To: Faculty Senate
From: LMIS: Susannah Hannaford (Chairperson), David Latimer, Wade Hands, William Kupinse, Lisa Wood, Jane Carlin, Kate Cohn Jeremy Cucco, and Ann Geason,
Concerning: Report LMIS Charges 2017-2018
Date: April 26, 2018

Dear Colleagues:

The following is a summary of our responses to the Faculty Senate Charges. For further information, we encourage you also to consult the LMIS minutes posted on SoundNet. Below we review our work on each of the charges from the Faculty Senate. Rather than following the convention of discussing each of the standing charges laid out in the Faculty Bylaws, we (1) begin with the additional charge from the Senate, since this work has dominated the committee's work this year. (2) Next, we report our progress on the standing charges. (3) Finally, the committee looks ahead to some issues next year's committee might explore.

I. This year the Faculty Senate charged the LMIS Committee *"to work with Institutional Research and Technology Services to identify which of the existing data use policies concerning the appropriate use of institutional data on campus are most relevant to faculty, and develop and distribute informational resources to help faculty understand and comply with these policies."*

LMIS is forwarding the Faculty Senate a draft document entitled "Best Practices for Managing Sensitive Documents" (attached). The committee has devoted the majority of its meetings to drafting this document. To this end, committee members have brainstormed about the sorts of sensitive documents we encounter in our professional capacities, we have reviewed policies of other universities, and we have consulted with in-house experts (i.e., Jeremy Cucco, Kate Cohn, Michael Judd, Ann Gleason) to gain insight into legal and practical issues of data management. In brief, members of the LMIS committee recognize that faculty are sometimes inattentive to how we manage sensitive data, but we also conclude that faculty would be willing (and would want to) implement practices to avoid exposing information that might cause our students and colleagues embarrassment. The committee appreciates that university staff is working to minimize such exposure; for example, Technology Services has been systematically encrypting university-issued faculty computers, so that if they are lost or stolen, no one will be able to access sensitive information. The committee also recognizes, however, that faculty inevitably are privileged to (and retain) sensitive information in their professional capacity. We have embraced the Senate's charge to "develop a resource to faculty understand and comply with these policies."

The Faculty Senate's charge extends further, suggesting that LMIS *distribute* this resource. The committee respectfully suggests that, prior to distributing our working document, the Faculty Senate refer the draft to other entities for review. In particular, we think it would be useful to have the Professional Standards Committee review the recommendations for Faculty and Staff Documents and to have the Institutional Review Board review the recommendations for HIPAA protected Documents. We also recommend that the Senate consider referring the document to CHWS, CWLT, Data Standards, the Student Accommodations Office, Registrar, and HR for feedback. The LMIS committee recognizes that following such review, it may be appropriate to return the document to next year's LMIS for further review and to address some unresolved issues. For example, this year's LMIS committee members are not confident that we have adequately considered issues of creative products with multiple authors, such as recordings of live music and theatre performances, podcasts, written work and other products. Finally, LMIS recognizes that the finalized "Best Practices" document will continue to evolve and we suggest that LMIS be prompted to review this document periodically to make sure that it remains current.

The LMIS committee has spent some time thinking about how best to distribute the completed document. We offer the Senate several suggestions, including:

- An open forum in Wednesday at Four or other settings to solicit faculty feedback,
- Distributing the document to all faculty, perhaps through faculty.coms or via the department chairs meeting,
- Including the document in new faculty orientation,
- Directing the Faculty Advancement, Professional Standards, and Academic Standards Committees (as well as any other adjudicating committees) to consider how they currently handle confidential and sensitive documents and to provide feedback about our guidelines. They may want to develop committee guidelines that would be shared with new members about retention and disposal,
- Linking the document to the university's website, so that faculty will find and be able to use this document on line, and
- Asking Technology Services to offer working sessions to assist faculty in organizing and purging sensitive documents from their computers.

Given the effort that has gone into drafting this working document, this year's LMIS committee sincerely hopes that the document will, in time, be distributed to all faculty campus-wide. Having said that, the committee also would like to move on to other issues. We feel that we have given the Senate's charge our best effort and that the university will be best served if next year's LMIS is able to focus on other business.

II. The standing charges laid out in the Faculty Bylaws are:

- *To develop general policies, procedures and plans in collaboration with the Library Director and the Chief Technology Officer.*
- *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.*
- *To review periodically the mission and objectives of the library and information systems and to recommend such changes as are needed.*
- *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 2017-2018 academic year LMIS acted on these charges as follows.
On 9/22/2017 the committee met in the Maker Space in the library. At this session, librarian Jada Pelger and student employee Max Assael, provided a tour of the space to the committee. Library director Jane Carlin briefed the committee on the promise of the space as well as the challenges associated with staffing and funding the facility. On 12/1/2017 Lindsay Morris and Annie Cain (of Technology Services) presented the new myPugetSound pages, to illustrate the improved mobile experience and other updates. In December the committee also reviewed the library's self-study of trends associated with library use as well as budget and space concerns. On 3/20/2018 LMIS discussed the growing cost of interlibrary loan. Also on 3/20/2018 LMIS discussed the library's policy on challenged library materials. This discussion led to a broader conversation about the value of archival material, including material which today is recognized as objectionable (e.g., racist, sexist material). The committee visited the library archives on 5/1/2018 to see how the Collins Library staff preserves archival materials. On 5/1/2018 the committee discussed how the upcoming library and Technology Services reorganization would impact faculty and students.

III. Looking ahead

As described above, this year's LMIS has focused on drafting guidelines for handling sensitive data. The committee affirms that the collaboration between faculty, associate dean's office, technology services, and the library has been key to producing a working document that we think faculty will find useful. We are proud of our effort and of the product. But there has been a tradeoff. Notably, while faculty has been kept *informed* of changes initiated by the library and media and information services, the faculty have not had an active role in planning for such changes. Thus, we recommend that next year's LMIS committee return to its normal agenda. In particular, we would like to see the committee facilitate a broad discussion of "the role of the library, media and information systems in support of the academic program" and to "review periodically the mission and objectives of the library and information systems and to recommend such changes as are needed." [Language taken from standing charges to the LMIS committee.] We note an increasing move to integrate technology and information systems in the library space. This integration provides new opportunities but also involves losses, both of which will be felt by faculty and students. These changes merit further exploration, and LMIS seems like an appropriate venue for such conversation.

BEST PRACTICES FOR MANAGING SENSITIVE DOCUMENTS – DRAFT

INTRODUCTION

This document is intended to provide guidance in the management of confidential and potentially sensitive documents that faculty may 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 are not legally part of the student's official education record but nonetheless contain sensitive information about the student that could be embarrassing or cause harm if made public. 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), research or clinical materials, and service related documents from committees on and off campus.

CONTEXT

Questions about how long to retain these 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) continue to arise. At the request of the Faculty Senate, the LMIS Committee addressed this topic over the 2017-2018 year. As we reviewed existing documentation, current protocol and legal requirements, we recognized that document retention is a complex issue. This document seeks to provide recommendations and guidance for faculty in a practical manner. 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.

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 a faculty member's home directory: staffiles.pugetsound.edu/username. University-issued personal computers are relatively secure, if password protected and encrypted. Personal computers and electronic devices are generally less secure, and sensitive documents should not be stored on these devices. 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 cost associated with the long-term electronic storage of documents is non-trivial, and we encourage faculty and departments to develop practices that are 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 as a confidential document. Delete appropriate messages from folders and then empty the Deleted Items folder in Outlook. 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 Home Directory.

2. SoundNet: SoundNet (`https://soundnet.pugetsound.edu`) is recommended as a repository for confidential documents that might be associated with search committees. Technology Services can assist in setting up access to SoundNet for Committees, Teams, and Departments.

3. Network File Shares: Files on network file shares that are past their retention periods should be deleted from the file server. Once files are deleted from network file shares, they will be purged from the system and not included in future backups. The university keeps 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/`).

4. Home Directories : University data that is stored in home directories 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.

5. Local Hard Drives: University data should not be kept on users' local hard drives. If university data exists on these drives, it should be moved to the appropriate location on a network file share or deleted.

6. University Data: Contact Technology Services for assistance in eliminating all records that are past retention. Staff may be able to help set up automated mechanisms for review and/or elimination of records when retention periods are reached.

7. 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 the Home Directory, as the university incurs the cost of 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 SoundNet? Programs like Dropbox and Google Drive should be discouraged, especially in cases where projects are distinctly tied to the university, for reasons of licensing and data protection. If

- 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?

Recommended Document Storage Guidelines LMIS **Working Draft 6** May 1, 2018

Type of Document: Legally Protected	Level of Protection	Recommended Storage Options	Retention & Purge Recommendations	Resources for Further Info Web Links
FERPA Protected **Examples:** **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. **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	**Highly Confidential** Not shared without signed informed consent, and release. Release includes specified time frame, and purpose. Must conform to FERPA guidelines. **Retention and review of permissions and releases should be addressed at an administrative level and in departments and committees**	**Do Store In**: Digital documents should be stored on University Share Drive, or encrypted disk drive or encrypted computer 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, cell phone. Do not store on personal computer or laptop.	**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.	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 protocol is clarified. Community research samples are not covered by FERPA. Data from non-students should be handled in accordance with HIPAA.
HIPAA Protected Docs **Examples:** 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	**Highly Confidential** See above guidelines on release. **Must follow HIPAA Protocols for Processing and Storing Data**	**Do Process and Store HIPAA docs**: on encrypted drives, or within a 3rd party, HIPAA-certified solution (such as those now in use by the University, i.e. MyClientsPlus, WebPT, Jituzu, and Point-N-Click).	**Follow HIPAA guidelines for retention of Healthcare Data**	Professor Ann Wilson is the campus contact for HIPAA regulations.

also education or work-related accommodation info.), 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 (They are HIPAA Entities).		**Do Not Store or Process HIPAA docs:** No HIPAA documentation should ever be stored on the university shared drives. Do not process on non-encrypted drives or personal computers		
IRB Protected Documents **Examples:** All student and faculty research data governed by IRB protocols, including participant information collected during recruitment or participant selection procedures.	**Highly Confidential** See above guidelines on release. **Must follow IRB Protocols**	See "**DO Store In"** guideline above See "**DO NOT Store In**" guideline above.	**Follow IRB guidelines for retention of Healthcare Data**	**Contact Chair of Institutional Review Board and/or department or school representative**
Type of Document: Sensitive	**Level of Protection**	**Recommended Storage**	**Retention Time**	**Resources and Web Links**
Student Documents Letters of Recommendation, student papers and other academic related products, emails from students containing personal information or documents.	**Moderate Confidentiality** Shared with permission & limited usage. Permission specifies level of confidentiality, time frame of permission, and recommended storage guidelines.	May vary depending on the nature of the document and permissions received to distribute or share	**Recommended 3-5 year retention, with extension based on immediate or long-term needs** **Student Work retained for 1-2 years**	**Academic Standards Committee** **Dean of Students Office** **Professional Standards** **Individual Department Guidelines**

Faculty and Staff Professional Documents 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-High Confidentiality** Shared with permission & limited usage. Permission specifies level of confidentiality, time frame of permission, and recommended storage guidelines.	Letters of Evaluation and disciplinary actious should be treated with the highest level of confidentiality, stored in locked filing cabinets and encrypted drives.	**Recommended 3-5 year retention, with extension based on immediate or long-term needs**	**Professional Standards Committee** **Office of the University Provost**
Other Professional Documents (Outside University Roles) Examples-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** depending on the type of document, purpose, or organization. May be confidential.	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	**Recommended 3-5 year retention, with extension based on immediate or long-term needs**	**Professional Standards Committee** **Faculty may also consult with professional organizations or ethics committees for best practices and standards in their field.**
Personal materials belonging to faculty and staff such as financial information	**Varies depending on the type of document, and purpose.**	**Varies depending on the type of document, 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.	**Determined by Individual Faculty**	**Professional Standards and Tech Services Policies may need to clarify further.**
Materials of Interest to University Archives	Materials (proposals, brochures, photos, historical records, letters) associated with university	**DO:** Retain in original form if possible and contact librarian for guidance on sharing, storage, retention time, and	**Please consult with University Librarian or Archivist for guidance**.	**Contact Person: Jane Carlin, University Librarian** **Other Contacts: Library Archivist**

	traditions, events, initiatives, artistic and intellectual performances, student organizations, portfolios etc.	location.		**(Adriana Flores) or Assistant Archivist (Laura Edgar)**

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 also known as hard-drive encryption which 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.

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`.

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. **Home directory** – A home directory 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 and may be referred to by the letter the file share is mapped to, for example the “P” drive.

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.

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.