

COMPUTER SCIENCE DEPARTMENT POLICY

The CS Dept systems staff is very capable and experienced, and very willing to help you to achieve your primary goal: attainment of a graduate degree at U.Va. You will find the systems staff a very amiable and supportive group. To help all of you achieve your goals, the following guidelines and related practices for using departmental, and by extension, University computing equipment must be observed. Conformance with these guidelines and practices maximizes the chances of success for all of us. Please read this policy document carefully and sign the attached form acknowledging that you have read, understood, and intend to adhere to these guidelines.

Most of the department resources are shared; the behavior of any individual user has an impact on other users. Common courtesy and consideration are essential to maintaining a pleasant and productive environment for all of us. Since resources are not unlimited, their use should be limited to the purposes for which they were purchased; use for inappropriate activities takes resources away from others who may need them for their work, and is inconsiderate. The integrity of data, processes and privacy of others should always be respected.

I. Guidelines:

- A. Considerate Use of Resources** (Golden Rule Part I) – Be considerate of others in using department resources; considerate use will result in optimum performance for everyone.
- B. Appropriate Use of Resources** – Accounts are to be used for research, instruction and administrative purposes *only*, in keeping with the University's mission.
- C. Respect for the Privacy of Others** (Golden Rule Part II) – If permissions aren't set for you to view someone else's material, you shouldn't be viewing it. Snooping someone else's email, in particular is a serious violation of privacy.

II. Implications:

The three guidelines above have implications in a number of areas. While the list below is not necessarily exhaustive, it is sufficiently thorough to give you a good idea of the behavior expected of a user. For each of the areas covered, the list includes:

1. What the user should do.
2. What the user should NOT do.
3. What actions the systems staff will take if the use of the resource(s) discussed is not in keeping with expectations.

Systems staff will act only to preserve conformance with the guidelines. **Serious infractions may involve departmental actions beyond system staff responses, up to and including dismissal from the graduate program.**

A. Computer Account Usage

1. **DO:** CS users should use only their own personal account, with only one exception – they may use a “role” account which has been created for some specific function or purpose while they are acting in that capacity. Role accounts may be for teaching (TA) or research (group accounts) purposes.
2. **DO NOT:** CS users should never use another user’s personal account nor share their account under any circumstances. There is never any legitimate reason to do this. If a user needs access to some data in another user’s account and for some reason are not able to obtain access from that individual, they should approach system staff with the problem.
3. **Staff Response:** Depending on the nature of the infraction, your account may be deactivated or revoked. If an honor violation has occurred it will be reported to the proper student authorities.

B. Computer System Usage:

1. **DO:** Systems are to be used for the purposes for which they were set up – a number of systems have been set up for specific purposes: interactive/login servers, compute servers, file servers, HTTP servers, Mail servers, FTP, etc. Similarly, the general mission of the university is research and teaching – all of these systems have been provided for those purposes, including individual workstations.
2. **DO NOT:** Users should not start long running, CPU-intensive compute jobs on interactive servers. Systems should not be used as multimedia entertainment centers.
3. **Staff Response:** System Administrators will respond to complaints about inappropriate jobs on shared systems by killing those jobs. The user will be asked to delete repositories of multimedia (MP3, MPEG, and JPEG) files. You may lose your account or network privileges.

C. Network Usage:

The university owns the network, and it is a shared resource in the purest sense. We have a generally good infrastructure within the department, but we pay for and share a single uplink. All traffic on the network has a real and immediate impact on other users.

1. **DO:** Network Policies to follow:

- a. Bandwidth is a limited and precious resource, and it should only be used for research and teaching purposes. Consideration for others is absolutely essential here.
 - b. *Addendum (01/26/2006)*: The use of personal NAT/Internet Sharing/Wireless AP/Router Devices is strictly prohibited unless specifically approved by the Systems Staff. Any and all networking devices must be registered before being used within the Department.
2. **DO NOT:** Other uses, notably file-sharing and streaming media, generally do not meet the guidelines for legitimate academic activities. In the cases where they do, the department provides the appropriate infrastructure. Sharing out MP3, MPEG and other media repositories is not permitted, nor is downloading them.
 3. **Staff Response:** Users who abuse the network will likely find their access revoked, regardless of whether the device connected is owned by the university or the user.

D. File system Usage

File system quotas are not currently applied, although there is clearly not an unlimited amount of space on any file system. There are very real and high costs associated with reliable storage (RAID and backup).

1. **DO:** A user should, “use what they need, but need what they use.” Storage should only be used for legitimate academic purposes. Users should take into account free space on their file system before writing large files to the system which might eliminate the free space other users are counting on. The privacy and integrity of data stored on the department’s systems must also be absolutely respected.
2. **DO NOT:** A user should not assume they have infinite storage. Accounts are in shared partitions. Check occasionally to ensure there’s room for what you need to store. Users should never access or modify another user’s data unless that user has made the data public or granted you access to the data.
3. **Staff Response:** The top twenty users on a full (>95%) file system will be published in a weekly email to other users of that file system, and they will be asked delete or compress their data. Accessing or modifying another user’s data without permission may be considered an honor violation.

E. Mail System Usage

The department maintains its own mail server for the convenience of its users, which, unlike the university’s central mail server, does not place quotas on the size of mail messages or the amount of stored mail. A list server is also provided. Mail is backed

up, and logs of mail transactions are available through systems staff. Users should be able to communicate using email as they need.

1. **DO:** Use the mail system with care. Watch the size of attachments. Be aware of alternatives such as FTP and HTTP for transferring large attachments.
2. **DO NOT:** E-mail should not be used to send SPAM, forged mail, commercial messages, or as a means of threatening or harassing anyone. Although there are not quotas on message sizes, email should not be used as FTP. The privacy of other users' mail must be respected; under no circumstances should a user read another's email without express permission to do so.
3. **Staff Response:** The university takes very seriously email abuse; depending on the nature of the abuse, the response may vary from the deletion of the mail to dismissal from the university. Complaints can be filed with systems staff, and abuse@virginia.edu.

F. Web Server Usage

The department provides a web server for general department usage – users may “publish” from the **public_html** directory in their home directory.

1. **DO:** The nature of the material posted should be in keeping with the mission of the university. Copyright laws must be observed.
2. **DO NOT:** Commercial and obscene material is prohibited; nonuniversity mission material is prohibited (especially mp3s and mpegs)
3. **Staff Response:** Depending on the nature of the abuse, the user may be asked to remove the posting, or it may be removed for them. Users serving up copyrighted material may be reported for copyright violation and subject to criminal prosecution outside the university.

G. “Enterprise” Class Services

Generating large amounts of traffic imposes a real cost on our network (which is paid for by the department) and a real cost on other users who are forced to deal with reduced performance in their legitimate work.

1. **DO:** Be considerate. In general, the department plans for and deploys all “enterprise” class services in a centralized way, or shares them with the University's information services department (ITC). These include file, mail, FTP, HTTP, DNS, etc. services. If a user needs some special customization of these services, they should put a request into systems staff, who will do their best to accommodate that need.

2. **DO NOT:** Users should not run services on any individual or personal workstation connected to the department network (regardless of the ownership of the actual machine running the service). Because they generate even more traffic, and generally do not satisfy a university related mission, file sharing programs like Napster, Gnutella, KaZaA, Morpheus and similar programs are *never* appropriate.
3. **Staff Response:** If any of these services is found on a system you control, you will be told to remove them immediately. If an abuse continues, you will lose your network privileges. Users serving up copyrighted material may be reported for copyright violation and subject to criminal prosecution outside the university.

H. Printing

The department provides a wide variety of printers and paper for your use free of charge. Users can print everything from simple letter size paper to photoquality posters. Like disk space, there are real costs associated with each page. The department currently incurs printing costs that are equivalent to support for three graduate research assistantships for a year.

1. **DO:** “print what you need and need what you print.” Retrieve your jobs promptly. Take care in not sending uninterrupted postscript to the printers.
2. **DO NOT:** Do not print jobs which are not work-related; this includes: posters for your home or office, family photos, fliers for your club, etc. Similarly, you should not continually submit jobs if they do not come out; they will eventually. Do not send PDF files directly to the printer. If a user has problems they should report it immediately to systems staff.
3. **Staff Response:** Abuse of the printer resources may result in the user reimbursing the department for the cost of the jobs.

I. Workstations

The workstation provided at the user’s desk is for that user’s primary use, but belongs to the department. Workstations are distributed throughout the department to achieve as heterogeneous a mixture as possible in each room. As older machines are replaced, the oldest are replaced first.

1. **DO:** Things that can be done with workstations:
 - a. The user may be granted administrative access to their system to facilitate their work.
 - b. As part of sharing resources, a user should be prepared to share their workstation if necessary, and may ask the same of others.

- c. A user may install personal hardware (sound card, extra hard disk) in a department system with staff knowledge beforehand.
 - d. You may install software and customize your system to suit you.
2. **DO NOT:** Things that should not be done with a workstation:
- a. Do not rely on the storage on workstations – they are not backed up, and no efforts are made at recovery of data in the event of a failure. Data the user cares about should be stored on the RAID servers.
 - b. A user should not expect their own software “misconfigurations” to be fixed for them – if a users assumes responsibility for administering the machine, then they are responsible for the configuration.
 - c. A user should not allow their workstation to be compromised by hackers.
 - d. A user should not “hog” the machine – they should be willing to share with other users who have a legitimate need.
3. **Staff Response:** If a machine is compromised, has a hard disk failure or is otherwise “broken”, the system will be fixed by wiping the hard drive and reinstalling the default departmental software build. A user may lose any software or data they have stored and are unable to move before the system is rebuilt.

J. Personal Systems

A user may bring a personal, private system into the department. Systems staff does their best to accommodate this, and generally allow network access to these systems.

1. **DO:** Things that can be done with personal systems:
- a. A user may store whatever they like on the file system of their personal system. *However*, the network based restrictions mentioned above still apply.
 - b. Any system which provides for meaningful security, and which is regularly connected to the network, must also include a root or administrator-equivalent account for systems staff to use to access the system in case of problems.
 - c. All efforts must be made by the owner of the system to ensure the integrity of the system (to guard against hacking)
 - d. NFS file systems are not exported to personal systems, or to any system where anyone other than systems staff has root access to the system.
2. **DO NOT:** Users should not use their system:
- a. For commercial purposes, since that involves commercial use of the University’s network.
 - b. To attack other systems, even for “black hat” purposes.
 - c. To provide any of the otherwise prohibited network services.

- d. Users should not expect systems staff to support or fix their private/personal system.
3. **Staff Response:** If there is a problem with a user's private system, it will be disconnected from the network. Compromised systems will be removed from the network, and will not be reconnected until systems staff has been satisfied that the system has been secured (this generally involves a complete wiping of the system drives).

K. Integrity of Systems

The integrity of all systems must be respected at all times. The department takes the view that it must protect itself from outside harm, but trusts, in keeping with the honor code, its own users not to attack department systems or users.

1. **DO:** Users should:
 - a. Respect the privacy of other users.
 - b. Respect the integrity of their data and processes.
 - c. A user should inform systems staff or "abuse@virginia.edu" if they suspect that a violation has occurred.
2. **DO NOT:** Users should not:
 - a. Attempt to compromise the integrity of data of any kind at any time.
 - b. Attempt to "explore" or investigate the systems, unless permission has been granted and systems staff informed of your activities in advance.
 - c. Under no circumstances should any exploration of non-university systems take place, unless that institution has agreed in advance as part of legitimate academic activity.
 - d. Attempt to "sniff" network traffic.
 - e. Attempt to "crack" user passwords.
3. **Staff Response:** If it appears that a user has done something to violate the integrity of our systems, their privileges and access be suspended immediately. Beyond staff reactions, the department as a whole views violations of the kind discussed here very seriously, and depending on the nature of the infraction, a student may be charged with an honor violation, and/or asked to leave the program.

Computer Science Department Resource Use Policy Agreement

I have read the Computer Science Department Policy, understand its guidelines and agree to abide by them.

Name (print)

Signature

Date