Faculty Senate Minutes
April 7, 2003

Senators Present: R. Wilson (presiding in place of Ostrom), D. Macey, Calla Ostrander (ASUPS representative), D. Tinsley, K. Porter, B. Haltom, T. Cooney, K. Bartanen, K. Hummel-Berry, J. Edgoose

The meeting was called to order at 4:09 pm.

The minutes from the March 10 meeting were approved as amended.

Special Orders

Calla Ostrander introduced herself as the new ASUPS representative to the Faculty Senate.

Cooney reported on efforts to prepare a useful staff organizational chart for the University. (This was a suggestion discussed at an earlier meeting.) He noted that it would be impossible to fit everyone on one page and still make it legible. Consequently, an online version is being developed that will have hyperlinks between major divisions.

Revisions to Privacy Policy

The following is a copy of the revisions to the Privacy Policy suggested by R. Wilson and A. Tullis. Suggestions for new language are indicated in italics; suggestions for deleting language are shown with strikethrough.

Privacy

Although University personnel (faculty, staff, and student staff) may expect a certain degree of privacy with respect to their desks, offices, lockers, machines, etc., all faculty, staff, and student staff should be aware of the limitations on the expectation of privacy. The University reserves the right to access University property such as lockers, desks, offices, cabinets, etc. All desk and filing cabinet keys, locker keys and combinations, etc., must be available to the University upon authorized request. The University may, for example, need to access business information in an individual's desk when he or she is away, and the University may access business information at any time ~~for business purposes~~. (Business information does not include data or documents that are part of faculty research materials unless those materials are derived from a faculty member's teaching, advising, or service within the University, *nor does it include patient or study subject records, files, or data*). The University should inform University personnel if and when such access will be, or has been, required. Personal information that University personnel want to be truly private should not be stored in University property (office, desk, locker, etc.).

Unauthorized University personnel should not request or use another individual's keys under any circumstances, nor should they attempt to gain access to another individual's office, desk, locker, etc., without permission. The unauthorized attempt to gain access to another's office, desk, locker, etc., is a serious breach of ethical conduct and will result in appropriate corrective action.

In cases of suspected possession of illegal or unauthorized drugs, alcoholic beverages, firearms, weapons or stolen property, the University reserves the right to search personal belongings on University property, including ~~but not limited to~~ articles of clothing, purses, briefcases, bags and vehicles. The search will ~~normally~~ be conducted in private by an appropriate supervisor, department head, or Security Services representative with a third person ~~normally~~ present. Although an individual, or an individual's personal property, will not be searched without consent under the circumstances described above, that individual's consent to such a search is required as a condition of employment, and refusal to consent will result in corrective action up to and including termination of employment under procedures specified by the Staff Policies and Procedures Manual and the Faculty Code. All such searches must be approved in advance by Human Resources in the case of staff, or the academic Vice President in the case of faculty.

Appropriate Use

The University of Puget Sound provides facilities, equipment, materials, information systems and other resources to support its academic programs and the administration of the University. ~~University personnel use University facilities, equipment, materials, and other resources to facilitate University business.~~ *All members of the University community have a general responsibility to use these resources civilly, lawfully, in accordance with University standards of conduct, and in support of the administrative and academic needs of the University* ~~Individuals are urged to exercise common sense and to use University resources in a manner consistent with the University's standards of conduct in the workplace. In general, University personnel should use University resources for University business only. In addition, the University's resources must not be used for activities that are illegal or contrary to University policy~~ (see the University's Information Use and Security Policy). Appropriate corrective action will be taken if an individual uses University resources in a manner inconsistent with the University's standards of conduct or other policies.   ???? *Suspected violations, in the case of a student, will be referred to the Dean of Students, for staff, to the Vice President for Finance and Administration and for faculty to the Professional Standards Committee.* Origination Date: 8/2002

Wilson highlighted the suggested changes and then asked for questions and comments.

Tinsley noted that the "consent to search" language (paragraph 3) was an area of concern to Haltom and others and wondered why it was still in the document. Wilson replied that they had consulted with Bruce Mann about this language and he noted that 1) the conditional clause at the beginning of the paragraph indicates that there must be some substantive suspicion of possession; 2) the remedy for refusing a search would not necessarily be termination of employment. Wilson noted that they were looking for suggestions about what to do here. Haltom suggested that we should highlight this portion of the document and ask for it to be looked at when it is discussed with Karen Goldstein.

Hummel-Berry suggested that the phrase indicating that the search will be conducted "with a third person normally present" should be changed to "with a witness present". The general consensus was that this was an improvement.

Haltom inquired about the italicized language under the Appropriate Use section. Wilson replied that this language had been taken from the language suggested by Hanson and Edgoose in their revision of the Information Use and Security Policy document.

Cooney noted that in the last sentence of the document "in the case of a student" wasn't parallel in construction to the rest of the sentence. In the same sentence, Cooney also noted that for faculty the grievance procedure doesn't necessarily start with the PSC and so the language should be changed to something like "for faculty, to the procedure outlined in the faculty code."

Haltom suggested that in the sentence that outlines the list of things that might be searched ("clothing, purses, briefcases, bags…."), we might want to add something more inclusive such as "or other containers". He also suggested that at the end of the third paragraph the phrase "Staff Policies and Procedures Manual **and** the Faculty Code" should be changed to "Staff Policies and Procedures Manual **or** the Faculty Code".

E-mail, Voice-mail, And Network Access Policy

The following is a copy of the revisions to the Privacy Policy suggested by D. Tinsley and K. Porter. Suggestions for new language are underlined; suggestions for deleting language are shown with strikethrough.

E-mail, Voice-mail, And Network Access Policy

This policy describes access to, and disclosure of, messages sent or received by University employees using the University's e-mail system, voice mail system, or network system. All members of the University community should be aware of expectations regarding proper use of University information and communication systems, as described in the University's "Information Use and Security Policy." (URL). ~~The University respects the individual privacy of its faculty and staff members. However, individual privacy does not extend to work-related conduct or to the use of University-provided equipment, services or supplies when it applies to legal issues or the violation of University policies.~~

The University's Right to Access Information

The electronic mail system, the voice mail system, and server and network systems ~~have been~~ were established by the University to facilitate mission-related communications. All e-mail and voice mail messages, computer and server files, and network use logs are University records and should be treated like other shared University filing systems. Therefore, employees should not assume that communications are confidential, even if the sender or the recipient so designates them. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

Although University students, faculty, and staff have individual passwords to access these systems and may expect a certain degree of privacy with respect to their use ~~of these systems, they~~ these systems belong to the University. The University ~~reserves the right to inspect those systems when necessary to uphold University policies or state or federal laws.~~ reserves the right to inspect University records for legal reasons or to ensure the wellbeing or security of the campus.

~~Any such communications should not be considered private even if the sender or the recipient so designates the communication. For example, despite the University's best attempts to provide security, hackers might be able to access e-mail for voice mail or to impersonate an e-mail or voice mail sender or network user. The University reserves the right to inspect University records for legal reasons or to ensure the wellbeing of the campus. The University's electronic mail, voice mail, and network and server systems should be treated like other shared University filing systems. Therefore, employees should not assume that messages are confidential.Back-up copies of e-mail may be maintained and referenced for business and legal reasons. All system passwords and encryption keys must be made available to the University's management upon authorized request.~~

Authorization Regarding this Policy

When in the course of business a supervisor requires access to an employee's computer files and the employee is not available, that employee should give password information to his/her supervisor. All system passwords and encryption keys must be made available to the University's management upon authorized request.

In cases requiring inspection of University records because of possible violation of University policies or state or federal laws, the authorities would be the Vice Presidents in each division of the University or, alternatively, the President. The University shall inform University personnel if and when such access will be, or has been, required. Personal information that University personnel want to be truly private, with the exception of medical or experimental research records ???? should not be stored in University property (office, deck, locker, etc).

Personal Use of E-mail, Voice Mail, and the Network

Because the University provides the electronic mail system, the voice mail system, and network access to assist University personnel with the performance of their jobs, these resources should

be used for such purposes. Incidental and occasional personal use of these resources is permitted by the University, but records of such use will be treated the same as other University records.

~~Misuse of these systems may result in corrective action up to and including termination under procedures specified by the Staff Policies and Procedures Manual and the Faculty Code.~~

University personnel should understand that deletions of messages and files do not fully prevent the messages and files from being recovered; that it is possible for third parties to intercept messages and files; and that messages and files may be disclosed to third parties (e.g., parties in civil litigation; law enforcement agencies in criminal investigations).

Unacceptable Use of E-mail, Voice Mail and Network Tools

University personnel may not use the University's e-mail, voice mail, or network systems in any way that is inconsistent with laws, regulations, and University policies ~~(see Information Use and Security Policy). University personnel are prohibited from the unauthorized use of others' passwords, access codes, and encryption keys to gain access to e-mail messages, voice mail messages, or network transmissions.~~ For examples of unacceptable use of communication and information systems, see Section 3 of the University's Information Use and Security Policy. (URL)

Copyright Awareness

Information posted by others on the network may be copyrighted. Information obtained through the network may be reproduced only by permission from the author or copyright holder unless the user is aware that the material is free of copyright.

The Consequences of Unacceptable Use

Unacceptable use of University electronic communication systems is a serious breach of ethical conduct and will result in corrective action up to and including termination of employment under procedures specified by the Staff Policies and Procedures Manual and the Faculty Code.

~~**Copyright Awareness**~~

~~Information posted by others on the network may be copyrighted. Information obtained through the network may be reproduced only by permission from the author or copyright holder unless the user is aware that the material is free of copyright.~~

Origination Date: 8/2002

Owner: President's Cabinet
Contact: Assistant to the President/Secretary of the Corporation
Revision Date: 4/2003
Renters: Karen Porter and David Tinsley
Contact: Hans Ostrom, Chair for Life of the Faculty Senate

Tinsley reported that the main problem with this document is its redundancy. In revising the document he and Porter took advantage of some of the revisions suggested by Hanson and Edgoose to the Information Use and Privacy document. In the Information Use and Privacy document there is a list of inappropriate uses of systems so it wasn't necessary to repeat that here. Tinsley briefly outlined the suggested changes and the rationale for them.

Hanson wondered whether it was necessary to have a separate E-mail, Voice-mail, and Network Access Policy document since many of these issues overlap with those in the Information Use and Security Policy document. Tinsley replied that it might not be necessary to have a separate document, but it does serve a useful informational purpose. Haltom argued that it seemed logical to include this information under the more capacious document, but that as a separate document it might better alert colleagues that there is no guarantee of privacy in email. In the end Haltom concluded that fewer documents would be better and suggested that we propose combining the two documents to Karen Goldstein.

Haltom also noted that under "The Consequences of Unacceptable Use" section, the wording "…procedures specified by the Staff Policies and Procedures Manual **and** the Faculty Code" should be changed to "…procedures specified by the Staff Policies and Procedures Manual **or** the Faculty Code."

Haltom then expressed his belief that many of the problems that these documents are trying to address could be dealt with more informally by the University community rather than being raised to the level of formal procedures and policies.

Bartanen remarked that most of the time this is probably true, but she could think of at least 3 times or so in the last year that threatening emails were being sent that required OIS to go in and investigate who was sending them, so a formal policy that articulates the right of the University to do this is important.

Ostrander and Bartanen both remarked on the importance of the policies in informing members of the University community about acceptable behavior and the fact that email is not truly private.

Edgoose and Wilson seconded Haltom's interest in promoting informal methods for trying to resolve matters before escalating to more formal rigid procedures and wondered how best to do this.

Edgoose wondered about the official status of these documents, and in what context they appear. Bartanen replied that on the Human Resources website there is a section on University Policies where most of these appear. She also noted that Gale Hunter is charged with creating a process for developing and amending policies.

Haltom argued that just slapping a policy up on a website is not a good process for implementing new policy. He encouraged the new president to involve Faculty, Students, and Staff in the development of new policies that affect them.

The general consensus of the senate was to recommend that the faculty senate chair (Ostrom) informally talk with the incoming president, encouraging him to involve faculty, students, and staff in developing policies that affect them.

After the departure of a couple senators for other appointments we no longer had a quorum, so Wilson adjourned the meeting around 5 pm.

Submitted by,

John Hanson