Chapter II

Faculty Legislation

Article I.   Harassment *(05/06/2020)*

Behavior directed at members of the College community or others that is sufficiently severe, persistent, or pervasive and objectively offensive such that it unreasonably interferes with, limits or deprives someone of the ability to participate in or benefit from the college's educational programs or employment opportunities is prohibited. This includes, but is not limited to, harassment on the basis of race, color, sex (including pregnancy and parenting status), gender, gender identity or expression, genetic information, sexual orientation, religion, age, marital status, national origin, disability, or veteran status or any other basis prohibited by applicable federal, state, or local laws.

Article II.   Statement on Consensual Relationships *(05/20/2011)*

Faculty are entrusted with advising students, judging their work, assigning grades, and making recommendations for further study and/or employment. One's ability to perform these duties is seriously jeopardized by questions about intent, fairness, or favoritism. It is therefore unacceptable for faculty to have romantic or sexual relationships with students, except when the relationship pre-dates either the student's initial enrollment in courses at Whitman College or the faculty member's initial appointment and the faculty member holds no supervisory or evaluative role over the student. Relationships that may appear consensual, even those that do not involve a supervisory or evaluative role, may in fact constitute or develop into a violation of the College's Grievance Policy (Faculty Handbook, Chapter XI. Whitman College Grievance Policy, https://www.whitman.edu/provost/faculty-governance/faculty-handbook).

The possible harm of such relationships can extend beyond the immediately involved parties, as they may generate a perception of unfair treatment and interfere with the ability of other students to work comfortably and effectively. Therefore, faculty are expected to remove themselves from any activity or evaluative role that could reward or punish individuals because of a prior or current romantic relationship. In such cases, the faculty member must work either with the relevant Division Chair or with the Provost and Dean of Faculty to devise an alternative evaluation mechanism. Failure to do so is inconsistent with the AAUP's evaluation mechanism and the AAUP's (2009) statement on professional ethics. Such a violation could reasonably constitute cause for dismissal under Chapter I, Article III, Section 4 of the Faculty Code. Faculty should be aware, moreover, that the power differential involved in faculty/student relations is complex, that students also evaluate faculty: students' formal evaluations of faculty members are taken seriously by the college as a factor in assessing teaching, and students can also approach the Provost and Dean of the Faculty, the Dean of Students, or the Board of Review with complaints or concerns about a faculty member's professional conduct.

Similar power differentials may also render it inappropriate for faculty to have romantic or sexual relationships with staff over whom they have supervisory authority. Relationships that may appear consensual, even those that do not involve a supervisory role, may in fact constitute or develop into a violation of the College's Grievance Policy. In any of these situations, faculty may find it difficult to argue that a relationship was fully consensual.

Article III.   Environmental Principles for Whitman College *(02/23/2000)*

Recognizing the impact Whitman College has on the environment and the leadership role Whitman College plays as an institution of higher learning, the College affirms the following environmental principles and standards, which shall be consulted to explore the practical ways Whitman College can promote an environmentally conscious campus.

To reduce the amount of non-recyclable materials used; to reuse whatever materials may be reused; and, to utilize recycled materials whenever possible.

To consider the eco-friendliest science and technology available to decrease our environmental impact.

To continue to build an energy-efficient campus in the 21st century.

To utilize companies, where possible, that are active in their defense of the environment from further degradation.

To encourage individuals' environmental accountability through programs of environmental education.

To consider environmentally friendly options when they exist and are practical in decisions regarding developmental projects.

To further the use of reused materials, recyclable materials, and the Internet in campus communications.

To encourage and request food service to make environmentally friendly decisions, where reasonable, in purchasing food and supplies, reducing waste, and reusing materials.

To maintain campus grounds through the employment of bio-friendly substances and services.

To strive to improve upon current practices so we may harmonize the trends of the industrial world with the natural environment.

Article IV.   Firearms, Explosives, and Other Dangerous Weapons Policy *(05/06/2020)*

No firearms or ammunition are permitted in outdoor areas of the campus or in any college-owned buildings, including all fraternities and college-owned rentals, or in conjunction with any college-sponsored activity.

For the purpose of this policy, BB guns, illegal knives (switch or spring blade), blowguns, swords, tasers, slingshots, bows and arrows, crossbows, and similar devices are considered "dangerous weapons," and their possession and use are prohibited.

Explosives of any type, including fireworks, firecrackers, cherry bombs, bottle rockets and the like, are prohibited at all times.

The only three exceptions to this policy are 1) law enforcement officers in the course of their duty; 2) firearms, explosives, and other dangerous weapons used by faculty for educational purposes, and 3) students using firearms, explosives, and other dangerous weapons for educational purposes and who have received prior permission from the Dean of Students Office..

Items such as airsoft guns, paint guns, paintballs, darts, knives, mace, pepper spray, or other realistic toys or replicas used inappropriately, or in contexts for which they are not intended, will be treated as dangerous weapons. All firearms, explosives, and dangerous weapons will be confiscated.

Article V.   Information Technology Policy *(05/19/2000)*

Section 1.   Account Policy

A. The computer and networking resources are the property of Whitman College. Every student, faculty, and staff is entitled to an account to access those resources. The account is for the exclusive use of the user who is assigned the account and password. Lending of an account to another person is not permitted, and is considered to be a violation of College policy and may result in disciplinary action. The College does not sell, share or rent account information in ways different than are described in this policy.

B. The Whitman College "Privacy Policy" describes the user's right to privacy.

 1. Limitation

    The Whitman College "Acceptable Use Policy" describes limitations on the usage of accounts.

 2. Suspension of Accounts

    The Whitman College "Acceptable Use Policy" describes those actions that may lead to suspension of accounts.

 3. Upon Leaving the College

    a. Graduating students have access to their accounts for one year after graduation. Extensions beyond the one-year period will not customarily be granted. After one year, students have an option to participate in the life-long e-mail forwarding service through the Office of Alumni Relations.

    b. Students who leave the institution without graduating (e.g., transfer, dismissal, etc.) will have access to their accounts for one month following the termination of their relationship with the College. Students on leave of absence (including study abroad) will have their accounts retained.

    c. Faculty or staff who permanently retire may keep their account for life.

    d. Faculty who leave the College for other reasons will have access to their accounts for six months following the termination of their relationship with the College. If a longer period is desired, contact the Chief Information Officer.

    e. Staff who leave the College for other reasons will be evaluated on an individual basis. Generally, staff accounts will terminate immediately.

Section 2.   Network and IT Services Privacy Policy *(04/17/2019)*

A. This policy addresses the College's commitment to protecting and defending the privacy of authorized users of its Information Technology (IT) systems (network and IT services), and other systems that are capable of recording information about the user. Authorized users are individuals with a Whitman Network ID and Password.

This policy is informed by the principles of the 2014 report from the American Association of University Professors entitled "Academic Freedom and Electronic Communications".

All members of the Whitman community are subject to the inherent insecurity of electronic information particularly on the Internet, and are responsible for ensuring the privacy of their account (e.g. users should use a secure password, not share their passwords or access to their accounts, encrypt sensitive data, etc.).

Despite the College's adherence to these policies it cannot assure the Whitman Community protection from the sorts of activities broadly referred to as "hacking" whose consequence might include a loss of electronic privacy.

B. The College is committed to protecting the privacy of the Whitman Community as it concerns materials stored on College computers or transmitted electronically on College networks or IT infrastructure. The College does not sell, share, or rent account information in ways different than are described in this policy. Whitman College will not access or monitor computer accounts, usage of IT services, personal files, or other electronic records except when:

1. Authorized by the user(s), or

2. Performing maintenance necessary for the operation of the relevant systems, or

3. Required by vendor contract after vetting by the CIO and Information Security Officer for security and/or privacy matters, or

4. Necessary for billing purposes (e.g. long distance), or

5. Required by court order, or

6. As a part of a formal investigation into a violation of College policy.

C. While it is necessary to store some information about users and individual use of electronic services, neither this information nor knowledge derived from this information will be accessed unless:

1. It is required to maintain the integrity and availability of the College's IT or electronic infrastructure, or

2. There is clear evidence suggesting that the security and/or the integrity of the system is being compromised, or

3. Such access is in direct support of a law enforcement investigation, and then only with a court order, or

4. Such access is a necessary part of a formal investigation into a violation of College policy.

User(s) will be notified of access that falls under the exceptions in both sections B and C unless expressly prohibited by law or per policies and procedures in the faculty code and handbook, staff handbook, student handbook, or grievance policy.

In the situations described above in sections B and C, only the Chief Information Officer or the Information Security Officer, in consultation with the relevant senior officer, will authorize the release of this information or its derivatives to the requesting party.

D. Whitman College is committed to the free flow of ideas and the freedom of electronic speech. The College will actively protect the Whitman Community's freedom of expression. The content of electronic communication is not censored; this includes, but is not limited to, personal web pages, postings to unmoderated listservs and social media, and email. However, in accordance with the principles of this policy, the following limitations apply:

1. The volume of information may be limited without regard to content because of the technical constraints of the system (example: internet bandwidth becomes saturated or a compromised account is used to send spam).

2. The College retains the right to protect itself from liabilities posed by the electronic behavior of members of the College, if these behaviors are in violation of College policies or local, state, and federal laws. Otherwise the College will make every reasonable effort to defend users whose rights to freedom of expression are being challenged.

3. Users are expected to abide by the laws of the State of Washington and the United States and by the policies of the College.

Section 3.   Acceptable Use Policy

A. Introduction

The Whitman Campus Network is provided as a service to students, faculty, staff, and other members of the Whitman community. Maintained by Whitman College Technology Services (WCTS), the Network supports the instruction, research, and service mission of the College. This document outlines the policy of acceptable use of Whitman Campus Network resources, the effective protection of individual users, equitable access, and proper management of those resources.

B. Individual Responsibilities

1. Whitman College strives to provide fair and distributed access to computing and network facilities for the entire community of users. It is the intent of Whitman College to make available unfiltered information on the Internet for the College community. Members are responsible for selecting, viewing, and utilizing resources. If it is necessary to filter or block any information to enhance security or performance, and if this filtering or blocking occurs regularly or more often than occasionally, a description of and rationale for the action will be posted with other WCTS online information.

2. To foster trust and intellectual freedom, it is necessary to practice courtesy, common sense, and restraint in the use of shared resources. Improper use of Whitman facilities may prevent others from gaining fair access to those facilities.

3. Furthermore, users must keep in mind that networks or systems outside of Whitman College (including those in other countries) may have their own distinctive policies and procedures. Users are advised to learn and abide by the policies and procedures of these external networks.

4. Insofar as a secure and reliable computer system is necessary to the academic mission of the College, all members of the College community should contribute to the security of the system by conscientiously protecting their access privileges, for example: users need to select a secure password and, furthermore, should change their passwords frequently. Likewise, the computer system administrators will act promptly when evidence of serious compromises to the security of the system is detected.

5. The Whitman College computing network must work within finite limitations of bandwidth and disk space. Users are reminded that electronic mail exists on a space shared by other members of the community, and users are responsible for maintenance of their electronic mailbox. Therefore, users are encouraged to keep only pertinent materials in their mailbox accounts. The user should:

    a. Conserve disk space: delete unwanted e-mail messages as soon as possible and arrange for forwarding of e-mail when appropriate (e.g. breaks, overseas study).

    b. Be aware that e-mail cannot be guaranteed to be perfectly private: others may intentionally or unintentionally forward or print your message, making it publicly available.

    c. Like electronic mail the maintenance of a user's own storage area is the user's responsibility. The user should:

        i. Conserve server disk space

        ii. Routinely and frequently check for viruses.

        iii. Not maintain anything that the user considers to be private in the network storage area. (Files in network storage may be accessible by persons with system privileges.)

C. Conduct

Activities that violate the Acceptable Use Policy include, but are not limited to, those in the following list:

1. Using a computer account that does not rightfully belong to you.

2. Violating copyright laws and their fair use provisions through inappropriate reproduction or distribution of copyrighted files (including movies, music, computer software, text, and images).

3. Using the Campus Information Technology (IT) infrastructure to gain unauthorized access to other computer systems.

4. Unauthorized connecting of equipment to the campus network (this includes personal hubs in rooms).

5. Attempting to break into the system by circumventing data protection schemes or uncovering security loopholes. This includes the wrongful use of programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

6. Knowingly or negligently performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.

7. Attempting to damage or to place excessive load on a computer system or network by using programs, such as (but not limited to) computer viruses, Trojan Horses, and worms.

8. Deliberately wasting or overloading computing or printing resources, or deliberately using excessive bandwidth on the network.

9. Violating terms of software licensing agreements.

10. Using College resources for non-academic commercial activity such as creating products or services for sale, without express College approval.

11. Using electronic mail or other Information Technology resources to abuse, harass, or intimidate members of the College community on any basis including race, ethnic origin, creed, gender or sexual orientation. Users are reminded that sexually suggestive materials displayed inappropriately in public places, the classroom, or the workplace may constitute sexual harassment.

12. Propagating mass mailings with the intent of flooding ("spamming" or "bombing") the accounts of others.

13. Forging the identity of a user or machine in an electronic communication.

14. Transmitting or reproducing materials that are slanderous or defamatory, or that otherwise violate existing laws or College regulations.

15. Attempting to wrongfully monitor or tamper with another user's use of the College's Information Technology infrastructure (such as reading, copying, changing, or deleting another user's files or software) without the knowledge and agreement of the owner.

D. Authorization

1. Personal use of Whitman College computing resources by staff employees during working hours is an issue that will be determined by the employee's supervisor.

2. Use of College computing and network facilities for non-academic commercial monetary gain requires the approval of the College and may require a written contract that gives full details of any financial obligation and/or charge for use, if any.

3. Connecting network devices, such as "network hubs" to the campus system will require authorization from the Chief Information Officer or their designee.

4. Setting up a new domain on a computer located on the Whitman College network will require authorization from the Chief Information Officer or a designee.

5. Authorization decisions may be appealed to the appropriate Dean or supervisor.

E. Enforcement of Policies

1. Failure to comply with any of the above policies may result in termination of network privileges, College disciplinary action, and/or criminal prosecution.

2. It is understood that users may unwittingly create problems for others by, for example, employing programs that monopolize the network bandwidth. In such cases the Chief Information Officer (or a designate) will contact the user and explain why and how the user needs to modify the user's electronic behavior. A policy clarification letter may be written. In cases of repeated problematic behavior, the CTO may recommend to the appropriate Dean or supervisor that a formal warning be placed in the user's College record. If so, the user will be notified of this recommendation and will be allowed the opportunity to provide a response to the recommendation in advance of the Dean's/supervisor's decision.

3. Access to computing resources may be suspended temporarily at any time by the Chief Information Officer (or a designate), if there is clear evidence to suggest that the resource(s) are being used in a manner that seriously compromises the security and/or integrity of the resource(s). In such a case, the owner of the account will be sent notification of this action within twelve hours and assisted in extracting such files as are immediately needed (e.g., for class assignments) and/or establishing a new, secure account, as appropriate.

4. Upon suspension, a user shall discuss the issue with the Chief Information Officer (or a designate) in order to reestablish an account. The account shall be reestablished within one business day of a satisfactory conclusion to this meeting. If the account is not reestablished to the user's satisfaction, the user may appeal to the appropriate office of the College. The Chief Information Officer (or the student's designate) may also choose to refer the case for disciplinary action in accordance with established procedures. For students, it is as described in Part 5, Section 2 of the Whitman College Student Handbook. For faculty, see Faculty Code, Chapter I; for staff, see Staff Handbook.

Article VI.   Procedures for Whitman Faculty/Staff-Led Trips Abroad *(04/11/2002)*

Section 1.   Approval of Trip

The approval process for any Whitman-affiliated or Whitman-supported course or field trip in foreign countries for Whitman students that are organized by Whitman faculty/staff is described below.

The Provost and Dean of the Faculty must approve of the activity, with the assistance of the Off-Campus Studies Committee, in terms of the risk and liability of taking students to a given destination. It is the responsibility of the faculty/staff member organizing the trip to provide as much information as possible to the Provost and Dean of the Faculty about the following:

A. Approval for the trip in writing from the appropriate academic department if credit is involved.

B. Summary of the trip, including itinerary, course descriptions and housing information

C. Description of the budget and program fees charged to students

D. Generally known risks in the destination

E. Names and qualifications of Whitman and non-Whitman staff for the trip

F. Information about the vendors for trip such as tour operators and bus companies

Faculty/staff members who propose potential trips should allow three months for the Provost and Dean of Faculty to reach a decision about the proposed trip. Approval for such trips may be withdrawn if conditions in the destination country(ies) deteriorates prior to departure.

Section 2.   Required Predeparture Documents

The faculty/staff member(s) leading the group is responsible for distributing and collecting the following required predeparture documents. The forms are available from the Off-Campus Study Office. (These requirements are consistent with what are required for study abroad students.)

It is the faculty/staff leader's responsibility to leave a copy of these forms with the Division Secretary for their building. These forms are all available in the Study Abroad Office.

A. *Health Statement and Liability Waiver* with the following attachments:

1. Center for Disease Control immunization recommendations for region

2. U.S. State Department Travel Advisories for countries to be visited

B. *Proof of Medical Insurance Form (*demonstrates student is covered while abroad)

C. *International Student Identity Card Application* (benefits include medical evacuation insurance)

D. *Dean of Students Clearance* (There is no form for this, but the organizer should send the names of the participants to the Dean of Students Office to make sure that

participants have no history of discipline or other non-academic problems that the organizer should be aware of.)

Section 3.   Predeparture Orientation Information

To help the students have realistic expectation for their foreign experience, Whitman faculty/staff taking students abroad should provide students with appropriate predeparture information. Guidelines for predeparture information are described below. While it is the faculty/staff leader's responsibility to organize the predeparture information, the Study Abroad Office can provide suggestions for sources of information.

A. Description of course/activity including details about credit, prerequisites and academic expectations

B. Description of physical abilities necessary for activity (e.g., strenuous hiking)

C. Calendar and itinerary

D. Program cost, availability of financial aid, and billing procedures

E. Information on how to obtain a passport and visa(s) if required

F. Description of housing and living conditions

G. Banking and money matters (ATM, Travelers Checks, etc.)

H. Description of local conditions including access to medical facilities, road safety, health risks, crime, attitudes towards Americans

I. Cultural norms and taboos

J. Appropriate clothing, luggage and other items to bring

K. Emergency contact information for families such as e-mail address, fax, telephone

Section 4.   Information for Parents

The faculty/staff leader will inform the parents or guardians of the participants of the risks of the activity and the cost/billing procedures, unless the student is no longer a dependent of their parents.

Section 5.   Predeparture and In-Country Procedures

The faculty/staff leader is responsible for taking the following precautions prior to departure and upon arrival in-country.

A. Leave a list of participants and contact information for the group with the Provost and Dean of Faculty's Office prior to departure.

B. Register all group participants by fax or telephone with the nearest U.S. consulate or embassy in the countries that you will be in so that U.S. officials can contact and assist the group in the event of an emergency in that country. (Embassy may be notified prior to departure from the U.S.) The U.S. consulate/embassy needs the following information: names and passport numbers of group members; name and phone number of the place where the group is staying. Contact information for U.S. consulates/embassies abroad can be found at http://travel.state.gov.

C. Provide participants with local emergency contact information such as how to reach the faculty director after hours and where to go for medical attention in the event of an emergency.

D. Remind students of local health and safety risks upon arrival at each new destination.

Article VII.   Smoking *(05/06/2020)*

It is the policy of Whitman College that students, faculty, staff, and visitors to the campus are entitled to live, study, and work in areas that are free of smoke. In accordance with this policy and Washington State law, smoking in any form, including tobacco, cannabis, electronic cigarettes or vaping, is prohibited inside any building on the Whitman College campus and is prohibited within 25 feet of any entrance, exit, window, or ventilation intake of any Whitman College campus building. (WAC 110-200-0420).