ABSTRACT
Instances of misuse and misbehavior in our electronic communities are on the rise. The panel will address some of the current policy issues facing our campuses and talk about how our varying organizational structures deal with these instances.

Keywords
Abuse, misuse, misbehavior, electronic community, policies practices.

1. INTRODUCTION
It seems that every campus is experiencing a growth in the misuse of their computer systems, either by people within their community or by those outside it who hack into systems and then use the systems for their own purposes. The ever-changing populations that colleges and universities experience is becoming more computer literate as a whole, which means that misbehavior by individuals within the institutions also seems to rise, despite our best efforts to educate them as to our standards.

The panel members will present an overview of how abuse situations within the electronic community are handled at their schools and also talk briefly about the hot topics on their campuses. We will then open the floor to a general question, answer and discussion time.

2. PANEL MEMBERS
As we talked at the lunch table for those interested in abuse issues at SIGUCCS 1999 in Denver, we found that the abuse issues that we faced often differed with the size of our schools and that how we handled issues varied most greatly with the public vs. private split though somewhat with geographical location, too. We talked at that table about doing a presentation on the various abuse issues our schools face and what methods we use to address them. Hence, as we considered who would collaborate for this panel, we chose a mid-sized east coast school, a small, private mid-west school, a large public west coast school and a small, private west coast school.

2.1 University of Virginia
The University of Virginia (U.Va.) is an east-coast, public institution that has a student body of about 18,000 undergraduate and graduate students and 10,000 faculty and staff.

At U.Va., instances of misuse/misbehavior within the electronic community are reported to an email address: abuse@Virginia.edu. abuse@Virginia.edu is a mailing list for a group of people within the U.Va. community who deal with these reports. While some of us on the team are not involved in development and/or enforcement of policies nor in judgments on behavior, others on the team have these responsibilities. The team acts as an initial point of contact to receive reports of misbehavior or misuse, acknowledges the reports that we receive and, when needed, directs the reports to the appropriate University department for further action, provides investigatory services, and works to protect the integrity of our systems and the systems of others. We try to avoid creating new policy or procedures, and we encourage those with whom we coordinate to use existing guidelines, standards of conduct, and procedures when they deal with a report from us.
In addition to the normal, now almost run-of-the-mill abuse situations, U.Va. had two situations in late spring that gave us pause. In the first situation, we had a department within our Health System request the alias clintrials@Virginia.edu as an administrative address. We assigned the alias and were then notified by an attorney that the company he represented considered our email alias address a potential source of confusion for his clients who hold a U.S. registered trademark for the name “clintrials.” We checked the online database for U.S. registered trademarks and “clintrials” is registered. Postmaster and webmaster are also registered trademarks. Do we remove the alias? Modify it in some way? Go to court for the right to keep it? The attorneys have this situation in hand at present. In the second situation, we have department systems connected to our network that are, by our investigations, insecure. Requests to the people responsible for these systems to bring their system to a current level of security sometimes results in no change. Can we force these systems to be secured? How? Can we just disconnect them from the network? What happens if the system provides a critical aspect of patient care and is insecure: can a hacker take over a system and harm a patient? We are beginning to try to resolve this type of situation with a University-wide committee.

### 2.2 University of California, Berkeley: A Distributed Environment

The University of California, Berkeley is a west coast, public institution that has a student body of about 23,000 undergraduate and graduate students and 11,500 staff.

At the University of California at Berkeley, computing services are provided through many independent jurisdictions over which the central organization, Information Systems and Technology (IST), does not have authority. IST supports a large number of student computer laboratories providing many hundred seats. Larger access offering is provided through residence halls, many departmental microcomputing facilities or laboratories as well as individual offices that comprise the 40,000 nodes that make up the campus network. Consequently, many individuals gain access to computing through a multitude of access points that may or may not have governing policy statements that encourage good citizenship on the network.

In the midst of this distributed environment, IST offers a Policy Services Office (PSO) (http://socrates:7015/), which has become the primary resource point for departments to report or discuss issues ranging from inappropriate use and security breaches to questions of legal activity. The PSO has taken the lead in offering consulting assistance to campus departmental computing services groups in order to ensure consistent response to reports of violation of policy or law.

Issues brought to the attention of the PSO range from complaints of unsolicited email (spam in many forms), abuse or harassing email, and copyright complaints, most particularly warnings for the RIAA regarding MP3 servers. The PSO accomplishes its work through its well established functional relationships with campus offices whose role it is to manage or adjudicate issues of inappropriate use of University resources: the Student Conduct Office, Residence Hall Judicial Affairs, Personnel Employment Analysts, Campus Police or Campus Legal Counsel.

The last two years have seen innumerable reports of MP3 violations and complaints of unsolicited email. Residence Hall use of Napster presented a significant challenge to bandwidth services. The campus administration has recently initiated an effort for management of official email announcements to the campus community. Additionally, a new initiative is underway to address a variety of policy issues relating to conducting the business of the campus on the Internet. These are some representative examples of the issues facing the PSO group today.

### 2.3 Reed College

Reed College is a private liberal arts college located in Oregon with a student population of about 1,400. The student–faculty ratio is 10:1.

At Reed, the sources of the abuse problems tend to originate primarily with students (on-campus situations) and from off-campus. The types of problems seen are typically the following:

- spams and other mass mailings (Senior Breakfast spam),
- harassment,
- piracy (hotline),
- complaints about students (unicorn and house of GORD), and
- privacy (.newsrc).

Solutions to these problems usually fall into one of three types:

- policy guidelines and the honor principle,
- cut them off, and
- education.

### 2.4 Oberlin College

Oberlin College is a private school located in Ohio, comprised of a College of Arts and Sciences and a Conservatory of Music, with a total student population of about 2,900.

Oberlin College’s Center for Information Technology (CIT) handles instances of electronic abuse/misuse with a small internal team, mainly consisting of the Director of Client Services, the Systems Manager, and the Networking Manager. Other staff members may be called in as the situation warrants. The Systems Manager maintains a constant vigil over the servers and systems and continuously monitors Postmaster email, checking for signs of abuse/misuse (such as mass mailings). The Network Manager assists in defining which computer was used for suspect situations and ensures port scans are done. He also calls upon his staff to have suspect computers placed into our “Black Hole”, a VLAN where the user has no access external to/from the campus. Users remain in this VLAN until the situation is resolved to our satisfaction (i.e., verification occurs that the user is not creating a security risk for the College’s computing environment.) The Director of Client Services confronts the user after all facts are obtained in order to
resolve the situation. Review of lab video surveillance tapes may be warranted to help define abusers. The Director of Client Services generally decides what follow-up action is required: discussion with user, education of user, formal complaint to the student Judicial Board, etc. We try to handle every situation at the lowest level possible and find that most instances can be linked to lack of knowledge.

Additionally, reports of abuse/misuse are sent to an email address, Client.Services@oberlin.edu, which is read by the Director of Client Services, or they are reported directly to that individual. These reports usually involve harassing email or misrepresentation of email addresses, and are brought to CIT’s attention by the recipient of the email or by campus Security personnel, who have been notified by the recipient. Harassing email often comes to an Oberlin client from an external address. Our Systems Manager notifies the external source in an attempt to resolve the situation (e.g., abuse@yahoo.com.) We often can link an external address to a specific Oberlin computer by tracking systems logs. In that case, confrontation with the sender is conducted by the Director of Client Services and follow-up action is taken, as warranted.

We make every effort to maintain our overarching “General Policies for the Use of Information Technology” at a minimal-directive or detailed posture. We believe it is impossible to cover every possible circumstance and do not desire to be in the position of producing continuous modifications to meet ever-changing circumstances. This past year, we added verbiage pertaining to mp3 files in order to ensure that users understand U.S. Copyright Law also affects most mp3 files. For the next academic year, we will add information on the process required to have a server in one’s dorm room.

Instances of abuse and/or misuse during the 1999-2000 academic year consisted of the following:

- mass emailings (forbidden by our policy),
- harassing email from one individual to another,
- use of another individual’s email address as the sender of a harassing email,
- use of fake email address as the sender of a mass email,
- conducting of a port scan on our DNS server,
- attempting shell access to our mail server (forbidden),
- “stuffing” of an online ballot,
- having an ftp server in one’s dorm room,
- using commercial banner ads,
- serving mp3 files, and
- setting up lab computers with a commercial, profit-making view-bar.

3. Conclusion

While our institutions may be larger than, smaller than or the same as yours, while our geographic locations may vary, while our approaches to managing the situations we encounter may vary, we find that we have commonality in issues we encounter and look forward to the opportunity to discuss them with each other and with you.