MEMORANDUM
Academic Council
Fairfield University

TO: Academic Council

FROM: Subcommittee to consider remaining items from review of the Journal of Record

DATE: October 25, 2011

RE: Recommendations for the nine remaining Journal of Record items

At a number of meetings in academic year 2010-2011, the Academic Council considered a report from the Ad Hoc Committee to Review the Journal of Record. Our subcommittee was formed in spring 2011 by the Council and charged “to consider all the items under bullet 4 [on page 4 of the Report from the Ad Hoc Committee to Review the Journal of Record dated 11/10/2010] and items #22 and #44 [in the document Journal of Record with 55 changes shown for the AC, dated 11/10/2010].”

Specifically, the items we were charged to consider are numbered 16, 19, 22, 23, 36, 44, 50, 51, and 52 from the Journal of Record with 55 changes shown for the AC and the Ad Hoc JOR committee report. Our recommendations for each of the nine items are in this report. All relevant documents can be found with the materials for the Council’s December 6, 2010 meeting.

Item 16.
The current entry in the Journal of Record is:

Rank and Tenure Applications by Committee Members:
It is the sense of the General Faculty that, if an individual faculty member should wish to apply for tenure or promotion while serving a term on the Faculty Committee for Rank and Tenure, that faculty member should relinquish committee membership for the academic year during which his application is being considered.

GF: 03/22/1985

Recommendation and Rationale: The Subcommittee recommends that this item be removed from the Journal of Record because this matter is covered in the Handbook as follows, “No member of the Committee may apply for promotion during his/her tenure on the Committee.” [I.C.b.2, paragraph 2]. Furthermore, only tenured faculty members are allowed to serve on the Rank and Tenure Committee.

Item 19.
The current entry in the Journal of Record is:

Research Applications by Research Committee Members:
It is the sense of the General Faculty that, if an individual faculty member should wish to apply for sabbatical leave, summer faculty stipend or research grant while serving a term on the faculty Research Committee, that faculty member should absent himself/herself from committee deliberations during the meeting(s) in which his/her application is being considered.

GF: 03/22/1985
The Research Committee is responsible for making decisions on applications in five different categories: Summer Stipends, Research Grants, Senior Summer Fellowships, Sabbaticals, and Pre-Tenure Research Leaves. The application guidelines for each category are in a separate appendix in the Journal of Record. For the first three, the application guidelines in the Journal of Record stipulate “Members of the Faculty Research Committee are not eligible to apply during their term in order to avoid a conflict of interest”. In addition, the Handbook states “No member of the [Research] Committee may apply for research grants and/or summer stipend awards during his/her tenure on the Committee; however, members may apply for sabbatical leaves and/or extraordinary research leaves concurrent with a term on the Committee.” [I.C.b.3, page 12.]

Recommendation: The Subcommittee recommends that this item be revised as follows:

Sabbatical and Pre-Tenure Research Leaves by members of the Research Committee:
If an individual faculty member applies for Sabbatical or Pre-Tenure Research Leave while serving a term on the Research Committee, that faculty member shall absent him or herself from committee deliberations during the meeting(s) in which his or her application is being considered.

GF: 3/22/1985
AC: Date of Approval

Rationale: The prohibition for Research Committee members applying for Summer Stipends, Research Grants or Senior Summer Fellowships is clearly stated in the application guidelines for each award in the Journal of Record and does not need to be addressed elsewhere in the Journal of Record. The revised entry is consistent with what is already in the Handbook and the Journal of Record. Even though it is unlikely that an untenured faculty member would be serving on the Research Committee and applying for a Pre-Tenure Research Leave, it is the position of the Subcommittee that Pre-Tenure Research Leaves should be treated in the same way as sabbaticals.

Item 22.
The current entry in the Journal of Record with changes suggested by the Ad Hoc Committee to review the Journal of Record is as follows:

Missed Classes:
"All instructors should begin and end their classes on time as a courtesy to their students and fellow instructors. When, for any valid reason, they are unable to meet their classes, they should notify the appropriate Dean and, if possible, make arrangements for conducting the class." (from the Faculty Handbook, I.C.1.a)

When faculty members are unable to meet their classes, they should notify the appropriate Dean, and, if possible, the students as soon as they know that they will not meet their classes.

In the event of unusual or inclement weather, when the University remains open, faculty members should make every reasonable effort to meet their regularly scheduled classes; the final judgment on what is reasonable effort resides with the individual faculty member.

Faculty members who are unable for any reason to meet with their classes should, if possible, make arrangements with a colleague to conduct class, or otherwise endeavor to...
cover missed class material through e.g. additional assignments or lengthened class meetings.

Similarly, when class time is lost through frequent school closings due to weather or other emergencies, faculty members should endeavor to cover missed class material through e.g. additional assignments or lengthened class meetings.

AC: 09/12/1994

Recommendation: The Subcommittee recommends that this item be revised as follows:

**Canceling classes in inclement weather:**

In the event of inclement weather, when the University remains open, faculty members should make every reasonable effort to meet their regularly scheduled classes. The final judgment on what is reasonable effort, and therefore whether to hold class, resides with the individual faculty member. Faculty members should try to notify their students of a decision to cancel class in a timely manner.

AC: 09/12/1994

AC: Date of Approval

Rationale: It is the position of the Subcommittee that only the information in the third paragraph is necessary and should remain in the Journal of Record; specifically, that faculty members need to understand that they are not required to travel to the University in dangerous conditions, even if the University is open.

Item 23.

The text from the Journal of Record with 55 changes shown for the AC is as follows:

<table>
<thead>
<tr>
<th>Entry that needs to be revised</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Make-ups for Missed Exams:</strong></td>
</tr>
<tr>
<td>The Dean of the student’s school and not the Office of Student Services should certify that a student was eligible to receive an absentee examination.</td>
</tr>
<tr>
<td>Recommendation: The AC should modify this entry as it may be too directive. The text should reflect the combination of policies in the catalog and the Student Handbook.</td>
</tr>
</tbody>
</table>

The subcommittee recommends that the current entry be deleted and the following entry be included:

**Class Attendance.**

All students are expected to attend every regularly scheduled class session. The impact of attendance on grading is specified in the syllabus for each course. Unexcused absences may be reported to the appropriate academic dean.

Faculty members should have a policy for dealing with student absence on the syllabus for each course. If a student will miss a class due to an illness/injury, the professor should be notified according to the policy on the syllabus. If a student will miss an exam, quiz or in-class presentation due to illness/injury or another type of emergency, the professor should be contacted beforehand. A faculty member may request that the student provide
verification of the absence from a health care provider. It is the purview of the faculty
member to determine when or if a student absence will be excused.

Item 36.
The text from the Journal of Record with 55 changes shown for the AC is as follows:

36. An entry that needs to be reviewed

Tutorials:
Students may be permitted to enroll in a course listed in the university catalogue on a tutorial basis with
approval of the Area Coordinator/Chair and by arrangement with the faculty member offering the tutorial.

1. To register, students must obtain the appropriate form from the Office of the Registrar and have it
completed by the faculty member offering the tutorial.

2. The tutorial appears on the transcript with appropriate notation as a tutorial under the equivalent
number, e.g., EN 11(t), PY 15(t).

Recommendation: The AC should revisit this entry to see if it is still relevant, or if it should be reconciled
with the entry above on Independent Studies. Process language is inappropriate for the Journal of Record.

The subcommittee recommends that this item be revised as follows:

Tutorials.
In rare circumstances, students may be permitted to enroll in a course listed in the
University catalog on a tutorial basis with the approval of the Area Coordinator/Chair and
the faculty member offering the tutorial.

Rationale. Occasionally, a student needs a specific course to satisfy core or major requirements. In such
cases, the student is allowed to register for that course as a tutorial. The revised entry allows a student to
have the appropriate information appear on the transcript (as opposed to the course number for an Independent Study), does not include the process language, and indicates that this should happen only in rare circumstances.

**Item 44.**
The current entry in the Journal of Record is:

Consideration of prior service for promotion and tenure:
Evaluation for promotion or tenure should be based on a faculty member's performance in the academic career starting with his/her initial appointment at the rank of full-time instructor higher at an institution of higher learning. While promotion and tenure is based on performance in the academic career, the committee may seek to convince itself that such performance will continue at Fairfield University.

AC: 11/05/1991

The revision proposed by the Ad Hoc Committee to review the Journal of Record is:

Consideration of prior service for promotion and tenure:
Evaluation for promotion or tenure are based on the candidate's performance in the entire academic career, the Rank and Tenure Committee must also judge that the candidate's performance at Fairfield University has met the requirements for rank and tenure.

Recommendation: The Subcommittee recommends that the entry be revised differently, as follows:

Consideration of prior service for promotion and tenure:
Evaluation for promotion or tenure should be based on a faculty member’s performance in the academic career starting with his/her initial appointment at the rank of full-time instructor higher at an institution of higher learning. While promotion and tenure are based on performance in the academic career, the committee shall not recommend tenure unless it has reasonable confidence that such performance will continue at Fairfield University.

AC: 11/05/1991
AC: Date of approval

Rationale: Apparently, the language proposed by the Ad Hoc Committee did not convey what it was intended to convey. The original entry was not stated in the language of policy and was not clearly consistent with the Handbook. The revision makes it clear that all work must count towards tenure and promotion, and is consistent with the Handbook language [II.A.3], “…tenure is granted not merely when a candidate meets minimum qualifications for rank, but only when there is reasonable confidence that the candidate will continue to develop as an outstanding teacher, a practicing scholar or artist, and a contributing member of the campus community.”

**Item 50.**
The current entry in the Journal of Record is:

Faculty Admission to University Courses:
I. Tuition is remitted for full time faculty when they wish to take courses sponsored in whole or part by the University. In some cases, tuition remission is governed by conditions, as follows:
1. For most courses offered by the University, the only condition is the completion of the proper tuition remission and registration forms.

2. For courses in which there are limitations on enrollment based on physical requirements (e.g., limited number of lab stations), faculty may enroll on a space available basis after regular full time and part time students.

3. For courses offered under a "contract" fee structure, faculty participation is contingent upon funding from some source; faculty will then have access to the course on an equal basis with anyone else.

II. Fees other than tuition are the responsibility of the faculty member.

III. Funding for "contract" courses (I.3 above) is to come from University sources.

AC: 05/16/1988

Recommendation and Rationale: See recommendation and rationale for Item 51.

Item 51.
The text from the Journal of Record with 55 changes shown for the AC is as follows:

51. Recommend that the location for this entry be reviewed.

Illness/Disability Policy:
The University will provide full salary and benefits for up to six (6) months of absence due to disabling illness, injury, pregnancy, childbirth or related conditions. Any faculty member who anticipates an extended disability absence will inform his/her Dean as soon as possible indicating the anticipated commencement and, whenever possible, the anticipated duration of the period of absence. The University may require medical certification in cases of recurring absences, or for absences lasting longer than a month.

The period of recovery due to a normal childbirth is presumed to be six weeks. The University may require medical certification for absences in excess of six weeks.

The University's total Disability Plan provides benefits for serious and long-term illness/injury after six months, subject to the terms of the Plan. Faculty members are expected to apply for and avail themselves of the Plan where appropriate.

Work-related injuries are covered by Worker's Compensation.

AC: 09/09/1991

Recommendation: that the AC consider whether the information in this entry belongs in the Journal of Record or the Benefit Plans Overview.

Recommendation and rationale for items 50 & 51: Items 50 and 51 deal with particular benefits for faculty. The Journal of Record may not be an appropriate place for entries on benefits for faculty as most benefits for faculty are now delineated in the Faculty Handbook and the Benefits Plan Overview. The
subcommittee’s concern is that any statement of an individual faculty benefit should be complete, up-to-date, and protected from being changed unilaterally by the administration or trustees; Item 51, in particular, is not up-to-date. Before making any recommendation to move the information in either of these two entries to the Benefit Plans Overview, the subcommittee’s position is that it is incumbent upon the faculty to reach agreement with the administration on language that items in the Benefit Plans Overview cannot be unilaterally changed. The subcommittee recommends that the Council ask the Faculty Salary Committee to work with the administration to reach agreement on language for the Journal of Record and/or the Faculty Handbook that will protect benefits in the Benefits Plan Overview from unilateral change by the administration or trustees. Draft language should be vetted by the Faculty Welfare Committee/AAUP. For the time being, the subcommittee recommends no change to either Item 50 or Item 51.

**Proposed Motion.** The Academic Council asks the Faculty Salary Committee to work with the administration to reach agreement on language for the Journal of Record and/or the Faculty Handbook that would protect benefits in the Benefit Plans Overview from unilateral change. Draft language should be vetted by the Faculty Welfare Committee/AAUP.

**Item 52.**

Item 52 involves a Journal of Record entry entitled Computer Usage Guidelines, approved by the Academic Council on 2/1/1993 (see Appendix I). The recommendation from the Ad Hoc Committee to Review the Journal of Record was “that the AC review this entry since the information may be outdated.” The present subcommittee found the following policies:

I. The Computer Usage Guidelines in the 11/2009 Journal of Record, approved by the Council 2/1/1993 (see Appendix I)

II. Fairfield University Computer Systems Acceptable Use Policy (AUP 2000), approved by the Council on 11/6/2000 (see Appendix II)


IV. Fairfield University Computer Systems Acceptable Use Policy (AUP 2004), found on the CNS website and dated November 13, 2000/Updated June 30, 2004/© 2011 (see Appendix IV)

V. Procedures in Support of Fairfield University’s Computer Systems Acceptable Use Policy (Procedures 2004), found on the CNS website, undated with © 2011 (see Appendix V)

The policy in the Journal of Record (Appendix I) is outdated. AUP 2000 and Procedures 2000 were approved by the Academic Council but, apparently, never entered into the Journal of Record. AUP 2004 and Procedures 2004 do not appear to have been approved by the Academic Council. There do not appear to be any substantive differences between the documents approved by the Council in 2000 and the updated 2004 documents.

**Recommendation.** That the Academic Council review and approve AUP 2004 (Appendix IV) and Procedures 2004 (Appendix V) and have these two documents replace the current entry in the Journal of Record, Computer Usage Guidelines (Appendix I).
APPENDICES

Appendix I:
Page 8

Appendix II:
Fairfield University Computer Systems Acceptable Use Policy (AUP 2000)
Page 9

Appendix III:
Procedures in Support of Fairfield University's Computer Systems Acceptable Use Policy (Procedures 2000)
Page 13

Appendix IV:
Fairfield University Computer Systems Acceptable Use Policy (AUP 2004)
Page 18

Appendix V:
Page 21
Appendix I:


Computer Usage Guidelines:

Only members of the Fairfield University community are eligible to use the computing resources available on campus.

Resources are available solely for:

* students needing resources for course-related work
* faculty engaged in research, instructional development, and other professional activities

The computer resources of Fairfield University are limited and should be used wisely and carefully. To assist in the most efficient uses of all computer resources on campus, the following guidelines have been established by the Educational Technologies Committee:

1. Each user must use the computing resources for the purpose(s) for which they are intended. Resources should be used for research, instructional, or administrative activities and must not be used for primarily commercial purposes.

2. Users may not engage in unauthorized duplication, alteration, or destruction of data, programs, or software belonging to other members of the University community. Users may not transmit or disclose data, programs or software belonging to others. Further, users may not copy materials protected by copyright or licensing agreement.

3. Users may not encroach on others' use of computer resources. This includes, but is not limited to, such activities as typing up computer resources for game playing; sending frivolous or excessive messages; spreading computer viruses; using excess amounts of storage; printing excessive copies; or running inappropriate programs that utilize inordinate amounts of computer time when more efficient programs are available.

4. Users must not attempt to modify computer system(s) facilities on the University's mainframe, networks, microcomputer, and external network links.

5. Users shall abide by the security policies set forth by the System Manager.

Identified violations will be reported to the appropriate office or Student Judicial Board for action as described in the Faculty Handbook or the Student Handbook.

AC: 02/01/1993
Appendix II:
Fairfield University Computer Systems Acceptable Use Policy (AUP 2000)

Fairfield University Computer Systems Acceptable Use Policy

This policy is designed to guide students, faculty, staff, and other authorized users in the acceptable use of computer and information systems and networks provided by Fairfield University according to the mission of the University. It is meant as an application of the principles of respect and reverence for every person, the development of community and the ideals of liberal education that are at the core of Fairfield’s Catholic, Jesuit identity. This policy supersedes the “Acceptable Use Policy” (number 610) adopted 1/1/94. This policy does not supersede any other University policies, including the student grievances, sexual harassment, and personal conduct.

Guiding Principles:
The Fairfield University community is encouraged to make innovative and creative use of information technologies in support of education and research. Access to information representing a multitude of views on current and historical issues should be allowed for the interest, information and enlightenment of the University community. Consistent with other University policies, this policy is intended to respect the rights and obligations of Academic Freedom, and recognizes that the educational mission of the University is served in a variety of ways.

The University recognizes that the purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorized use or sale of works available in the private sector. Publication, distribution, or broadcast of copyright protected materials without permission is prohibited (See Policy on Copyright, attached). Also consistent with other University policies, an individual’s right of access to computer materials should not be denied or abridged because of race, creed color, age, national origin, gender, sexual orientation, or disability.

The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be recipients of material they find offensive. Those who use e-mail and/or make information about themselves available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual’s distribution of personal information.

In the interests of promoting the free exchange of ideas, Fairfield University does not exercise prior review of electronic documents available on its network and accessible locally or through the internet. Individuals who access materials available on the Fairfield University network should understand these materials, unless otherwise posted, do not necessarily reflect the views of Fairfield University. Individuals who feel that particular materials posted on the Fairfield University network are inappropriate or otherwise objectionable, may lodge a formal complaint through the office of Computing and Network Services.

Fairfield University computing and network resources are to be used for University-related research, instruction, learning, enrichment, dissemination of scholarly information, and administrative activities. The computing and network facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. Computers and network systems offer powerful tools for communication among members of the community and of communities outside the University. When used appropriately, these tools can enhance dialog and communication. When used unlawfully or inappropriately, however, these tools can infringe on the rights of others.
Responsibilities:
The following examples, though not covering every situation, specify some of the responsibilities that accompany computer use at Fairfield and/or on networks to which Fairfield is connected.

1. Users may not attempt to modify the University system or network facilities or attempt to crash systems. They should not tamper with any software protections or restrictions placed on computer applications or files.

2. All users must obtain authorized computing accounts and may only use their own user names and passwords to access University computing and network systems. Users may not supply false or misleading data nor improperly obtain another's password in order to gain access to computers or network systems, data or information. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Users should not attempt to subvert the restrictions associated with their computer accounts.

3. Users are responsible for all use of their computer account(s). They should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources. Individual password security is the responsibility of each user.

4. Users may not encroach on others’ use of computer resources. Such activities would include, but are not limited to, tying up computer resources for excessive game playing or other trivial applications; sending harassing messages; sending frivolous or excessive messages, including chain letters, junk mail, and other types of broadcast messages, either locally or over the Internet; using excessive amounts of storage (as determined by Computing and Network Service policies); intentionally introducing any computer viruses, worms, Trojan Horses, or other rogue programs to Fairfield University hardware or software; physically damaging systems; or running grossly inefficient programs when efficient ones are available.

5. Users are responsible for making use of software and electronic materials in accordance with copyright and licensing restrictions and applicable university policies. Fairfield University equipment and software may not be used to violate copyright or the terms of any license agreement. No one may inspect, modify, distribute, or copy proprietary data, directories, programs, files, disks or other software without proper authorization.

6. Users must remember that information distributed through the University's computing and networking facilities is a form of publishing, and some of the same standards apply. For example, anything generated at Fairfield that is available on the Internet through the University’s network represents the University and not just an individual. Even with disclaimers, the University is represented by its students, faculty and staff, and appropriate content, language and behavior is warranted.

7. Users may not transmit any material that is unlawful, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any federal, state, or local laws. Materials made available or transmitted on University Computer systems must comply with all University policies governing conduct of students, faculty and staff.

Administration:
The University encourages all members of its community to use electronic communications in a manner that is respectful to others. While respecting users’ confidentiality and privacy, the University reserves the right to examine computer files and monitor electronic activity within the limits of other applicable University policies. The University may exercise this right in order to enforce its policies regarding harassment and the safety of individuals; to prevent the posting of proprietary software or electronic copies of electronic texts or images in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data either at the University or elsewhere; and to protect the University against seriously damaging consequences. The University may restrict the use of its
computers and network systems for electronic communications when faced with evidence of violation of University policies, or federal, state or local laws. The University reserves the right to limit access to its networks through University-owned or other computers, and to remove or limit access to material posted on University-owned computers.

All users are expected to conduct themselves consistent with these responsibilities and all other applicable University policies. Abuse of computing privileges will subject the user to disciplinary action according to established University procedures. Abuse of networks or computers at other sites through the use of Fairfield University resources will be treated as an abuse of computing privileges at the University. When appropriate, temporary restrictive actions will be taken by system or network administrators pending further disciplinary action; the loss of computing privileges may result.

The University and users recognize that all members of the University community are bound by federal, state and local laws relating to civil rights, harassment, copyright, security and other statutes relating to electronic media. It should be understood that this policy does not preclude enforcement under the laws and regulations of the United States of America nor the State of Connecticut.

This policy may be amended or changed by the University Vice-Presidents, and in matters affecting the Academic Division, with the mutual consent of the Academic Council.

The undersigned acknowledges that they have reviewed and understand Fairfield University’s Acceptable Use Policy noted above and that failure to adhere to these principles and policies may result in the revocation of authorized access to electronic networks and computer systems at Fairfield University. A signed statement is required to gain access to Fairfield University’s network(s) and computer systems. Please return the lower portion of this form to the Help Desk (Bannow Science Center, Room GR-33) in order to obtain your e-mail account.

Name (Printed) 
Signature 
Date:
Appendix III:
Procedures in Support of Fairfield University’s Computer Systems Acceptable Use Policy (Procedures 2000)

Procedures in Support of Fairfield University’s Computer Systems Acceptable Use Policy
November 1, 2000

Preface
These procedures have been designated to complement rather than supercede existing university procedures, guidelines, and policies relating to computer use by faculty, staff and students. For this reason, final authority for the resolution of complaints, including any penalties rests with the appropriate chief administrator.

For the purposes of this policy, “appropriate chief administrator” shall be defined as the senior administrator who has jurisdiction over the alleged offender of the Fairfield University Computer Systems Acceptable Use Policy (hereafter cited as the Acceptable Use Policy). The “appropriate Chief administrator” for faculty is the Academic Vice President. The “appropriate chief administrator” for students will either be the Academic Vice President if the offense is related to academics, or the Vice President for Student Services in non-academic affairs. In circumstances where the jurisdictional lines are not clearly demarcated, authority will rest with both Vice Presidents, disputes being resolved by the President. In the case of non-faculty staff, the Associate Vice President of Human Resources is the chief administrator.

Guiding Principles: These procedures were designed to balance seven interests:
1) respecting the rights and responsibilities of academic freedom as defined in applicable policies for faculty and for students engaged in academic work
2) protecting the rights of the university;
3) protecting users’ privacy;
4) protecting the System or network Administrator (SNA) in the performance of his or her job;
5) allowing routine administrative actions that might affect users’ files;
6) providing a mechanism to allow non-routine, non-emergency access to users’ files when it can be justified;
7) providing guidelines for the occasional need to take immediate action. The ability of an SNA to read a user’s files does not imply that he or she may do so without obtaining the approval required by these procedures.

Balancing Rights
“Incidental personal use” of computing systems is an accepted and appropriate benefit of being associated with Fairfield University. However, “incidental personal use” must still adhere to all university policies, and must never have an adverse impact on the use of technology and information resources in support of the University’s mission. Examples of “adverse impact” are described in the section entitled “Responsibilities” in the Acceptable Use Policy. The respective chief administrator of the Academic Division, Student Services, Human Resources, and Information Services share the responsibility to interpret the Acceptable Use Policy along with existing university policies relating to personal use of computers and to establish procedures to assist them in the investigation and enforcement of these procedures. For example, in accordance with existing university procedures an employee’s supervisor may also decide that personal activities are affecting the abilities of the employee or colleagues to perform job functions and it is their right to ask the employee to
cease those activities. Ultimately, the office of Human Resources will arbitrate disagreements concerning the interpretation of the Acceptable Use Policy relating to non-faculty staff.

Privacy
This policy defines “private” either as physically or technically not accessible to the general public or accessible only through non-obvious password protection or other security schemes designed to limit access to known or identified individuals. Network system logs which may record an individual’s network activity shall be considered private.

Routine Operations
During routine administration SNAs may need to archive or delete privacy user files or messages from the system; for example, this usually is due to physical data storage limits or an individual’s departure from the University. In this situation, it is not necessary for an SNA to read or view user files; all work is done using system utilities, machine to machine. Given that these situations are foreseeable, each organization responsible for a computer or network system on which these actions will take place must define how and when they will occur. Reasonable efforts must then be made to ensure that system users understand the policy.

Violations, Investigations and Due Process
Non-routine situations may occur where it is necessary to examine a user’s private files without being able to obtain his/her specific permission or authorization. Such situations may include the investigation of violations of this policy or other University policies. The intent of these procedures is to separate the authority to read private user files or messages from the technical ability to do so. This separation attempts to protect both the user and the SNA.

1. Scope. The procedures outlined in this section shall apply to the investigation of University policy violations, including violations of the Acceptable Use Policy, which involve University computing resources or which require access to the private computer activities or files of students or faculty.

2. Reporting of complaints. Any member of the University community may bring a complaint of unacceptable use of computing resources. It is also conceivable that individuals or agencies outside the University may bring such complaints. Complaints shall be brought to the Vice President for Information Services or his/her designee who will be responsible for coordinating the presentation of complaints to the “appropriate chief administrator” as follows:

A. The Vice President for Information Services is charged with making judgments of whether a given activity, use, or publication involving Fairfield University computing resources (including but not limited to the use of the campus network and internet gateway, use of servers-e-mail, web, file, mainframes, etc.-desktop computers, public terminals, etc.) requires further investigation and/or referral to the appropriate chief administrator.

B. For alleged violations of the AUP by faculty members or by students engaged in academic work, complaints that merit investigation will be referred to the Academic Vice President. Before any action is taken the Academic Vice President will refer the matter to an Acceptable Use Policy Committee (AUPC) composed of two tenured faculty appointed by the Educational Technologies Committee and one tenured faculty appointed by the Academic Vice President to investigate and make a recommendation.

C. Students whose conduct is alleged to violate the AUP may appeal to the Academic Vice President on the grounds that their activity is course related and within the scope of academic freedom. The Academic Vice President will refer the matter to AUPC. Student activities that are related to course work and found in violation of the AUP may be sanctioned by the Academic Vice President and the matter referred back to the Vice President of Student Services.
D. For Non-Academic Violations the Vice President for Information Services may make recommendations regarding suspension of computer privileges or other punitive or remedial action to the respective chief administrator.

For the disposition of computing privileges, the due process procedures outlined in this document shall be sufficient, on the authority of the appropriate chief administrator, to revoke or limit computing privileges of an individual found in violation of acceptable use. However, this policy does not limit any further disciplinary action the appropriate chief administrator may seek to bring according to established disciplinary procedures for faculty, staff and students.

3. Authorization for Investigative Action. This policy makes a distinction between electronic files and activities that take place on common University computing equipment (file and e-mail servers, the network and internet gateway) and files and activities that take place on a personal computer belonging to or assigned to an individual. Private electronic files that reside on, or activities that take place on, common University computing equipment (file servers, etc.) and private computing activities that take place over the University network and internet gateway are covered by this policy and may be searched according to the procedures set out in Sections 3a and 3b below. Electronic files residing on personal computers belonging or assigned to individuals may only be searched according to the procedures set forth in Section 3b below. Electronic files that have been made publicly available (that is, not protected through the use of non-obvious passwords or other security measures), either on common University file server equipment or through the use of “sharing” or other forms of file server programs on equipment owned by or assigned to a user are not considered private according to this policy. Computing equipment that resides off campus is not covered under this policy, though all activity of such equipment by authorized Fairfield users that takes place through the University network and computing systems is covered by this policy.

a. Searching private computer files or monitoring electronic activities that do not violate the Acceptable Use Policy. Situations may arise in which the conduct of a computer user is under investigation for violations of other University policies. In such cases, authorization to access private electronic files or monitor electronic activity must be made in writing by the appropriate chief administrator to the Vice President for Information Resources and Services, who in turn must authorize the System or Network Administrator (SNA) in writing to perform the requested search. Any attempt to access private electronic files or other private electronic activities must conform to all applicable operating procedures of the University.

b. Searching faculty offices and student dorm room. Different policies govern the privacy of student dorm rooms and faculty office space:

i) Student Dorm Rooms and Personal Computers Owned by Students. Under the authority of the Room Entry and Room Search sections of the Student Handbook (pp. 118-119), the Vice President of Student Services may authorize that a search be conducted on a personal computer. Entry to the student room shall be conducted in accordance with the Room Entry and Room Search clauses in the Student Handbook. The SNA may be authorized to assist the staff of student services by accompanying them and conducting the search of student computer in accordance with Section 4a of this policy.

ii) Faculty Desktop Computers. This policy recognizes that files stored on a desktop computer are part of the faculty office, unless made publicly available (i.e., not password protected) through networking programs such as file sharing, web, or other such server software. Entry to a faculty desktop computer shall occur only when authorized by the Academic Vice President, in accordance with existing policies.

All users of computing resources at the University should be aware that this policy does not limit any applicable State and Federal search and seizure procedures.
4. Emergency Situations. Situations will occur that pose immediate threats to the operations or security of computer or network systems. Because of the immediacy, the SNA will need to intervene without obtaining the written permission usually required before taking actions that may affect user files, messages or system access privileges. The intent of these procedures is to allow SNAs to take appropriate, timely action when protecting University computer systems while ensuring that the user and appropriate University officials will be made aware of the situation as soon as possible.

a. If an SNA determines that user files or messages pose a significant threat to the operation or security of a University computer or network system, he or she will take appropriate action to correct the problem only upon the authorization of the Vice President for Information Services. If the Vice President for Information Services is not available, the SNA may take such action as is necessary to resolve the emergency. Such action may include, but is not limited to disabling user privileges, deleting or disabling a user file, or disconnecting a network connection. SNAs are not authorized to enter a private office or dorm room on an emergency basis, but may temporarily disable network connections until proper authorization is obtained to inspect computing equipment in these areas. The SNA will not perform any action on user files or messages that are not relevant to the current problem and will not take any technical action, a this point, that would permanently deprive the user of access to the computer or network system.

b. As soon as possible after action is taken, but no later than the next business day, the SNA will make a written report to the Vice President for Information Services and the appropriate chief administrator outlining the nature of the threat; protective actions taken; the user(s) involved; and the user file or messages that were affected.

5. Sanctions. For nonacademic violations the appropriate chief administrator will review the recommendations of the Vice President for Information Services and make the final decision concerning any penalty or sanctions to be imposed on the offending party. Under this policy, those sanctions or penalties may consist of limitation or suspension of any or all computing privileges. Imposition of such penalties does not preclude further disciplinary action according to established policies for faculty, students and staff.

Guidelines for Systems and Network Administrators. Computer systems and network administrators (SNA’s), by the nature of their work, have privileges and responsibilities that other users of technology generally do not have. Without system privileges, SNAs would not be able to do their jobs. The use of these privileges must be wise and thoughtful. These guidelines were developed to articulate responsibilities SNAs have in addition to those outlined in Fairfield University’s Acceptable Use Policy.

1. SNAs are bound by the Acceptable Use Policy and the procedures set forth in Sections I and II of this policy. Further, SNAs have a responsibility to educate users about all applicable computing policies.
2. All SNAs have an additional responsibility to assure the operation, security and integrity of Fairfield University's computers, networks, and data.
3. Consistent with the other obligations imposed on them under the Acceptable Use Policy, other applicable University policies, and the law, SNAs will treat as confidential any private and/or confidential information obtained during system administration.
4. SNAs must not disclose privileged and confidential information about Fairfield University’s systems or any other information that could prove detrimental to operations or compromise system security.
5. It is against University policy for an SNA to read a user’s files. However, SNAs in the course of routine system administration, may need to delete or archive user files or messages. In order to do this, SNAs must first promulgate a clear policy to the users describing how and when delete or archive actions
will be taken. These policies may vary by department. This section does not, however, grant SNAs authority to read user files or messages during routine system administration. Procedures for obtaining authorization to read user files or messages in routine, non-emergency and emergency situations are provided in Section II of this policy.

6. When reacting to or preventing actions by users that may violate the Acceptable Use Policy or other actions by users that may have significantly detrimental effects on system or network operation, SNAs may need to read, modify or delete user files or messages. These actions will take place in accordance with the procedures outlined in this policy and the SNA will document any access to user files or messages.

7. SNAs will take all practical measures to ensure that all hardware and software license agreements are faithfully executed on all systems, network, servers, and computers for which he or she has responsibility.

Violations of these Guidelines for SNAs will be handled following the administrative and disciplinary processes outlined in the applicable operating policies and procedures of the University.
Appendix IV:

Fairfield University Computer Systems Acceptable Use Policy (AUP 2004)

Fairfield University Computer Systems Acceptable Use Policy

November 13, 2000,
Updated June 30, 2004

This policy is designed to guide students, faculty, staff, and other authorized users in the acceptable use of computer and information systems and networks provided by Fairfield University according to the mission of the University. It is meant as an application of the principles of respect and reverence for every person, the development of community and the ideals of liberal education that are at the core of Fairfield's Catholic, Jesuit identity. This policy supersedes the "Acceptable Use Policy" (number 610) adopted 1/1/94. This policy does not supersede any other University policies, including those pertaining to student grievances, sexual harassment, and personal conduct (Policy No. 480, Item #27).

Guiding Principles:

The Fairfield University community is encouraged to make innovative and creative use of information technologies in support of education and research. Access to information representing a multitude of views on current and historical issues should be allowed for the interest, information and enlightenment of the University community. Consistent with other University policies, this policy is intended to respect the rights and obligations of Academic Freedom, and recognizes that the educational mission of the University is served in a variety of ways.

The University recognizes that the purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorized use or sale of works available in the private sector. Publication, distribution, or broadcast of copyright protected materials without permission is prohibited. Also consistent with other University policies, an individual's right of access to computer materials should not be denied or abridged because of race, creed, color, age, national origin, gender, sexual orientation, or disability.

The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be recipients of material they find offensive. Those who use e-mail and/or make information about themselves available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information.

In the interests of promoting the free exchange of ideas, Fairfield University does not exercise prior review of electronic documents available on its network and accessible locally or through the internet. Individuals who access materials available on the Fairfield University network should understand that these materials, unless otherwise posted, do not necessarily reflect the views of Fairfield University. Individuals who feel that particular materials posted on the Fairfield University network are inappropriate or otherwise objectionable, may lodge a formal complaint through the office of Computing and Network Services.
Fairfield University computing and network resources are to be used for University-related research, instruction, learning, enrichment, dissemination of scholarly information, and administrative activities. The computing and network facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. Computers and network systems offer powerful tools for communication among members of the community and of communities outside the University. When used appropriately, these tools can enhance dialog and communication. When used unlawfully or inappropriately, however, these tools can infringe on the rights of others.

Responsibilities:

The following examples, though not covering every situation, specify some of the responsibilities that accompany computer use at Fairfield and/or on networks to which Fairfield is connected.

1. Users may not attempt to modify the University system or network facilities or attempt to crash systems. They should not tamper with any software protections or restrictions placed on computer applications or files.

2. All users must obtain authorized computing accounts and may only use their own user names and passwords to access University computing and network systems. Users may not supply false or misleading data nor improperly obtain another's password in order to gain access to computers or network systems, data or information. The negligence or naiveté of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Users should not attempt to subvert the restrictions associated with their computer accounts.

3. Users are responsible for all use of their computer account(s). They should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources. Individual password security is the responsibility of each user.

4. Users may not encroach on others' use of computer resources. Such activities would include, but are not limited to, tying up computer resources for excessive game playing or other trivial applications; sending harassing messages; sending frivolous or excessive messages, including chain letters, junk mail, and other types of broadcast messages, either locally or over the Internet; using excessive amounts of storage (as determined by Computing and Network Services policies); intentionally introducing any computer viruses, worms, Trojan Horses, or other rogue programs to Fairfield University hardware or software; physically damaging systems; or running grossly inefficient programs when efficient ones are available.

5. Users are responsible for making use of software and electronic materials in accordance with copyright and licensing restrictions and applicable university policies. Fairfield University equipment and software may not be used to violate copyright or the terms of any license agreement. No one may inspect, modify, distribute, or copy proprietary data, directories, programs, files, disks or other software without proper authorization.

6. Users must remember that information distributed through the University's computing and networking facilities is a form of publishing, and some of the same standards apply. For example, anything generated at Fairfield that is available on the Internet through the University's network represents the University and not just an individual. Even with disclaimers, the University is represented by its students, faculty and staff, and appropriate content, language and behavior is warranted.

7. Users may not transmit any material that is unlawful, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any federal, state, or
local laws. Materials made available or transmitted on University Computer systems must comply
with all University policies governing conduct of students, faculty and staff.

Administration:

The University encourages all members of its community to use electronic communications in a manner
that is respectful to others. While respecting users' confidentiality and privacy, the University reserves the
right to examine computer files and monitor electronic activity within the limits of other applicable
University policies. The University may exercise this right in order to enforce its policies regarding
harassment and the safety of individuals; to prevent the posting of proprietary software or electronic copies
of electronic texts or images in disregard of copyright restrictions or contractual obligations; to safeguard
the integrity of computers, networks, and data either at the University or elsewhere; and to protect the
University against seriously damaging consequences. The University may restrict the use of its computers
and network systems for electronic communications when faced with evidence of violation of University
policies, or federal, state or local laws. The University reserves the right to limit access to its networks
through University-owned or other computers, and to remove or limit access to material posted on
University-owned computers.

All users are expected to conduct themselves consistent with these responsibilities and all other applicable
University policies. Abuse of computing privileges will subject the user to disciplinary action according to
established University procedures. Abuse of networks or computers at other sites through the use of
Fairfield University resources will be treated as an abuse of computing privileges at the University. When
appropriate, temporary restrictive actions will be taken by system or network administrators pending further
disciplinary action; the loss of computing privileges may result.

The University and users recognize that all members of the University community are bound by federal,
state and local laws relating to civil rights, harassment, copyright, security and other statutes relating to
electronic media. It should be understood that this policy does not preclude enforcement under the laws
and regulations of the United States of America nor the State of Connecticut.

This policy may be amended or changed by the University Vice-Presidents, and in matters affecting the
Academic Division, with the mutual consent of the Academic Council.

© 2011 All Rights Reserved | Fairfield University, 1073 North Benson Road, Fairfield, Connecticut 06824
| (203) 254-4000
Appendix V:


---

Procedures in Support of Fairfield University's Computer Systems Acceptable Use Policy

These procedures have been designated to complement rather than supercede existing University procedures, guidelines, and policies relating to computer use by faculty, staff and students. For this reason, final authority for the resolution of complaints, including any penalties rests with the appropriate chief administrator.

For the purposes of this policy, "appropriate chief administrator" shall be defined as the senior administrator who has jurisdiction over the alleged offender of the Fairfield University Computer Systems Acceptable Use Policy (hereafter cited as the "Acceptable Use Policy"). The "appropriate Chief administrator" for faculty is the Academic Vice President. The "appropriate chief administrator" for students will either be the Academic Vice President if the offense is related to academics, or the Vice President for Student Affairs in non-academic affairs. In circumstances where the jurisdictional lines are not clearly demarcated, authority will rest with both Vice Presidents, disputes being resolved by the President.

In the case of non-faculty staff, the Associate Vice President of Human Resources is the chief administrator.

Guiding Principles

These procedures were designed to balance seven interests:

- respecting the rights and responsibilities of academic freedom as defined in applicable policies for faculty, and students engaged in academic work;
- protecting the rights of the university;
- protecting users' privacy;
- protecting the System or network Administrator (SNA) in the performance of his or her job;
- allowing routine administrative actions that might affect users' files;
- providing a mechanism to allow non-routine, non-emergency access to users' files when it can be justified;
- providing guidelines for the occasional need to take immediate action. The ability of an SNA to read a user's files does not imply that he or she may do so without obtaining the approval required by these procedures.

Balancing Rights

"Incidental personal use" of computing systems is an accepted and appropriate benefit of being associated with Fairfield University. However, "incidental personal use" must still adhere to all university policies, and must never have an adverse impact on the use of technology and information resources in support of the University's mission. Examples of "adverse impact" are described in the section entitled "Responsibilities" in the Acceptable Use Policy. The respective chief administrator of the Academic Division, Student Services, and Human Resources share the responsibility to interpret the Acceptable Use Policy along with existing university policies relating to personal use of computers and to establish procedures to assist them in the investigation and enforcement of these procedures. For example, in accordance with existing university
procedures an employee's supervisor may also decide that personal activities are affecting the abilities of the employee or colleagues to perform job functions and it is their right to ask the employee to cease those activities. Ultimately, the Office of Human Resources will arbitrate disagreements concerning the interpretation of the Acceptable Use Policy relating to non-faculty staff.

Privacy

This policy defines "private" either as physically or technically not accessible to the general public or accessible only through non-obvious password protection or other security schemes designed to limit access to known or identified individuals. Network system logs which may record an individual's network activity shall be considered private.

Routine Operations

During routine administration SNAs may need to archive or delete privacy user files or messages from the system; for example, this usually is due to physical data storage limits or an individual's departure from the University. In this situation, it is not necessary for an SNA to read or view user files; all work is done using system utilities, machine to machine. Given that these situations are foreseeable, each organization responsible for a computer or network system on which these actions will take place must define how and when they will occur. Reasonable efforts must then be made to ensure that system users understand the policy.

Violations, Investigations and Due Process

Non-routine situations may occur where it is necessary to examine a user's private files without being able to obtain his/her specific permission or authorization. Such situations may include the investigation of violations of this policy or other University policies. The intent of these procedures is to separate the authority to read private user files or messages from the technical ability to do so. This separation attempts to protect both the user and the SNA.

Scope

- The procedures outlined in this section shall apply to the investigation of University policy violations, including violations of the Acceptable Use Policy, which involve University computing resources or which require access to the private computer activities or files of students or faculty.
- Reporting of complaints
- Any member of the University community may bring a complaint of unacceptable use of computing resources. It is also conceivable that individuals or agencies outside the University may bring such complaints. Complaints shall be brought to the Director of Computing & Network Services or his/her designee who will be responsible for coordinating the presentation of complaints to the "appropriate chief administrator" as follows:
  - A. The Director of Computing & Network Services is charged with making judgments of whether a given activity, use, or publication involving Fairfield University computing resources (including but not limited to the use of the campus network and internet gateway, use of servers-e-mail, web, file, mainframes, etc.-desktop computers, public terminals, etc.) requires further investigation and/or referral to the appropriate chief administrator.
  - B. For alleged violations of the AUP by faculty members or by students engaged in academic work, complaints that merit investigation will be referred to the Academic Vice President. Before any
action is taken the Academic Vice President will refer the matter to an Acceptable Use Policy Committee (AUPC) composed of two tenured faculty appointed by the Educational Technologies Committee and one tenured faculty appointed by the Academic Vice President to investigate and make a recommendation.

- C. Students whose conduct is alleged to violate the AUP may appeal to the Academic Vice President on the grounds that their activity is course related and within the scope of academic freedom. The Academic Vice President will refer the matter to AUPC. Student activities that are related to course work and found in violation of the AUP may be sanctioned by the Academic Vice President and the matter referred back to the Vice President of Student Affairs.

- D. For Non-Academic Violations the Director of Computing & Network Services may make recommendations regarding suspension of computer privileges or other punitive or remedial action to the respective chief administrator.

- For the disposition of computing privileges, the due process procedures outlined in this document shall be sufficient, on the authority of the appropriate chief administrator, to revoke or limit computing privileges of an individual found in violation of acceptable use. However, this policy does not limit any further disciplinary action the appropriate chief administrator may seek to bring according to established disciplinary procedures for faculty, staff and students.

Authorization for Investigative Action

This policy makes a distinction between electronic files and activities that take place on common University computing equipment (file and e-mail servers, the network and internet gateway) and files and activities that take place on a personal computer belonging to or assigned to an individual. Private electronic files that reside on, or activities that take place on, common University computing equipment (file servers, etc.) and private computing activities that take place over the University network and internet gateway are covered by this policy and may be searched according to the procedures set out in Sections 3a and 3b below. Electronic files residing on personal computers belonging or assigned to individuals may only be searched according to the procedures set forth in Section 3b below. Electronic files that have been made publicly available (that is, not protected through the use of non-obvious passwords or other security measures), either on common University file server equipment or through the use of "sharing" or other forms of file server programs on equipment owned by or assigned to a user are not considered private according to this policy. Computing equipment that resides off campus is not covered under this policy, though all activity of such equipment by authorized Fairfield users that takes place through the University network and computing systems is covered by this policy.

- a. Searching private computer files or monitoring electronic activities that do not violate the Acceptable Use Policy. Situations may arise in which the conduct of a computer user is under investigation for violations of other University policies. In such cases, authorization to access private electronic files or monitor electronic activity must be made in writing by the appropriate chief administrator to the Director of Computing & Network Services, who in turn must authorize the System or Network Administrator (SNA) in writing to perform the requested search. Any attempt to access private electronic files or other private electronic activities must conform to all applicable operating procedures of the University.

- b. Searching faculty offices and student dorm room. Different policies govern the privacy of student dorm rooms and faculty office space:

  - i) Student Dorm Rooms and Personal Computers Owned by Students. Under the authority of the Room Entry and Room Search sections of the Student Handbook, the Vice President of Student Affairs may authorize that a search be conducted on a personal computer. Entry to the student
room shall be conducted in accordance with the Room Entry and Room Search clauses in the
Student Handbook. The SNA may be authorized to assist the staff of student services by
accompanying them and conducting the search of student computer in accordance with Section 4a
of this policy.

• ii) Faculty Desktop Computers. This policy recognizes that files stored on a desktop computer are
part of the faculty office, unless made publicly available (i.e., not password protected) through
networking programs such as file sharing, web, or other such server software. Entry to a faculty
desktop computer shall occur only when authorized by the Academic Vice President, in accordance
with existing policies.

All users of computing resources at the University should be aware that this policy does not limit any
applicable State and Federal search and seizure procedures.

Emergency Situations. Situations will occur that pose immediate threats to the operations or security of
computer or network systems. Because of the immediacy, the SNA will need to intervene without obtaining
the written permission usually required before taking actions that may affect user files, messages or system
access privileges. The intent of these procedures is to allow SNAs to take appropriate, timely action when
protecting University computer systems while ensuring that the user and appropriate University officials
will be made aware of the situation as soon as possible.

• a. If an SNA determines that user files or messages pose a significant threat to the operation or
security of a University computer or network system, he or she will take appropriate action to
correct the problem only upon the authorization of the Vice President for Information Services. If
the Director of Computing & Network Services is not available, the SNA may take such action as is
necessary to resolve the emergency. Such action may include, but is not limited to disabling user
privileges, deleting or disabling a user file, or disconnecting a network connection. SNAs are not
authorized to enter a private office or dorm room on an emergency basis, but may temporarily
disable network connections until proper authorization is obtained to inspect computing
equipment in these areas. The SNA will not perform any action on user files or messages that are
not relevant to the current problem and will not take any technical action, at this point, that would
permanently deprive the user of access to the computer or network system.

• b. As soon as possible after action is taken, but no later than the next business day, the SNA will
make a written report to the Director of Computing & Network Services and the appropriate chief
administrator outlining the nature of the threat; protective actions taken; the user(s) involved; and
the user file or messages that were affected.

Sanctions. For nonacademic violations the appropriate chief administrator will review the
recommendations of the Director of Computing & Network Services and make the final decision
concerning any penalty or sanctions to be imposed on the offending party. Under this policy, those
sanctions or penalties may consist of limitation or suspension of any or all computing privileges. Imposition
of such penalties does not preclude further disciplinary action according to established policies for faculty,
students and staff.

Guidelines for Systems and Network Administrators

Computer systems and network administrators (SNAs), by the nature of their work, have privileges and
responsibilities that other users of technology generally do not have. Without system privileges, SNAs
would not be able to do their jobs. The use of these privileges must be wise and thoughtful. These
guidelines were developed to articulate responsibilities SNAs have in addition to those outlined in Fairfield University's Acceptable Use Policy.

1. SNAs are bound by the Acceptable Use Policy and the procedures set forth in Sections I and II of this policy. Further, SNAs have a responsibility to educate users about all applicable computing policies.
2. All SNAs have an additional responsibility to assure the operation, security and integrity of Fairfield University's computers, networks, and data.
3. Consistent with the other obligations imposed on them under the Acceptable Use Policy, other applicable University policies, and the law, SNAs will treat as confidential any private and/or confidential information obtained during system administration.
4. SNAs must not disclose privileged and confidential information about Fairfield University's systems or any other information that could prove detrimental to operations or compromise system security.
5. It is against University policy for an SNA to read a user's files. However, SNAs in the course of routine system administration, may need to delete or archive user files or messages. In order to do this, SNAs must first promulgate a clear policy to the users describing how and when delete or archive actions will be taken. These policies may vary by department. This section does not, however, grant SNAs authority to read user files or messages during routine system administration. Procedures for obtaining authorization to read user files or messages in routine, non-emergency and emergency situations are provided in Section II of this policy.
6. When reacting to or preventing actions by users that may violate the Acceptable Use Policy or other actions by users that may have significantly detrimental effects on system or network operation, SNAs may need to read, modify or delete user files or messages. These actions will take place in accordance with the procedures outlined in this policy and the SNA will document any access to user files or messages.
7. SNAs will take all practical measures to ensure that all hardware and software license agreements are faithfully executed on all systems, network, servers, and computers for which he or she has responsibility.

Violations of these Guidelines for SNAs will be handled following the administrative and disciplinary processes outlined in the applicable operating policies and procedures of the University.

© 2011 All Rights Reserved | Fairfield University, 1073 North Benson Road, Fairfield, Connecticut 06824 | (203) 254-4000