***DRAFT***

**Minutes of the Faculty Senate**
**17 February 2003**

**Senators present—**Kris Bartanen, Terry Cooney, Julian Edgoose, Bill Haltom, Kathie Hummel-Berry, Christine Kline, Juli McGruder, Hans Ostrom (Chair), Curt Sanders, David Tinsley, Alexa Tullis, Roberta Wilson

**Visitors present—** Karen Goldstein, David Macey, Bob Matthews, Jason Ronbeck, Theodore Taranovski

**Agenda Item #1** **Minutes of 27 January 2003 Meeting** approved without change

**Agenda Item #2** **Special Orders —Sanders** informed faculty that we are now in the midst of the ASUPS election campaign. He also told us that the "Conspiracy of Hope" week raised $1000.

**Agenda Item #3** **Review polished resolution (passed on January 27) concerning benefits for domestic partners—Ostrom** circulated David Macey's revised motion and rationale for senators to review. **Bartanen** and **Kline** expressed their appreciation of the values based arguments in the documents but hoped that the economic rationale would also be included. **Ostrom** assured them that both documents would be forwarded to the Trustees.

**Begin Embedded Document**

**Resolution on Educational Benefits**
University of Puget Sound Faculty Senate
January 27, 2003

Resolution (M/S/P):

1. The Faculty Senate declares its support for the extension of educational benefits to the same-sex domestic partners of full-time faculty and staff members and to same-sex domestic partners' dependent children who live permanently in a full-time faculty or staff member's home.

2. The Faculty Senate requests that the Board of Trustees take appropriate action to provide educational benefits to the same-sex domestic partners of full-time University employees and to same-sex domestic partners' dependent children who live permanently in a full-time faculty or staff member's home.

Background:

1. The University of Puget Sound's Equal Opportunity Policy states that the University "does not discriminate in education or employment on the basis of sex, race, color, national origin, religion, creed, age, disability, *marital or familial status*, *sexual orientation*, Vietnam-era veteran status, gender identity, or any other basis prohibited by local, state, or federal laws" (emphasis added).

2. The University of Puget Sound Education Benefits Policy for Spouses and Dependent Children provides tuition scholarships to spouses and dependent children of full-time faculty and staff members.
    a. Under this policy, "a spouse is defined as one to whom a faculty or staff member is *legally married*" (emphasis added), while a dependent child is defined as "one who is claimed as a dependent child on the faculty or staff member's previous year's income tax return and who is the faculty or staff member's natural or adoptive child or a stepchild living permanently in the faculty or staff member's home."
    b. Same-sex domestic partners, who are legally unable to marry, are ineligible for this benefit.
    c. Dependent children by other partners whom same-sex partners bring into domestic partnerships with full-time faculty or staff members are also ineligible for this benefit unless those children are legally adopted by the full-time faculty or staff member, whereas dependent children by other partners whom married opposite-sex partners bring into domestic partnerships are eligible for this benefit because their parents are married to full-time faculty or staff members.

Rationale:

1. Restricting eligibility for educational benefits to legally married spouses and their children is a form of discrimination based on marital status and on sexual orientation.
    a. Tuition scholarships for spouses and their dependent children are part of a valuable package of benefits associated with employment at the University of Puget Sound, but they are extended only to specific category of employee (those who are legally married) and are denied to other employees whose domestic partnerships cannot be legally recognized as marriages in the State of Washington.

2. The University of Puget Sound seeks to "liberate each person's fullest intellectual and human potential to assist in the unfolding of creative and useful lives." To this end, the University offers a variety of programs and supports a vibrant campus culture that nourish the personal as well as the professional lives of its students, staff, and faculty.
    a. The same-sex domestic partners of full-time faculty and staff members and their dependent children are members of the extended University community and stand in the same relationship to the University as do their legally married counterparts and their dependent children.
    b. Denying educational benefits to the same-sex domestic partners of full-time faculty and staff members and to their dependent children places a severe constraint on their ability to realize their fullest intellectual and human potential.

3. This form of discrimination has a variety of deleterious consequences for the entire Puget Sound community.
    a. Discrimination in the provision of educational benefits for spouses and dependent children is inconsistent with the University's Equal Opportunity Policy.
    b. It implies that the University attaches less value to the domestic partnerships and families of its lesbian and gay employees.
    c. It places a significant financial burden on faculty and staff members whose same-sex domestic partners and their dependent children choose to pursue studies at the University of Puget Sound.
    d. It is disheartening to lesbian and gay faculty and staff members and their domestic partners and dependent children, and this has significant implications for the recruitment and retention of faculty and staff members.
    e. It sends the wrong message to students, alumni, and the wider community about the University's attitude toward its lesbian and gay faculty and staff members and their domestic partners and dependent children.

**End Embedded Document**

**Agenda Item #4 Discussion of "Privacy Documents" and "Weapons Policy"**— **Ostrom** asked it to be noted that Karen Porter had a job candidate talk so she could not attend, and that the members of the Professional Standards Committee also had other engagements and could not attend this discussion.

**Ostrom** suggested this discussion be focused on information gathering. A copy of the policies was circulated (see below). **Tinsley** expressed his interest in understanding the motivations for this policy and why we need it now. **Haltom** echoed the sense that we should hear information now and argue later. **Ostrom** summarized the parts of the policy as

- The Non-Disclosure and Confidentiality Agreement
- Email, Voice-mail, And Network Access Policy
- Information Use and Security Policy
- Privacy and Appropriate Use of Resources
- Weapons Policy

**Begin Embedded Document**

**University of Puget Sound**

**Non-Disclosure and Confidentiality Agreement**

I recognize and acknowledge that during the course of my employment with the University, I will have access to certain information not generally known to the public relating to the University, its operations and business. I agree that this information is "Confidential Information" that belongs to the University.

I understand that "Confidential Information" includes, without limitation, any information in whatever form that the University considers to be confidential, proprietary information relating to the University. For example, Confidential Information includes information relating to the University's databases; inventions; software (including source code and object code); procedures; purchasing; accounting; marketing and marketing plans; students; donors; trustees; licensees; suppliers; financial status; contracts or employees. Confidential Information includes information developed by me, alone or with others, or entrusted to the University by its students, donors, trustees or others.

I agree to hold the University's Confidential Information in strict confidence, both during my employment and thereafter, and not disclose or use it at any time except as authorized by the University and for the University's benefit. My agreement to protect the University's Confidential Information applies both while I am employed by the University and after my employment with the University ends, regardless of the reason it ends.

_____

Signature

_____

Name (printed)

_____

Department

_____

Date

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

Telephones, computers, and electronic information are essential tools for University personnel (faculty, staff and student staff) to use to perform their jobs in support of the mission of the University. Each faculty and staff member can help to ensure that these tools are used for job-related purposes in a manner that preserves confidential information. Incidental and occasional personal use of these tools is permitted, as long as the use does not detract from job performance or productivity and as long as the use conforms to other provisions of this policy and other relevant University policies.

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. 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 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. 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 belong to the University, and the University reserves the right to inspect those systems when necessary to uphold University policies or state or federal laws.

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. 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.

**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. In any event, University personnel should not use these systems for such purposes as soliciting or proselytizing for commercial ventures, religious or personal causes or outside organizations or other similar, non-job-related solicitations. 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. 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.

**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.

## *Information Use and Security Policy*

### *Expectations for All Members of the University Community*

The University of Puget Sound has an interest in providing campus telephones and telephone systems, voice mail, campus computers, servers and network systems, and electronic mail primarily to support its academic programs and the administration of the University. This interest implies some responsibilities and constraints for members of the University community. The University provides appropriate access to these systems to all matriculating students, to faculty and staff, to emeritus faculty members, and to those holding special faculty appointments. All members of the University community—students and employees (faculty, staff, and students)—have a general responsibility to use these resources civilly, lawfully, and in accordance with University standards of conduct.

Inappropriate use of University electronic communication resources (telephones, voice mail, computers, servers, electronic mail, network systems) include but are not limited to:

- Disseminating confidential or proprietary information to any unauthorized person
- Sharing access to University systems or information with any unauthorized person
- Charging someone for use of the resources assigned to a student or employee
- Harassing, threatening, defaming, or otherwise interfering with the legal rights of others
- Violating standard citation requirements or using/copying copyrighted software or other copyrighted material in violation of the copyright agreement
- Gaining unauthorized access to other systems
- Disrupting service intentionally
- Introducing or knowingly spreading viruses or destructive programs
- Sending chain-letters
- Sending unauthorized blanket e-mail messages
- Consuming inordinately large amounts of system resources knowingly.

Other policy statements that are incorporated by this reference in the Information Use and Security Policy are:

- Academic Honesty Policy
- Sexual Harassment Policy
- Political Activity Policy
- E-mail, Voice-mail and Internet Use Policy
- Privacy and Appropriate Use of Resources Policy
- Solicitation Policy
- Education Records Policy

### *Security and Use Objectives and Scope for University Personnel*

The importance of maintaining the integrity of Puget Sound's information resources cannot be overstated. The University's objectives in managing information resources properly are (1) to permit effective planning and decision-making, (2) to conduct University business in a timely and effective manner, and (3) most importantly, to insure that confidential data are handled appropriately. Each faculty member, staff member, student staff member and contractor with access to institutional information resources is responsible for knowing and complying with Puget Sound's information use and security policies. Supervisors and managers are responsible for regularly training the University personnel and contractors in their areas of responsibility regarding the proper application of the information use and security policies.

Information resources include data maintained by the University, whether centralized or decentralized, regardless of the medium. Information resources media include but are not limited to electronic communication (electronic mail, telephone, voice mail, fax, network communications, etc.) and other University information resources (databases, computer files and directories, written information, spoken information, etc.)

***Confidential Information***

"Confidential Information" includes, without limitation, any information in whatever form that the University considers to be confidential, proprietary information relating to the University. For example, Confidential Information includes information relating to the University's databases, inventions, software (including source code and object code), procedures, purchasing, accounting, marketing and marketing plans, employees, students, donors, trustees, licensees, suppliers, financial status, or contracts. Confidential Information includes information developed by University personnel, alone or with others, or entrusted to the University by its students, donors, trustees or others.

Department heads are responsible for determining and communicating what information is confidential to the University personnel and contractors in their areas of responsibility. Department heads are also responsible for determining who in their areas of responsibility has a need to know confidential information and for authorizing access to those individuals. When department heads grant access to confidential information to University personnel and contractors, both the department head and the individual or company will sign a non-disclosure and confidentiality agreement to insure that University personnel and contractors have a clear understanding of their roles and responsibilities. Users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to the University's systems and information. Finally, department heads are responsible for ensuring that University personnel and contractors are trained in the proper use of information systems.

The Office of Information Services (OIS) is responsible for supporting department heads in managing access to data maintained electronically and for standardizing and streamlining account administration across multiple information technology systems. OIS support includes prompting department heads to review users' access rights regularly to ensure that access rights are consistent with employees' job responsibilities.

## Sanctions for Policy Violations

Failure to comply with the University's information use and security policies may result in the denial of access to campus information services and/or in sanctions as provided in the University Integrity Code, the Faculty Code, or the Staff Policies and Procedures Manual, up to and including termination of employment or permanent expulsion.

**Privacy and Appropriate Use of Resources**

***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 information in an individual's desk when he or she is away. The University may access information at any time for business purposes. 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***

University personnel use University facilities, equipment, materials, and other resources to facilitate University business. 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.

**Date:** November 25, 2002

**To:** Faculty Senate

**From:** Professional Standards Committee

**Subject:** Report on the Four Written Policies

## Faculty Senate Charge on the "four written policies"

Consider whether the four new written policies on confidentiality, so-called "political statements" appearing on email, distribution of information, and security of information threaten the academic freedom guaranteed by the Faculty. Determine the extent to which these policies have been implemented. Recommend appropriate responses and or actions, if any, to the Faculty Senate. (These policies, apparently drafted by Karen Goldstein, were presented to the PSC in draft-form last year.) **The Senate considers this charge to be of the highest priority.**

## The four documents in question

1. Privacy and Appropriate Use of Resources

2. Information and Use Security Policy

3. E-mail, Voice Mail, and Network Access Policy

4. University of Puget Sound Non-Disclosure and Confidentiality Agreement**.**

In the following discussion, these four documents will be referenced by the relevant underlined terms: "Privacy," "Information," "E-mail," and "Confidentiality."

The PSC has thoroughly examined all four of the documents and discussed each of them in detail. The results of the committee's deliberation are contained in the following report. We have two general remarks that apply to all four of the documents, as well as a few more specific comments about each one individually. Regarding the question of implementation, we were informed that all four of the documents have in fact been implemented as policy. In the particular case of the Confidentiality document, the committee was unable to determine who will be required to sign the agreement

The first general conclusion is that we did not find any of the four documents to be in direct violation of academic freedom as specified by the Faculty Code (Ch.1, part D). Nor did we find that the documents violated anything specified under "Relations with the University" (Ch. 1, part B, Section 4) or "Professors as Citizens" (Ch. 1, Part B, Section 5). As will be clear from the rest of this report, the committee did not find these documents to be entirely unproblematic – they definitely raised a number of issues and concerns – but we did not find any direct conflict with the Faculty Code.

Second, we would like to note that all four of the document raise legal issues that are beyond the committee's area of expertise. Is it clearly the case that because the University owns the desks, computers, lockers, and e-mail systems it can reserve the right to "access information at any time for business purposes" (1st paragraph of Privacy document)? Is it the case that because the University owns the telephone and computer system it can specify what constitutes appropriate and inappropriate use of these systems (Information document)? Is it the case that because the telephones, computers, and electronic information systems "belong to the University" the

University can "inspect those systems when necessary to uphold University policies or state and federal laws" (3rd paragraph of E-mail document)? These are very interesting and important questions; they are also questions that the PSC cannot answer. Undoubtedly there are various contexts in which all of these questions would be answered affirmatively, but the details of when, why, and under what circumstances that would be the case clearly involves legal issues that are beyond the scope, knowledge, or jurisdiction of the PSC. We too would like to know which of these statements are in fact unconditionally "the law," and which are the law only under certain conditions (and what those conditions are). For this reason the committee would suggest that if the Senate shares these concerns and has similar questions, it should seek the advise of legal counsel. The PSC can interpret the Faculty Code, not delineate legal rights, obligations and responsibilities.

In addition to these two main recommendations, the committee also believes that there are a number of ways in which these documents could be improved by making various revisions – some minor, some not so minor – and these suggested revisions are outlined below. Since the types of changes, and the motivations for those changes, vary greatly among the four documents, each will be discussed individually. The committee realizes that it does not have any official right or responsibility to make recommendations about the specific wording of these documents, nonetheless the PSC was charged with recommending "appropriate responses and or actions," and we consider recommending ways that the documents might be improved in the interest of clarity, coherence, or perhaps even just in sounding a bit less authoritarian, to be one such appropriate response.

**1. Privacy**

The committee's suggested changes for the Priority document are shown below. The original document has been modified to reflect the desired changes with underlining used for additions and ~~strikeout~~ used for words to be removed. The only substantive revisions to this document are contained in the middle of the first paragraph: rewording the way that "business" appears and adding the parenthetical remark to make it clear that business information is distinct from faculty research.

***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.)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***

University personnel use University facilities, equipment, materials, and other resources to facilitate University business. 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. Origination Date: 8/2002

**2. <u>Information</u>**

The first (and minor) suggested changes to the Information document involve clarification of various bulleted items: the parenthetical additions to the prohibition on "chain letters" and a clarification about the problem of "consuming inordinately large amounts of system resources." The second, and more substantial, change involves modifying the section on "confidential information" so that it reflects existing and suggested changes in the Confidentiality document (discussed below under #4). The second paragraph under Confidential Information is also changed to help clarify the responsibilities of University personnel regarding network connections.

***Information Use and Security Policy***
***Expectations for All Members of the University Community***

The University of Puget Sound has an interest in providing campus telephones and telephone systems, voice mail, campus computers, servers and network systems, and electronic mail primarily to support its academic programs and the administration of the University. This interest implies some responsibilities and constraints for members of the University community. The University provides appropriate access to these systems to all matriculating students, to faculty and staff, to emeritus faculty members, and to those holding special faculty appointments. All members of the University community—students and employees (faculty, staff, and students)—have a general responsibility to use these resources civilly, lawfully, and in accordance with University standards of conduct.

Inappropriate use of University electronic communication resources (telephones, voice mail, computers, servers, electronic mail, network systems) include but are not limited to:

· Disseminating confidential or proprietary information to any unauthorized person

· Sharing access to University systems or information with any unauthorized person

· Charging someone for use of the resources assigned to a student or employee

· Harassing, threatening, defaming, or otherwise interfering with the legal rights of others

· Violating standard citation requirements or using/copying copyrighted software or other copyrighted material in violation of the copyright agreement

· Gaining unauthorized access to other systems

· Disrupting service intentionally

· Introducing or knowingly spreading viruses or destructive programs

· Sending chain-letters. (Chain letters are understood to be messages that ask the recipient to send the message again to multiple new recipients in a structured pattern that through repetition seeks ever-wider diffusion. Messages that may ask managers, faculty, or staff to share messages with others for purposes of University business are not considered chain letters.)

· Sending unauthorized blanket e-mail messages

· Maliciously or knowingly consuming inordinately large amounts of system resources ~~knowingly~~ for non-academic purposes.

Other policy statements that are incorporated by this reference in the Information Use and Security Policy are:

· Academic Honesty Policy

· Sexual Harassment Policy

· Political Activity Policy

· E-mail, Voice-mail and Internet Use Policy

· Privacy and Appropriate Use of Resources Policy

· Solicitation Policy

· Education Records Policy

**Security and Use Objectives and Scope for University Personnel**

The importance of maintaining the integrity of Puget Sound's information resources cannot be overstated. The University's objectives in managing information resources properly are (1) to permit effective planning and decision-making, (2) to conduct University business in a timely and effective manner, and (3) most importantly, to insure that confidential data are handled appropriately. Each faculty member, staff member, student staff member and contractor with access to institutional information resources is responsible for knowing and complying with Puget Sound's information use and security policies. Supervisors and managers are responsible for regularly training the University personnel and contractors in their areas of responsibility regarding the proper application of the information use and security policies.

Information resources include data maintained by the University, whether centralized or decentralized, regardless of the medium. Information resources media include but are not limited to electronic communication (electronic mail, telephone, voice mail, fax, network communications, etc.) and other University information resources (databases, computer files and directories, written information, spoken information, etc.)

**Confidential Information**

~~"Confidential Information" includes, without limitation, any information in whatever form that the University considers to be confidential, proprietary information relating to the University. For~~

~~example, Confidential Information includes information relating to the University's databases, inventions, software (including source code and object code), procedures, purchasing, accounting, marketing and marketing plans, employees, students, donors, trustees, licensees, suppliers, financial status, or contracts. Confidential Information includes information developed by University personnel, alone or with others, or entrusted to the University by its students, donors, trustees or others.~~

"Confidential information" may include any information, in whatever form, that the University states through its officers, policies, and publications to be confidential or proprietary information relating to the University. Confidential information includes but is not limited to information relating to the University's databases, inventions, software (including source code and object code), business procedures, purchasing, accounting, marketing and marketing plans, licensees, and contracts. It includes information about the University's financial status other than that published in the annual financial report. Information about individuals associated with the University as students, employees, donors, trustees, parents, alumni, parties to agreements, or business associates will be considered confidential except as provided for in policies covering student and employee information, as made general knowledge through University publications, or as allowed with the consent of those concerned. Confidential information may include business information developed by University personnel, alone or with others, or information entrusted to the University by its students, employees, constituents, or associates.

Department heads are responsible for determining and communicating what information is confidential to the University personnel and contractors in their areas of responsibility. Department heads are also responsible for determining who in their areas of responsibility has a need to know confidential information and for authorizing access to those individuals. When department heads grant access to confidential information to University personnel and contractors, both the department head and the individual or company will sign a non-disclosure and confidentiality agreement to insure that University personnel and contractors have a clear understanding of their roles and responsibilities. Users may not intentionally establish Internet or other external network connections that could allow unauthorized persons to gain access to the University's systems and information and should exercise due care in all such connections. Finally, department heads are responsible for ensuring that University personnel and contractors are trained in the proper use of information systems.

The Office of Information Services (OIS) is responsible for supporting department heads in managing access to data maintained electronically and for standardizing and streamlining account administration across multiple information technology systems. OIS support includes prompting department heads to review users' access rights regularly to ensure that access rights are consistent with employees' job responsibilities.

**Sanctions for Policy Violations**

Failure to comply with the University's information use and security policies may result in the denial of access to campus information services and/or in sanctions as provided in the University Integrity Code, the Faculty Code, or the Staff Policies and Procedures Manual, up to and including termination of employment or permanent expulsion.

Origination Date: 8/2002

**3. E-mail**

The committee has a few typo and wording changes for the e-mail document, but the most significant change is the addition of the final sentence in the section on Authorization.

***E-mail, Voice-mail, and Network Access Policy***

Telephones, computers, and electronic information are essential tools for University personnel (faculty, staff and student staff) to use to perform their jobs in support of the mission of the

University. Each faculty and staff member can help to ensure that these tools are used for job-related purposes in a manner that preserves confidential information. Incidental and occasional personal use of these tools is permitted, as long as the use does not detract from job performance or productivity and as long as the use conforms to other provisions of this policy and other relevant University policies.

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. 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 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. 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 belong to the University, and the University reserves the right to inspect those systems when necessary to uphold University policies or state or federal laws.

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 or 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 or security 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. 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 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.).

**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, and 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. In any event, University personnel should not use these systems for such purposes as soliciting or proselytizing for commercial ventures, religious or personal causes or outside organizations or other similar, non-job-related solicitations. 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. 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.

**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

**4. Confidentiality**

This was clearly the document that raised the most concerns among the members of the PSC. This said, it is also useful to point out that the committee reviewed an earlier draft of the confidentiality document (4/18/02) and made a number of recommendations regarding ways that it could be improved, and that all of these suggestions were integrated into the existing document. The PSC's response to the original document is attached below as #5. Even though the original PSC memo is attached, it is useful to review these earlier recommendations and emphasize the role they play in the current version of the confidentiality document. The committee actually made five recommendations, but the following three seem to be the most important.

First, the original draft defined confidential information to be any information the University "considers" to be confidential. The committee found this wording to be "unclear about its range of application, its definitions, and its intent" and allowed for retrospective designation of the confidentiality status, in a way that was at best rather vague, and at worst dangerously arbitrary. As a result of the committee's recommendation, the current confidentiality document specifies that "confidential information" is information that the University "states through its officers, policies, and publications to be confidential." This is more clear and helps to prevent retrospective designation.

Second, the committee wanted a statement that made it clear that "the policy was not intended to restrict discussion among University employees of their working conditions, exchanges about issues in the campus community, or other conversations between employees inside or outside the campus community about general issues or concerns." A version of the committee's statement has been added; it is now the final paragraph.

Finally, the PSC requested that a statement be included "indicating that any determination of a violation or handling of a breach would occur within the established contexts for addressing student, staff, or faculty performance issue." The last sentence of the third paragraph of the current document makes a clear statement to this effect.

Despite the fact that all of the PSC's earlier recommendations were integrated into the confidentiality document – and it is important to emphasize how significant these changes were – the committee still has one more small suggestion. The last sentence of the second paragraph should have the word "business" inserted before the second instance of "information." The sentence should read: "Confidential information may include business information developed by me, alone or with others, or information entrusted to the University by its students, employees, constituents, or associates." This is to make it clear that that the information that may be developed "by me" does not include a faculty member's research or related materials. This word has been added to the version of the Confidentiality Agreement at the end of this section.

Although the committee has just this one small additional change to the Confidentiality document, it is important to note that the document raised a number of significant questions and concerns. Members of the committee were frankly not certain who could/would be in a position to address any or all of these issues, but also felt that it would be useful for the Senate to be aware of the various concerns that emerged during the committee's deliberations.

One concern involved the question of who constitutes an "officer" in the first sentence of the second paragraph: "any information, in whatever form, that the University states through its officers, policies and publications to be confidential." Stating through written policies and publications is pretty straightforward, but "officers" is certainly less so. Does one officer of the University stating something is confidential make it so, even if the majority of others do not agree? There is also the question of departmental chairs. Are departmental chairs "officers of the University" for the purpose of deciding what is and is not confidential? A "yes" answer to this last question would raise a number of additional concerns.

A second issue involved confidential material that has entered the public domain. Is a faculty member still tied to the confidentiality agreement when the relevant confidential information is in the public domain and clearly no longer confidential? Can one talk about "confidential information" after one reads it in the newspaper?

A third concern raised by various Committee members involved the question of ethical dilemmas. What if a faculty member must choose between the confidentiality agreement and moral responsibilities to others? The question of responsibility to students versus the confidentiality agreement was raised explicitly, but it is fairly easy to think of others.

Although these three issues do not exhaust the concerns that emerged during the Committee's deliberations, they seem to be the most important: the three that generated the most discussion, uncertainty and consternation. Again, the Committee realizes that there are no obvious and easy answers or solutions these concerns. Nonetheless they are serious matters that were raised by multiple committee members, and the Committee felt that the Senate should be aware of them.

**University of Puget Sound Non-Disclosure and Confidentiality Agreement**

I recognize and acknowledge that during the course of my employment with the University of Puget Sound, I will have access to certain information not generally known to the public relating to the University, its students and employees, and its operations and business. I agree that this information is "confidential information" that belongs to the University or is protected by law.

I understand that "confidential information" may include any information, in whatever form, that the University states through its officers, policies, and publications to be confidential or proprietary information relating to the University. Confidential information includes but is not limited to information relating to the University's databases, inventions, software (including source code and object code), business procedures, purchasing, accounting, marketing and marketing plans, licensees, and contracts. It includes information about the University's financial status other than that published in the annual financial report. Information about individuals associated with the University as students, employees, donors, trustees, parents, alumni, parties to agreements, or

business associates will be considered confidential except as provided for in policies covering student and employee information, as made general knowledge through University publications, or as allowed with the consent of those concerned. Confidential information may include business information developed by me, alone or with others, or information entrusted to the University by its students, employees, constituents, or associates.

I agree to hold the University's confidential information in strict confidence and not to disclose such information outside the University. I agree to treat confidential information with care during my employment with the University, using it in ways consistent with good operating practices, established policies, or instructions from the officers of the University. My agreement to protect the University's confidential information applies both while I am employed by the University and after my employment with the University ends, regardless of the reason it ends. Determination of violations of this agreement and of sanctions for any violations will be handled through the procedures provided in the Faculty Code, the Staff Policies and Procedures Manual, or the Student Integrity Code, depending on whether the person charged with a breach of the agreement is a member of the faculty, staff, or student body, respectively.

Nothing in this document is intended to restrict discussion within the University of campus issues, policies, or conditions so long as that discussion does not reveal confidential information to parties who would not normally have access to such information. This agreement also does not restrict discussion between members of the campus community and the public about issues of mutual concern so long as confidential information is not a part of such discussion.

Signed by:

_____
Signature of staff member, faculty member, or student staff member

_____
Name (printed)

_____
Department

_____
Date

Countersigned by:

_____
Signature of Department Head

_____
Name (printed)

_____
Date

**5. Statement of PSC objections to original disclosure document:**

The Professional Standards Committee, in its meeting of April 18th 2002, discussed the proposed "Non-Disclosure and Confidentiality Agreement" and makes the following observations.

1. The document appears to committee members to be unclear about its range of application, its definitions, and its intent. Members did not understand the capitalization

of Confidential Information, which seemed to imply a specifically defined category or suggest some special meaning not evident in the document. Faculty suggested that confidential information, in a context such as this statement, should be defined in part by concrete example (such as the Cascade data bases). They also believed that confidential information must be better defined at the point of stating the policy rather than retrospectively (*i.e*, not information the University "consider to be confidential" as determined after the fact).

2. In keeping with the first concern, committee members suggested that the phrase "includes, without limitation, any information in whatever form that the University considers to be confidential," is too sweeping and provides no practical guidance. Because information about suppliers is mentioned later in the statement, a committee member noted that if a science staff member from another institution called a science department and asked, where do you buy your [any specific chemical or biological lab supplies], staff and faculty here would expect to be able to answer and could see no issue of confidentiality. Committee members thus suggested as substitute wording for the sentence in question, confidential information "may include any information in whatever form the University states to be confidential."

3. Committee members believed it was important to identify who would decide what information is considered confidential. The "University" is not an actor in this case but the equivalent of the "government"—ambiguous as to persons or processes.

4. Faculty believed it was important to make clear that the policy was not intended to restrict discussion among University employees of their working conditions, exchanges about issues in the campus community, or other conversations between employees inside or outside the campus community about general issues or concerns. The committee would like to see a statement to this effect added to the agreement.

5. The committee would like to see included in the agreement a statement indicating that any determination of a violation or handling of a breach would occur within the established contexts for addressing student, staff, or faculty performance issues. For example, the committee notes the following sentence in the University's Sexual Harassment Policy meeting the same objective: "Complaints may be handled informally as described below or by means of the formal procedures as provided by the Faculty Code, the Staff Policies and Procedures Manual, or the Student Integrity Code, depending on whether the person charged is a member of the faculty, staff, or student body, respectively."

**Date:** December 4, 2002

**To:** Faculty Senate

**From:** Professional Standards Committee

**Subject:** Additional questions on 4 Policies

The **PSC** responded to the Senate's charge regarding the "4 Written Policies" with a detailed memo dated November 25, 2002. In response, we received an e-mail from the Chair of the Faculty Senate containing the following five additional questions:

> 1. Given the Committee's substantial concerns about the Confidentiality document, would the Committee recommend that faculty members sign or not sign the agreement (in its current unamended form) if they were asked to do so? This need not be a formal recommendation based on an interpretation of the Faculty Code; even a "straw poll" of faculty members who sit on the committee would, I believe, be useful to the Senate. **No faculty member has studied these documents more than colleagues who sit on the PSC; therefore, the Senate would benefit from a sense of how many colleagues on the PSC would sign the document--as it is now written.**
>
> 2. A related question: How many colleagues on the PSC would sign the Confidentiality Agreement if it incorporated revisions suggested by the PSC? Again, senators would, I think, be interested in an informal straw poll, not a formal recommendation.
>
> 3. In its deliberations, did the PSC discover any other instances in the University's history when all members of the faculty were asked to sign an agreement unrelated to annual contracts? In the view of the PSC, to what extent would the situation, in itself, of being asked and/or required to sign the Confidentiality Agreement affect the faculty's ability to "maintain a superior academic climate" (By Laws, Article II, section 2)?
>
> 4. Does the PSC know whether the University would have the authority to fire a member of the faculty if that person, upon being asked to sign the Confidentiality agreement, declined to do so?
>
> 5. Does the PSC know whether the administration is planning to ask the faculty to sign the Confidentiality agreement (in any form--amended or unamended)? If so, what are those plans?

Some members of the PSC questioned the appropriateness of responding to these questions. After deliberation it was decided that the PSC would respond informally to as many of the questions as the members of the committee, as a committee, felt comfortable and qualified in answering.

1 & 2. The committee concluded that the issue of whether an individual faculty member would sign the Confidentiality Agreement (either the original or the revised version) was a personal matter that was outside the role of the PSC. A straw poll of the individual members of the committee on this matter thus seemed to be inappropriate. We made it clear in our response to the Senate that we did not find any conflict with the Faculty Code, but we also stated that it would

be useful for the Senate to obtain some additional information, particularly about the legal issues involved with all four of the documents. This continues to be the judgement of the committee.

3. The committee did not discover any previous case where "all members of the faculty were asked to sign an agreement unrelated to annual contracts," but it should be noted that not all faculty will be asked to sign the Confidentiality Agreement (see #4 and #5 below). It should also be noted that such historical questions were not part of our inquiry. We were concerned first with whether the policies violated the Faculty Code, and second with ways that the text of the various documents could be improved. The committee did not see any reason why signing the Confidentiality Agreement should affect the faculty's ability to "maintain a superior academic climate."

4. The conditions for dismissal of a faculty member are clearly stated in Chapter 5 of the Faculty Code and those conditions remain in effect whether a particular faculty member is asked to sign the confidentiality agreement or not. Since the only faculty members that will be asked to sign the agreement are those who have access to certain types of confidential, particularly on-line financial, information, it is conceivable that a faculty member who does not sign the confidentiality agreement might not be given responsibilities that require the agreement be signed.

5. As stated in #4 above, only certain faculty members will be asked to sign the confidentiality agreement. The agreement is associated with specific responsibilities of certain faculty members, and not with the mere fact of being a member of the UPS faculty.

From webpage: http://www.ups.edu/humanresources/zzzz/manual/cplcyFireArms.htm

Firearms/Weapons Policy

Policy

University policy strictly prohibits the possession or use of firearms or other weapons of any kind on campus by anyone except law-enforcement officials. That possession includes but is not limited to storage in lockers, desks, briefcases, or personal vehicles parked on university property. With respect to University personnel (faculty, staff and student staff), possession of firearms or other weapons of any kind on campus or while away from campus on University business is subject to corrective action, up to and including termination of employment. With respect to students, possession of firearms or other weapons of any kind on campus or while away from campus on University-sponsored activity is subject to sanctions up and including expulsion. Sanctions will be imposed in accordance with the procedures of the Student Integrity Code, Staff Policies and Procedures Manual, or Faculty Code, as appropriate. With respect to visitors, possession of firearms or other weapons of any kind is subject to expulsion from campus by Security Services.

All students, faculty, and staff who have knowledge of weapons on campus must report that knowledge immediately to the Director of Security Services or, in the Director's absence, an on-duty Security Officer.

Search

In cases of suspected possession of firearms or weapons of any kind by University personnel (faculty, staff and student staff), the University reserves the right, as stipulated in the Privacy and Appropriate Use of Resources policy, to search personal belongings on University property, including but not limited to articles of clothing, purses, briefcases, bags, and vehicles. All such searches must be approved in advance by the Vice President for Finance and Administration or the Director of Human Resources in the case of staff, or the Academic Vice President in the case of faculty, or the Vice President of Student Affairs in the case of students. In the absence of the pertinent individual, the president must authorize the search. Persons may be asked to leave campus or remain in the presence of Security Services or Tacoma Police until a search is conducted or the situation is resolved.

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 enrollment or employment, and refusal to consent will result in corrective action up to and including expulsion or termination of employment under procedures specified by the Student Integrity Code, Staff Policies and Procedures Manual, or the Faculty Code as appropriate.

Applicability

The above policy applies to anyone on the Puget Sound campus, including University personnel, students, and visitors. It also applies to University personnel and students away from campus on University business or University sponsored activity.

Origination Date: 11/2002

Owner: President's Cabinet

Contact: Assistant to the President/Secretary of the Corporation

**End Embedded Document**

**Non-Disclosure and Confidentiality Agreement**

**Cooney** noted that the Non-Disclosure and Confidentiality Agreement on p. 1 of the package is not the current version. The version modified by the PSC is on p. 10-11 of the circulated document.

**Goldstein** explained that many of the policies are not new. The University's general audit has, since November 2000, included an information technology (IT) audit in addition to a financial review. The IT auditors made recommendations on tightening controls in various ways. For example, the Banner system (unlike Cascade) did not force a change of passwords as the company that sells it does not include that feature. The auditors wanted to ensure security of the systems as well as policies and practices to ensure confidentiality.
Some of these policies predated the audit, but were repackaged with new clauses. Others were written from scratch, although **Goldstein** could not recall which ones these were. As IT gets more use, we become more used to sharing information and need to realize that information is still confidential. The Non-Disclosure and Confidentiality Agreement was designed to make employees more aware of these issues. The University's legal counsel reviewed the policies and gave further suggestions. Some of these suggestions were adopted but others were seen as too extreme for this institution.

**Cooney** did request the policies go before the PSC when they came up in the Cabinet. The revised Non-Disclosure and Confidentiality Agreement on p. 10-11 was the result of this PSC review.

**Wilson** asked whether all employees would be asked to sign this agreement. **Goldstein** replied that it would be asked of new employees. **Cooney** added that, among faculty, department chairs, program heads and others with access to Cascade budget information would be asked to sign it. **Ostrom** asked what would happen if they refused. **Cooney** replied that he hoped they could have a conversation about it, but thought he could imagine a situation where only the department secretary would have access to the budget.

**Taranovski** asked what would happen if he, as a department chair, discovered illegal activity. Would this policy prohibit him from contacting legal authorities? **Cooney** assured him it would not. For this reason, he explained, the PSC changed the wording in the definitional phrase "any information… that the University considers to be confidential" – "considers" was changed to "states" (p. 10). This should avoid the problem of the University deciding something is confidential *ex post facto* to prevent a possible embarrassment.

**Bartanen** explained that the University is not acting to protect specific data (such as the details of one budget) but, rather, the security of the system as a whole. **Goldstein** added that, in terms of practices, the University had tried to eliminate all generic passwords and allow only person-specific ones so they can track access. **Cooney** noted that there are numerous attempts to hack in to the system.

**Haltom** asked for more clarification about what they are trying to protect – pay lists? **Goldstein** and **Cooney** suggested some other sensitive data – systems as a whole; donor information; employee medical claims; social security numbers.

**Tinsley** followed on by asking how far this extends. What about information about University decisions? What about when a faculty member talks to the press? **Cooney** drew attention to the

last paragraph on p. 11, that states that this is not intended to stifle on-campus discussion or limit contact with the public. But confidential information should not be shared in such a setting just as it would be inappropriate to discuss as student discipline problem or faculty evaluation. In response to a further question from **Tinsley**, **Cooney** reported that a senior administrator could not use this policy to silence any unwanted talk, but confidentiality has always been a part of faculty life (such as the law prohibiting faculty from leaving graded papers in the hallway for collection).

**Sanders** asked about the student impact of this policy. **Goldstein** replied that when students have access to confidential University information (such as when students work for Financial Services) they already sign confidentiality agreements. This would not apply to students working with confidential ASUPS information, as ASUPS is a separate organization and would need its own policy. **Cooney** noted that a student employee of Financial Services who broke the agreement would lose his/her job.

**Information Use and Security Policy**

**Tinsley** asked if this policy on p. 4 is in its final form. Cooney explained that the underlined changes are not yet approved by the President. Goldstein explained that they are constantly revising policies and are looking for better ways to do things.

**Email, Voice-mail, And Network Access Policy**

**Tinsley** questioned the legal implications of the word “should” in the first paragraph of p. 8. **Cooney** replied that “shall” is clearer and was the PSC’s intention.

**Haltom** asked about the origins of this policy, particularly its focus on “misuse.” **Goldstein** replied that there was a policy predating the audit but it was cleaned up and, presumably, the misuse section was a response to specific incidents. She explained that this is a resource issue. **Haltom** further pushed the question of what is University business for email and web use, and **Cooney** added that, in the language of the old 1990s policy, “incidental and occasional use” is OK.

**McGruder** then raised a specific case of a faculty member using email for peace activism and being told that this was not OK, but would be if he were a political scientist. **Cooney** replied that if a faculty member uses the University’s network to serve as a node for an external organization, then large amounts of our bandwidth resources can be consumed. **Haltom** agreed with that “tragedy of the commons” problem but thought the wording was too broad. Some technology will choke off traffic, others will not. Shouldn’t the policy address specific misuses?

**Goldstein** explained that these University-owned resources should be used for University work. **Cooney** explained that faculty and staff concerns differ here. He is less concerned about a faculty member playing an internet game so long as their work is good at review. With staff, it is another matter.

**McGruder** returned to her case, explaining that her colleague was using a list-serv and not a server, and that he used his role in the organization to bring speakers to campus for the benefit of faculty and students. She noted that she would object to this policy on the grounds of this case.

**Tinsley** noted the Senate’s own recent political stance and wondered whether marginalized political positions would be as accepted. He focused on the reference to “commercial, religious or personal causes” on p. 8, asked where one draws the line. **Kline** echoed this concern, noting that causes are “the heart of what we teach.”

**Cooney** acknowledged those problems and added another: there is no intent to stifle self-expression but there is a problem when one is seen to be speaking for a group. In the case raised by McGruder, there was an external complaint: it was spam. He noted that it is tricky to draw

boundaries here. **Taranovski** explained that he is careful not to claim to represent the University's views when, say, writing to the News Tribune. Would it not be better, he asked, to use general phrases like "systematic and excessive personal use" or "commercial solicitations" in the policy rather than listing types of misuse.

**Matthews** voiced a general sentiment that the wording of such policies is difficult. He asked where the decision will be made (the Dean, he assumed) and whether there would be a mechanism for appeal. He suggested thee PSC might serve as the appeals body. **McGruder** echoed these concerns.

**Kline** drew our attention to the ambiguity of the phrase "may be copyrighted" on p. 8 and **Haltom** pointed out a similarly ambiguous "may" in the confidentiality section – was it permissive or probabilistic?

**Non-Disclosure and Confidentiality Agreement (revisited)**

**Matthews** returned to the issue of confidentiality and pointed out that many academics have confidential research data in their offices that should only be released by subpoena. **Hummel-Berry** agreed, adding that this aspect of the confidentiality policy is in conflict with IRB policy. She suggested that this disagreement should be reflected in the IRB paragraph.

**Cooney** reported that some PSC members thought that research data should not be kept in the office, but added that the rationale for a search is specific – only if the faculty member is thought to be breaking policy or law. If scientific research standards are broken, then it is a breach of federal law. **Hummel-Berry** pointed out that many homes are less secure than offices, and that such data should be kept in the office. **Matthews** added that the courts will mandate the release of any documents connected with an investigation. **Taranovski** noted that many universities have denied faculty under investigation access to their offices and data, and suggested that a bank vault is the best place for such data. **McGruder** disagreed strongly, reminding the Senate of the standard phrase in research subject permission forms that the data will be locked in a secure place at the institution. **Tullis** agreed, saying that keeping research data at home is like expecting physicians to keep patient files at home – a "ridiculous" suggestion.

**Cooney** assured the faculty members that the University is not interested in looking at confidential research data, but they are concerned with situations such as firearms in offices, sexually harassing communication, or students breaking in to change grades.

**Haltom** suggested we return to issues concerning Karen Goldstein, as she was visiting. He asked her whether the privacy policy started with the audit, and she replied that it was an update of an earlier policy.

**Tinsley** asked about the search policy: Does it include a personal search or cavity searches? **Goldstein** said that it did include personal searches, and added that if there were cavity searches legal authorities would be present. **Tinsley** then noted that gender is not mentioned in the policy, nor is the presence of a third-person. Can a female employee be searched by a male supervisor? Where is the protection if wrongly accused? Where is the sanction for a false accuser? **Bartanen** noted that there is a grievance policy in the faculty code, and **Taranovski** noted that one could refuse to be searched. **Tinsley** suggested that would result in firing. **Cooney** reported that the PSC's understanding was that, if faculty declined, the move to sanction or terminate would go through the normal process of the faculty code.

**Tinsley** asked whether this process applies to all, including the President and senior administrators. **Goldstein** replied that it did, and that in each case the next highest officer has authority, with the Trustees having authority over the President.

**Haltom** agreed with Tinsley's concerns. He suggested that consent that cannot be withheld is not consent and thus the language of consent should be dropped.

**Haltom** then went on to ask a question of process. Why weren't these policies shared with faculty *before* they were introduced? The Dean decided to give them to the PSC, but if the Senate had not charged the PSC, when would this have received faculty review? **Cooney** added that an earlier faculty discussion would not have been inappropriate, but reminded the Senate that the President has the authority to create policy. **Haltom** agreed but questioned why it was done this way as a *political* decision. He suggested that most faculty members are dismayed by the corporate tone of top-down decisions like this.

**Ostrom**, noting the time, suggested adjournment (MSP). **Tinsley** added his thanks to Karen Goldstein for her time.

The Senate then adjourned at 5:35pm.

Respectfully recorded by Julian Edgoose