive are not secure places for confidential documents. The PSC would appreciate guidance as to what cloud services are secure.

Would faculty be liable if something was hacked out of his/her/their personal Dropbox?

Provost Bartanen told us that Puget Sound has become a Google University and is moving (or has moved) to Google Suite. Does this mean that the Google Drive within the Google Suite is more secure? Will this be the new preferred location for confidential documents?

A Madlung asked if LMIS will adopt guidelines regarding file saving. Could LMIS adopt guidelines for best practices for new faculty members and best practices for existing faculty members (with multiple hard drives, flash drives, computers in various states of functionality).

With our PSC hats, what if we get news that the preferred way is X, and faculty member prefers to do Y. We'd like clarity on what is required of faculty, versus what is preferred. If we're all behaving using our best professional judgment, then if there is a problem, can we assume that we are legally protected?

4. Can you comment on how you might apply the guidelines within the framework of your Committee work?

We have questions about the preferred location for confidential information.

LMIS indicates that the preferred location for confidential and sensitive documents is SoundNet, which is Puget Sound's name for Sharepoint software. PSC members indicated that SoundNet is not particularly user friendly.

Or is the preferred location for confidential and sensitive documents Google Suite? If yes, then the LMIS document may need to be updated.

PSC and FAC documents are HR or personnel documents, not under FERPA or HIPAA purview. It would not be difficult for PSC to be in compliance if we had a secure location for storing the confidential files that was for the long-term and easy for faculty to use.

To summarize, we appreciate the work done by LMIS to draft the document *Standards and Best Practices for Handling Sensitive and Confidential Documents.* PSC members agreed that we feel good about how the committee handles sensitive and confidential documents. Several committee members agreed we have work to do as individual faculty members and look forward to clarity about best practices for new and existing faculty with respect to handling sensitive and confidential documents.

Andreas Madlung
Professor and Chair
Biology Department
UNIVERSITY OF PUGET SOUND
1500 N Warner St
Tacoma, WA 98416-1088
Tel: 253-879-2712 | Fax: 253-879-3352
http://www.pugetsound.edu/faculty-pages/amadlung

Dear Andreas and Jo,

I'm writing in my role as LMIS chair to check in and see if the Academic Standards and Professional Standards Committees have had a chance to look over LMIS's draft document.

Let me know if you have questions,

Sue

I'm writing to you as the chairs of the ASC and PSC committees in my role as chair of the LMIS committee. (We are so powerful!)

Scroll down for the boiler plate and formal request. I would like to add my own personal plea to this request. I had never thought much about how many confidential information I had on my computer, in my emails, or as paper until LMIS started looking at this question. I quickly realized that I have a lot of information -- home addresses of my advisees and information about their disabilities, letters of recommendation for incoming students and for candidates for faculty members, notes from hearing boards (from when I was on the PSC), drafts of letters I wrote when I was on the FAC, my own letters of evalution for lots of colleagues, and more. I think that many other faculty members have a similar collection, and if this information were to be hacked it could cause (at a minimum) embarrassment and even legal exposure to me and the university. So, please, ask your colleagues to think about their own exposure and provide us feedback.

Thanks in advance, and if you have any questions for me, I am happy to chat with you.

Sue

Last year the LMIS Committee developed a document which is attached titled: *Standards and Best Practices for Handling Sensitive and Confidential Documents.* As a follow-up to our work, the faculty senate has charged the current LMIS Committee felt to gather information on how standing faculty committees manage sensitive and confidential documents.

We ask that your Committee examine the LMIS document and provide responses to the following questions. We would prefer responses by December 1, 2018. Once your feedback is shared, we will compile the results and share with Faculty Senate. Our objective is to ensure that faculty committees operate within the framework of best practices.

1. Within the Committee, have you discussed how you handle and manage confidential information?
2. Do you or are you planning to have documentation associated with your Committee processes and procedures that address handling and management of confidential information? If so please share it with us.
3. As you review the LMIS document, what parts of the guidelines and best practices are helpful? Unclear? Do you have suggestions for improving the document?
4. Can you comment on how you might apply the guidelines within the framework of your Committee work?

Fw: FAC input on LMIS document

Sue Hannaford

Wed 1/30/2019 9:05 AM

To:David C Latimer <dlatimer@pugetsound.edu>;

From: Kristine Bartanen
Sent: Monday, December 10, 2018 11:48 AM
To: Sue Hannaford
Cc: Kristine Bartanen
Subject: FAC input on LMIS document

Dear Sue,

Thanks for your work with LMIS related to best practices for managing sensitive documents. I am writing with notes from the Faculty Advancement Committee.

1. FAC has been involved increasingly in transition from paper to electronic documents.
    a. Moodle evaluation files are used more often than not by evaluees. This year, only 1 file is not a Moodle file.
        i. Our understanding is that the Moodle evaluation site will be maintained, even as course LMS moves from Moodle to Canvas.
        ii. The paper file maintained, as per Faculty Code, Chapter 3, Section 8, is protected in a locked file cabinet behind a locked door (Provost's Office); historical paper files are in locked files in a locked portion of the Library (a space/records management issue, as the space is full).
    b. FAC uses a confidential shared drive for access to all components of the evaluation file (departmental standards, most recent evaluation letter, personal statement, colleague letters, department deliberation summary (and summary of letters, if closed file), originals of Instructor and Course Evaluation Forms, and any official correspondence as outlined in the Faculty Code. Only FAC members and the Administrative Assistant to the Provost have access to the shared drive.
    c. This year, for the first time, we have used a confidential Google drive within G-Suite for drafts and editing of FAC letters for evaluees. Only FAC members and the Administrative Assistant to the Provost have access to the Google drive.
    d. **FAC is interested in learning of the relative security of a shared drive vs. Google drive** (given Google Drive was discouraged in the LMIS draft document; if, in fact, Google drive is more secure, we could entirely switch to that mode. Our practice has been to use a password on any file materials for an evaluee who is a member of a department of someone serving on FAC; we do not think that capability appears to be possible in Google (or maybe we need lessons), so that is a possible flaw relative to a shared drive. (We rely on top professional/ ethical responsibility of FAC members, just as we do if there is any reason for a member to recuse themself from review of a file.)

2. All computers used by FAC members are encrypted, including laptops.
3. Members minimize any printing of materials. **FAC would like to know if the "print queue" between computers and departmental or the Provost office printers is cleared on a daily or other basis so that there is not vulnerability in the computer -> printer network**. It is possible, if network printing is not secure, that the university should provide in-office printers for FAC members.
4. In any email correspondence, e.g. if needed to let members know that Sue's letter is ready for review, we use initials; if LMIS recommends use of "a random number" rather than initials, we could do that. Obviously, letters themselves need to have names.
5. FAC checked with legal counsel a couple of years ago; counsel affirmed that electronic signatures are acceptable as pen and ink signatures.
6. SETs (Instructor and Course Evaluation Forms/I&CEF), what the literature calls student evaluations of teaching): There is a whole protocol for departmental assistants to collect, type – if requested, scan SETs, label, and store. There is a confidential evaluation shared drive maintained by TS; hard copies are hand-delivered to the Provost's Office. Scans of the evals are transmitted to the evaluee by email, thumbdrive, or (apparently, if requested, in hard copy – news to me!). Department chairs have access to specific evals in an "admin hold" area of the confidential evaluation shared drive for a limited period of time. Original hard copy SETs/I&CEFs are retained for 10 years (see archives information above).
7. OT and PT requested from PSC the ability to put the official Puget Sound SET/I&CEF into Qualtrix for electronic administration. **FAC has no information on the security/vulnerability of Qualtrix, and we would like to learn of that**.
8. Evaluation materials are provided to the President and to Trustee members of the Academic and Student Affairs Committee of the Board of Trustees through Diligent Boardbooks, a secure boardbook software. The administrative assistant to the Provost, and administrative assistant to the Board (S. Benevides) have access as managers of the Diligent software. The materials are posted two weeks prior and taken down from Diligent immediately following a Board meeting.
9. FAC does not consider SETs/I&CEFs to be student educational records, so we do not see a FERPA issue in the evaluation process. Occasionally, there are student letters or notes in the files; we do not see those as student educational records either. If LMIS so considers them to be educational recors, or is unsure, I would be happy to consult legal counsel.
10. FAC discussed "what is the threat?"
    a. An evaluee altering a file?
    b. Malfeasance on the part of someone trying to expose an evaluee?
    c. Someone trying to discern individual colleague recommendations in a closed file? To discern an FAC "vote"?
    d. Outside exposure of the Puget Sound evaluation process in terms of potential "bad practice"?

If FAC can be of further assistance, or needs to be aware of other risks or best practices, please let me know.
Best,
Kris

Kristine Bartanen | Provost

UNIVERSITY OF PUGET SOUND
1500 N. Warner St. #1001
Tacoma, WA 98416-1001
253.879.3205
provost@pugetsound.edu

pugetsound.edu

Feedback from the ASC

i. Within the Committee, have you discussed how you handle and manage confidential information?

Before seeing this document, the committee assumed that we (and the University) were taking the necessary precautions. On the surface we were—hard copies were collected and shredded, electronic versions were on the shared drive. However, we never thought beyond that (for example, when items were downloaded to a computer, etc.).

ii. Do you or are you planning to have documentation associated with your Committee processes and procedures that address handling and management of confidential information? If so please share it with us.

After reviewing this document, the committee decided that we will craft a document specific to the handling of sensitive documents relative to the committee such as petitions and Honor Board materials. This summary document can be "reviewed" at the beginning of each semester after the petition subcommittee has been assigned. The key points in the summary will be:

**To store and download confidential documents via the University's shared drive.*

**If necessary, to use University email to share materials.*

**Setting a date at the end of the semester to remove petition materials that were downloaded to computer or sent via email.*

iii. As you review the LMIS document, what parts of the guidelines and best practices are helpful? Unclear? Do you have suggestions for improving the document?

1. *We were initially confused by the differences in the requirements between the information that falls under HIPAA vs. FERPA (esp. since the petition subcommittee deals with medical documents for medical leaves/reinstatements, etc.)*
    - a. *After a discussion with Ann Wilson, we now understand that FERPA covers the student at any stage of their "interaction" with the University (prospective students to alumni). We offer two suggestions for clarifying the document:*
        - i. *Begin the table with the section "HIPAA Protected Docs" since they relate to more people (staff, faculty, or community) and the protocols are stricter. "IRB- and FERPA-protected Documents" sections would follow.*
        - ii. *In the "HIPAA protected Docs" section, it states that the HIPAA protected docs relate to "staff, faculty or the community" (i.e. nonstudents). We recommend adding the parenetical to highlight/clarify that students are covered under FERPA*

2. *Several terms were used throughout the document but were not well-defined and may have been used interchangeably.*
    - a. *It may be beneficial to have a section that defines: password protected, secure, encrypted, etc. Is a device that is password protected secure? If a drive is secure, is it also encrypted?*
    - b. *It may be beneficial to have a section in the document that outlines the security "levels" between the various tech systems that people at the University use: PeopleSoft/my Pugetsound, the share drive, email, PCs, Macs, etc. What if the user uses the "remember my password" feature? Does that negate the password protection defense? The "Electronic Records" section begins to outline the various types of electronic records but doesn't go into sufficient detail as to the level of "protection" it provides.*

iv. Can you comment on how you might apply the guidelines within the framework of your Committee work?

The majority of these guidelines apply to the ASC petition subcommittee

Re: IRB response to LMIS "sensitive documents" document

Alexa Tullis

Tue 2/26/2019 5:46 PM

To:David C Latimer <dlatimer@pugetsound.edu>; Ann M Wilson <awilson@pugetsound.edu>;

Cc:Sue Hannaford <shannaford@pugetsound.edu>;

Hi David,
Members of the IRB did discuss this briefly and felt that a discussion of what constituted sensitive data was needed. The committee member who volunteered to look into this further, including the issue of categorizing levels of sensitivity, is currently on sabbatical so the discussion on our end has stalled for now. Sorry I couldn't be of more help.

Alexa Tullis
Professor of Biology
University of Puget Sound
(253) 879-2857

From: David C Latimer <dlatimer@pugetsound.edu>
Date: Sunday, February 24, 2019 at 10:08 PM
To: Alexa Tullis <atullis@pugetsound.edu>, Ann M Wilson <awilson@pugetsound.edu>
Cc: Sue Hannaford <shannaford@pugetsound.edu>
Subject: IRB response to LMIS "sensitive documents" document

Hi Alexa and Ann,

After taking a sabbatical last fall, I'm back on the LMIS committee as chair, and I'm writing to you in that capacity. Last semester, Sue Hannaford reached out to the IRB for comments on an LMIS draft doc called "Standards and Best Practices for Handling Sensitive and Confidential Documents." I see from your meeting minutes that there was some discussion about the draft in your Oct 22 meeting. Has there been further discussion? If so, could you please summarize any comments/concerns/critiques/etc that the were raised?

Many thanks!

David

Library Communication and Policy Discussions
Submitted to LMIS Committee
Jane Carlin, Library Director
Fall 2018

Introduction:

A review of the minutes of the LMIS Committee, as well as the Annual Reports from 2014 to the present time document that LMIS Committee consulted on policies and practices associated with the Library. In addition, a substantial number of reports and updates about library issues and operations were provided to the LMIS Committee.

It is important to remember that the last few years have been a time of substantial change associated with the implementation of PeopleSoft and many of the meetings focused on the processes and policies associated with this new technology. The LMIS Committee has to balance both library and technology issues and that can sometimes be a challenge due to the impact and complexity of operations.

LMIS provided substantial feedback on many issues such as:

- Review and recommendation of circulation policies associated with the new Shared Integrated Library System
- Review and endorsement of the library's recommendation to curtail the Government Depository program
- Endorsement of the effort to develop an Archives & Special Collections research and teaching space

In addition, presentations and documentation were provided to LMIS by library staff on a range of topics, including:

- Explanation of the library budget, as well as concerns and trends in budget management
- LIBQUAL Survey Results
- Collection use and collection development
- The continued shift from print to digital journals
- Update on the Learning Commons and library spaces

Library Shift and Discard Project, 2018:

In terms of the situation that transpired last spring associated with the renovation of the lower level library space and the library collections, the library actively shared information.

- The library communicated via faculty coms and with departments about the project numerous times. There were many moving pieces associated with the project and we did the best we could to share updates and be transparent.

- Liaison librarians also met or talked individually with concerned faculty who wished to review books slated for deselection. In the case of some of the bound journal runs, the library staff packed the journals for delivery to faculty departments.

- An update on the project was shared with LMIS prior to the end of the semester.

- The sheer volume (no pun intended) of the collection shift was immense and required a multitude of internal temporary shifts to accommodate the change of locations of materials, as well as the identification and subsequent discard of materials. Again, at every point we did our best to communicate with faculty throughout the summer.

- Our work is further impacted due to the aging compact shelving that has to be removed. This complicates the space issue. The failing compact shelving combined with the shift project exacerbated the collection review process.

- We created a guide that shares information on the project and requests feedback by October 19, 2018 concerning journal review. This guide was shared with Deans, Directors, and Department Chairs as well as distributed to faculty through faculty coms in fall of 2018: http://research.pugetsound.edu/Summer2018. The guide also provides information about our existing collection development policy and criteria used to review collections.

Feedback about the process from the perspective of the Library:

- Ideally, this project would have been announced far in advance to provide the library with time to plan, consult and follow our established practices of consultation.

- Ideally, this information would have been shared with LMIS well in advance to seek input about how to plan for a thoughtful and reflective review process.

- While it was the Space Study conducted by the University combined with the Welcome Center project that drove the changes, it would have been beneficial to have had the information well in advance so that we could do a better job on soliciting feedback and planning.

- Timing of the project was awkward as it was at the end of the academic year and continued throughout the summer. Not only did this hamper direct communication with faculty, but impacted library work schedules, as well as necessitated a reorganization of work priorities. Staff spent close to 2.5 months of work effort on this project. We are still working on details of this project and have yet to make decisions about final journal locations and discards. The level of commitment and effort was extraordinary and library staff should be commended for their flexibility and willingness to undertake such a large project.

Next Steps:

- Collection culling is an ongoing process and a normal part of the operations of a liberal arts library. Faculty have always been involved in review of collections. Liaisons work with departments to review existing print collections and ask for feedback. Depending on the discipline, approaches vary. We conduct journal reviews and solicit feedback from faculty. In cases of individual journal title increases, we usually check with the department prior to cancellation. In recent years we have actively promoted the shift from print to digital for journals because of demonstrated user preference and space requirements. While the library has shared collection development and budget information through *Collins Library Links*, in formal reports to LMIS, Faculty Senate, and the Administration as well as with academic departments, this project brought to light the need to review, clarify and discuss with stakeholders the current state of our budget, purchases, trends in scholarly publishing, and the future of library collections. We anticipate working closely with LMIS to help foster discussions and to reassess collecting practices with the goal to formulate a shared understanding of the collections and resources of a 21st century liberal arts library.

- The renovation transformed the lower level of the library. The Library's input as to space renovation was largely as an advocate for the retention and enhancement of public study spaces for students. Prior to the renovation, library space studies and observations confirmed that the lower level rooms were prime study areas for students and always in use so it was important to provide enhanced student space in the lower level.

  We are delighted that new and engaging study areas are now available for students.

  During the renovation project, there were many conversations with facilities about additional projects associated with the lower level. Some of the issues that we still need to work on include:

  - Review faculty input after the October 19 deadline associated with the remaining bound journal collections and determine space needs
  - Work with facilities to establish a timeline to:
    - Remove compact shelving in the large journal room
    - Install free standing shelving saved from the former A-C books and re-install in the large journal room
    - Remove wall shelving in the A-C print book room, paint and install counter height computer bar
    - Discuss the possibility of updating the former Archives Processing Room into an expanded Maker area or collaborative work environment