ITCWeb Mobile

Responsible Computing at UVa

A Handbook for Students

In support of its mission of teaching, research, and public service, the University of Virginia provides students access to computing and information resources. Use of these resources is governed not only by the University's own Standards of Conduct and Honor System but also by local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media. It is important that you read and understand the information in this booklet; irresponsible behavior can jeopardize both your computing privileges and your University career.

Table of Contents

Please note: The online version of this booklet may be updated from time to time. Use the online version as the authoritative and current source. Questions about this publication may be emailed to itc-docs@virginia.edu (mailto:itc-docs@virginia.edu) .

I. You, the University, and the Electronic Community

As a student at the University of Virginia, you will have many opportunities to improve your proficiency in the use of information technologies. As a leader in the 21st century, you will want to know how these technologies are used in your major field and in society at large.

Information technologies can help you be more productive as a student — to produce papers and submit assignments on-line, to use the library services, to send messages to your professors and friends, to access class notes, and to participate in many other aspects of student life. The University makes information technologies available to you in many ways:

- Everyone at the University has access to information servers for electronic mail (email) and other Internet services.
- The University's World Wide website contains information to help you register for classes, apply for financial aid, keep up with University events, and much more.
- MyUVa Web portal (https://myuva.virginia.edu) combines many of the information technology resources (email, course websites, podcasts, online calendar and more).
- Public computer labs are available for general use at locations around the Grounds. These public computer labs sites provide access to the Internet and essential software for coursework. Some locations have student consultants on duty to help you with your computing questions.
- You can drop and add courses and check semester grades and other related information by using the Web.
- Selected classrooms, labs, and library carrels are equipped with video and data outlets for Internet access, and most University locations feature wireless network access.
- There are data network connections in on-Grounds residence hall rooms to connect your personal computer to the Internet.
- The University broadcasts more than 25 channels of television programming to residence hall rooms and classrooms, including The Student Information and Academic Access Channels.
- You can purchase computers through the Desktop Computing Initiative (DCI) program at Cavalier Computers (http://www.cavcomp.virginia.edu/bts) , a division of the UVa Bookstore.
- Many at the University have access to a voice mail system, which makes it easy and convenient to keep in touch with friends and professors.

II. Who Owns What

We will use the possessive word "your" frequently in this booklet, but the term does not always mean ownership. In some cases, it means "exclusive use." You may own a personal computer or workstation. You will make the decisions about how that equipment will be used. You may own a software license — word processing or spreadsheet software, perhaps — that you purchased from a software vendor. Your license usually allows you to possess ONE copy of this software for your own use.

The University owns the central computers, departmental computer labs, the public computer labs, the computers it places on its employees' desks, the printers and other devices it has attached to them, and all the software it has installed on them. The University determines who may use these resources and how they may use them.

The University owns the University network — all the wires, wireless hubs, cables, and routers that connect the central computers, computer labs, microcomputer sites, and perhaps your personal computer to each other and, beyond the Grounds, to the Internet. The University determines who is authorized to use its network, and can limit the nature of the use.

III. Email: Rules, Responsibilities, and Privacy

Except in specific circumstances, the content of the electronic communications and files associated with your account will be treated as confidential by the University because it does not routinely examine or monitor such content. You should be aware, however, that your electronic communications and files can sometimes be records that are subject to review with sufficient

justification. They may be subject to Virginia Freedom of Information Act if they were produced, collected, received or retained in pursuance of law or in connection with the transaction of public business (rarely the case with student email). They may lose whatever confidentiality they have if their release is compelled by orders issued through courts of law. Also, officials overseeing the University's disciplinary processes may rule that electronic communications and files are evidence that may be reviewed as part of investigations. Under these circumstances, the privacy of your email and other files is not guaranteed. ITC system administrators, however, must follow certain guidelines (http://www.virginia.edu/abuse/info.html) when dealing with requests for individual-account log or content information from persons other than the account holder.

Although you might have downloaded and/or deleted your email messages, ITC's delivery systems work in such a way that messages may be preserved for a time as computer files on centrally-administered disks and at system back-up locations, so your capacity to control if and where copies exist is not absolute. The array of storage locations is another factor making the confidentiality of your electronic communications and files conditional. And, although some email programs allow for use of encrypted email, most still produce messages in plain text; they are like postcards in that others might view the messages in transit or those left in plain view.

Your use of email at the University may from time to time put you in communication with the University's email postmaster (postmaster@virginia.edu). The email website (http://www.itc.virginia.edu/email/) provides information about the kind of help the postmaster staff can provide for your use of email.

Sometimes messages are so badly misaddressed that they cannot be delivered and will end up in the hands of computing staff for redirection. People often make mistakes in addressing their mail that puts private messages in the mailbox of someone other than the intended recipient. If you are the recipient of such a message, common courtesy dictates that you either return the message to the sender with a brief note explaining its misdirection or that you delete the message.

University procedures allow ITC's system administrators to view and modify any files, including email messages, in the course of diagnosing or resolving system problems and maintaining information integrity. ITC system administrators, as part of their jobs, are expected to treat any such information on the systems as confidential. However, if an administrator comes across information that indicates illegal activity, he or she may report the discovery to appropriate authorities. For example, electronic mail messages that carry threats to persons or their immediate families may be prosecuted and punished as felonies under Virginia law. If an ITC system administrator inadvertently encounters an email message containing a threat or other illegal content, it will be turned over to law enforcement officials.

University policies prohibit certain other kinds of email messages. For example, email, University computers, and the University network cannot be used by individuals for commercial purposes or for personal gain. Such policies pertain to email just as they do to any other University resource and are enforced when brought to the attention of appropriate University officials.

Large-scale mailings (to more than 1,000 addresses) impose loads on the University's electronic mail services. They should be used judiciously and often require approval from the president, executive vice president, other vice presidents or deans. For these reasons any large-scale mailing must be coordinated with the University's email postmaster (postmaster@virginia.edu) and must follow an approved process (http://www.itc.virginia.edu/email/massmail.process.html) .

Email accounts are vulnerable to malicious use when others know the owner's computing ID and password; carefully protect your electronic identity from use by anyone other than you. Your email account is also subject to misuse when you leave open a computing session that you have begun in a University computing lab or when you fail to logout from the University's WebMail service before

you close your browser. It is prudent to reboot the computer you use in any lab setting when you finish your work there or even if you leave the workstation, planning to return to it soon. *You are held accountable for any misuse of your email account.*

Other important tips related to email:

- Remember — the email messages you send become the possession of the receiver. They can easily be redistributed by recipients, and rules of disclosure by their systems apply to mail they received from you. When in doubt, double-check the addresses of your intended recipients.
- Do think before you send email — once sent, it is almost impossible to keep email messages from reaching their destinations.
- Realize that University policy and secure passwords provide good but not complete assurance of the privacy of your email messages. When the privacy of a message is of the utmost importance, only a person-to-person verbal conversation may be sufficiently secure.
- Delete messages that should not be preserved.
- Never send or forward chain mail, whether it promises fame and fortune, or even supposed donations for a sick child. In virtually every known case, the claims made by such messages are untrue. A message that has been forwarded ten or more times is by definition in our policy (http://www.itc.virginia.edu/desktop/email/chain.html) a chain letter. This policy violation is a waste of computing resources and a nuisance and often offends recipients.
- Don't pass on unconfirmed rumors — especially about viruses — because they often only cause needless panic. Snopes.com (http://www.snopes.com) provides a useful list of well-known computer-related and other hoaxes about which you may receive information via email.
- Don't open or execute attachments about which you have any question, even if they appear to be coming from a friend. Attachments are a popular way for cyber criminals to automatically distributing viruses, and your friend may not even know that his or her email account is being used for that purpose.
- Configure your email program so that attachments are only opened when you choose to open them.
- If you are sending attachments, include personalized text and specific references to the attachment (i.e., "Attached, in Word format, is my paper on . . .") to help the recipient know that the message and attachment are indeed from you.
- University policy prohibits use of University resources, computing or otherwise, for commercial purposes.
- Realize that if you die while you are a member of the UVa community, your stored electronic communications and files are a part of your personal effects and records that will be given to your executor (the person — usually a family member — designated to deal with your property at your death) if he or she requests it.

IV. About Home Pages

The University's Web server and tools are in place to help you publish a personal home page. ITC's Training Services group and the University Library provide courses designed to help you publish your home page. Remember that you are expected to act responsibly when publishing your home page, just as you are in all use of computing resources at the University.

The University's computing resources are intended to enable the institution to carry out its responsibilities of education, research, and public service. Therefore, these functions have priority in

using computing resources; however, the University recognizes the value of the Internet as a resource for information and communication. When computing resources are available, students may use them for co-curricular or personal purposes provided they abide by the policies and procedures governing such use.

Responsibility

All users of University computing systems must comply with the requirements of responsible computing in the University environment, as outlined here and in the full array of University information technology policies (http://www.itc.virginia.edu/policy) . Individual users assume full legal responsibility for the content of their home pages, and they must abide by all applicable local, state, and federal laws, including laws of copyright. Copyright law is designed to protect the rights of the creator of the material. It applies to many types of materials, including cartoons, pictures, graphics, text, song lyrics, and sounds (including most MP3 and other files shared via so-called peer-to-peer procedures). See Section V (#copyright) for additional important information about copyright.

The University is not responsible for the content of Web pages other than those defined as its "official" Web pages (the official Web pages of University schools, departments, divisions, and other units). As a neutral provider of computing services and access to the Internet, ITC does not review in advance or monitor the content of any materials transmitted, received, published or stored on or otherwise available through its systems. If ITC receives complaints regarding the content of such materials, it will refer the complaint to the appropriate disciplinary system within the University (or to the police for alleged violations of law), and it will cooperate with any resulting investigation in accord with the policies, procedures, and principles described or cited in this handbook.

Assumptions about audiences who will see information you publish

You will be wise to remember the very public nature of information you disseminate on the Internet through the World Wide Web. Information in a home page is published and available to everyone who can get to the Web. You must not assume that your information is restricted to only a close circle of friends, or even the University of Virginia community. You must assume that others will know how to find and view unlinked files that you store in your public Web directory.

You are also responsible for the way you handle information you gather using your Web pages (the University has practices for its own Web pages (http://www.virginia.edu/copyright.html)). See "Revealing Personal Information" below (#reveal) for more information.

Fundraising and Advertising

You may not use home pages for fundraising or advertising for commercial or non-commercial organizations, except for University-related organizations and University-related events and in accord with policies governing these activities.

Use of the University Name, Logo, Seal, or Photographs

You may not use the University name in your home pages in any way that implies University endorsement of other organizations, products, or services. You may not use University logos and trademarks, including the crossed sabers and "V," the Cavalier mascot, the University seal or photographs copyrighted by the University. Photos from the University's home page and secondary pages are copyrighted by the photographers, including the Lawn panoramic photo on the home page, and cannot be used or reproduced in any form. Requests for permission to use the University logos or seal in Web or print publications should be directed to the Office of Web Communications (email webmaster@virginia.edu (mailto:webmaster@virginia.edu) or phone (434) 924-4524). The Director of Licensing in Sports Marketing must approve the use of trademarks and logos for any other purpose. Call (434) 982-5600 for assistance.

V. Copyrights: Ethical and Legal Use

Unauthorized use of copyright-protected or licensed materials (including, but not limited to, graphic images, movies, music or audio files, and written word) is a serious matter and is a violation of federal law. An individual who reproduces and/or distributes digitized copyrighted material without permission and in excess of "fair use" has violated federal digital copyright law, has put him or herself at real personal risk for a lawsuit brought by the copyright owner, has violated University policy, and might have violated the University's Honor and Judiciary Codes. An introduction to copyright law (http://www.lib.virginia.edu/copyright/) and University copyright policy (http://www.itc.virginia.edu/policy/copyright.html) may help you understand more.

Individuals who use software, such as BitTorrent and LimeWire, to listen to or view files over the network often unknowingly allow their computers to be used by the software to share these files and all the individuals' personal files with everyone on the Internet. Be aware that the penalties cited above apply in these cases. The University will not protect individuals who use or share (knowingly or not) copyrighted materials without an appropriate license to do so.

Copyright laws and policies also apply to software. Most software available for use on computers at the University of Virginia is protected by federal copyright laws. The software provided through the University for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses. Licenses sometimes specify that you may use the software only while you are a member of the UVa community, which means you must discontinue use of — and remove copies of — the software when you leave the UVa community.

It is the policy of the University to respect the copyright protections given to software owners by federal law. It is against University policy for faculty, staff, or students to copy or reproduce any licensed software on University computing equipment, except as expressly permitted by the software license. Of course, faculty, staff, and students may not use unauthorized copies of software on University-owned computers.

It is worth repeating that at the University of Virginia, unauthorized use of copyrighted materials of all types is a serious matter. Any such use is without the consent of the University and is subject to University disciplinary action and possible prosecution through the federal court system.

VI. Good Citizenship in the Internet Community

As more than one writer has observed, the Internet isn't a thing; it is neither an entity nor an organization; it isn't owned or run by anyone. It is a world of a million publishers with some of the characteristics of a frontier. The only code of behavior on that frontier is one that demands individual responsibility and accountability and that rewards those attributes with rational self-government, albeit quite limited in scope. The University provides Internet access to its students and employees with the expectation that they be good, responsible, and accountable Internet citizens. But, what does that mean in practical terms? How can you be a good Internet citizen?

READ and understand applicable policies, notably Ethics in Computer Usage (http://www.itc.virginia.edu/policy/ethics.html) .
KNOW what it means to take responsibility for your safety and security in the Internet environment and for deciding what is right and wrong in circumstances where often rules have not yet been written. You must take responsibility for educating yourself about the medium that you're using and for helping shape its use by good personal behavior.
BE AWARE of the thousands of others who rely on the University's computers to do their work. Consider how your on-line behavior will affect them.
UNDERSTAND that University policies that address academic dishonesty, including theft,

plagiarism, disruptive conduct and misuse of materials and property, must guide your computing activities, just as they guide your activities in the classroom, residence halls or elsewhere on Grounds.

DON'T let other students, relatives or any other person gain access to the University's computing resources through your account. Understand that you will be held accountable for any abuse of computing resources by persons who use your UVa computing ID and password.

DON'T use computer accounts, computing IDs, and passwords that belong to someone else. Don't forge email from faculty, staff, other students or anyone. To do so violates policy and may violate law.

BE ACCOUNTABLE for your actions. Hiding your identity to avoid responsibility for your behavior on the network or using someone else's network identity are — at a minimum — violations of policy, and they may be serious violations of law.

DON'T waste shared computing resources on activities that have no academic purpose.

KNOW that local, state, and federal laws and regulations pertain to computing activities wherever appropriate — laws dealing with fraud, forgery, harassment, extortion, gambling, threats, copyright, obscene content, among others. Violators may be prosecuted.

BE WARY of those who will (sometimes unknowingly) provide on-line information that is untrue or fraudulent. If you are not certain, ask.

KNOW that messages you post to newsgroups or Web pages that you create in an attempt to be humorous may not be received in that spirit. After writing an email, it is often a good idea to read your email aloud before sending it. Remember that archives of newsgroups and Web pages remain accessible for years — don't be surprised if an interviewer asks about something you posted to a newsgroup while a student when you're trying to get that job you really want in a few years.

UNDERSTAND what you are authorized to do. Know what the University's purpose is in making these computing resources available to you.

- Your computer account is provided so you can send and receive email, read and post notices to newsgroups, have access to library and other information resources, and have a website.
- In some cases, your professors will authorize further account access so you can do class assignments.
- Public computer labs are available so you can do word processing, make spreadsheets, and access other ITC and University computer resources and the Internet. The software in the labs is for use there; you cannot copy it and use it elsewhere.

USE bandwidth wisely. Excessive use of bandwidth is often caused by downloading music and movie files. It is defined by standard deviations from the norm. Excessive bandwidth use hurts everyone on the network. Remember — there may be a time that you may be experiencing slow connectivity due to abuse of bandwidth. Furthermore, repeated excessive bandwidth use may result in loss of network privileges. For more information, read about Network Capacity Management (http://www.itc.virginia.edu/network/dormnetworks.html) .

DON'T TRY TO GAME THE SYSTEM. Looking for ways to take advantage of the University's computing resources by abusing the rules for ethical use is considered gaming the system. For example, using computers that are not registered to you in order to download excessive amounts of data and thus use too much bandwidth is gaming the system. The rules are intended to protect the fair use of UVa's computing resources.

DON'T MISUNDERSTAND. Violation of University computing policy can result in your network access being revoked. In extending these resources, the University trusts students to make responsible use of them. If you violate that trust, you may lose access through various processes described elsewhere in this booklet.

VII. Threats to Your On-Line Safety and Security

The Internet community is under regular attack — at varying levels of seriousness — from "outlaws." Such outlaws (both within our community and outside it):

- steal other people's computing IDs and passwords
- hack into your computer and use it without your permission and often without your knowledge
- disrupt computer systems and networks
- flood electronic mail systems with unwanted messages (spam)
- send forged electronic messages from celebrities, politicians, the University president, your government professor or, maybe, YOU
- post messages that vilify and threaten other people
- post inappropriate messages to mailing lists
- spread viruses
- subscribe others to mailing lists, or unsubscribe them, without their permission
- tempt you to reveal private information like your password or credit card number
- or invade the privacy of others.

Students who do these things at the University of Virginia may lose computing privileges and be subject to suspension or expulsion from the University. They might even be subject to prosecution under state and federal laws.

Cracking Passwords

Your password may be guessed or "cracked" if you choose a common word, or a friend's or a pet's name, or your nickname, or the name of your favorite team or the name of a celebrity. Choose a password that combines letters, numbers, and special characters (for example, $, *, !). Whether you use your UVa computing ID and password or not, it is your responsibility to keep them secure. Do not let anyone talk you into "sharing" — not even your closest friend or loved one. Don't keep your password and computing ID together. If you can remember your password without writing it down, that is best. Don't tell your friends — or anyone, even someone assisting you with problem solving — what your password is. Change your password regularly. A good password (http://www.itc.virginia.edu/accounts/passwords.html) , will help keep your account secure.

Crashing and Disrupting the System

Malicious computer users make the system stop working or perform poorly. It's like speeding, shop-lifting, spray-painting cars, or slashing tires. These users find out, from a variety of sources — sometimes each other — about things they can do to disrupt the systems. In almost every instance, such behavior violates the law, and, in every instance, it violates University policy. Consequences are severe.

Forging Email

It is not hard to forge electronic messages. It also is usually against the law in its own right, and, in connection with the sending of unsolicited bulk email, may violate other state or federal laws.

Spamming

Spam is essentially the same message emailed over and over and broadcast to recipients who did not request it. Just because a message is annoying, off-topic or stupid doesn't make it spam; the defining characteristic of spam is the volume with which it is sent. Most common forms of spam violate Virginia law. Spamming is an international problem, however, and unfortunately no one as yet

has found an effective way to eliminate it. There are things you can and can't do about spam (http://www.virginia.edu/abuse/spamemail.html) . In many cases, simply deleting the unwanted message is the best action you can take.

Phishing
Phishing is a high-tech scam that uses email or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information. These messages should be viewed as illegitimate attempts to gain this personal information and should be deleted. These emails may appear to be legitimate. Be wary. Legitimate sources will not ask for personal or account information without providing a way to verify the email. If you receive an electronic communication such as an email from what appears to be your bank or credit card company directing you to click an embedded link, delete the email.

Revealing Personal Information
The Internet offers the ability to share information easily. However, be wary of what information you share. Identity theft, leading to disastrous financial consequences, may result from sharing details like your Social Security number. Websites like Facebook, MySpace, Friendster, and Xanga make it is easy to share information about your whereabouts, your contact information, and your physical attributes. Be cautious about sharing any information that may put you at personal risk now or that may prove to be embarrassing later. Revealing information about your whereabouts including your class schedule, your dorm room, or your apartment address may put you physically at risk. Additionally, many employers now search Facebook and MySpace for inappropriate conduct for job candidates. Information shared on the Internet may be available for years.

Controlling Access to Your Computing Files
The University's computing environment is designed to be an open environment. Many faculty and students want, or need, others to view and use their computer information — their files. An instructor may want students to find a class assignment on the network. A student may want to share some information with friends. Computer networks are designed to let this happen.

But many students and faculty do not want others seeing their messages, course work or research. On computers, you can control who can see your files by protection settings. Use these settings as you would locks to keep your files private. However, malicious users realize that many people don't know how to use the settings. If you need help in using the settings, introductory computing documents (like this one for PCs (http://www.itc.virginia.edu/security/checklistforPCs.html)) are available on ITCWeb and from the ITC Help Desk (http://www.itc.virginia.edu/helpdesk/) . The Help Desk is located in the Dynamics Building (2015 Ivy Road), First Floor, Room 116, and is open from 8:00 a.m. to 4:30 p.m., Monday through Friday, for walk-in assistance (except on most University holidays).

Because some people don't know how to limit access to their files, sometimes information is left unintentionally unprotected. When people are good citizens of the Internet community, unprotected files are not a problem. Good Internet citizens respect one another's privacy. Students who gain access to resources either by directly breaking into them or because they are just poorly protected violate the Ethics in Computing Usage policy (http://www.itc.virginia.edu/policy/ethics.html) and the Standards of Conduct (http://http://scs.student.virginia.edu/~judic/soc.php) . If you have any doubt about whether any resources or materials were intended to be public, ask the owner before you look. If you happen across resources or materials that you suspect weren't intended to be public, let the owner know. That owner may have no idea that he or she has left something open to worldwide viewing.

VIII. What You Should Do if You are a Victim of Computing Abuse or Irresponsible Behavior

Unfortunately computer abuse, malicious behavior, and unauthorized account access do happen.

Should any of these things happen to you, report them to ITC, your system administrator or other appropriate University authority. Computing resource abuse should be reported to abuse@virginia.edu (mailto:abuse@virginia.edu) . This step will alert a number of ITC and University staff to your situation. Abuse cases are handled individually and confidentially;see the Abuse website (http://www.virginia.edu/abuse) for more information.

IX. Security and Connecting Your Equipment to the University Network

If you connect your personal computer equipment to the University of Virginia's network, you are responsible for the security of your resources — not only for risks to the resources themselves but also for the possibility that your unsecured resources can be used by anyone on the Internet as remote locations to mount attacks on other computing systems.

Note: In order to connect your computer to the University of Virginia's network, you will have to register your computer with ITC (http://www.itc.virginia.edu/network-registration) . This registration links your name to your computer and its network activity.

Any misuse of your equipment through your neglect in providing safeguards may be reason to deny access for your equipment to our network. "Neglect" in this instance may take many forms — here are a few:

- Failure to:
    - use a strong password
    - limit access to your equipment
    - keep files from unknown sources off your equipment
    - back up your files
    - use up-to-date antivirus and antispyware software
    - use great caution in opening email attachments
    - keep your operating system up-to-date
    - keep application software updated
    - turn off or delete unneeded software features, such as file sharing

The Security of Networked Devices policy (http://www.itc.virginia.edu/policy/netdevices/) provides more details on the security-related responsibilities of connecting equipment to the University network, as does ITC's security website (http://www.itc.virginia.edu/security) . This site (http://www.itc.virginia.edu/security) also provides helpful guidance for keeping your computer secure.

X. Disciplinary Action for Abuse of Computing Resources

Students at the University have both rights and responsibilities. The University is committed to supporting the exercise of any right guaranteed to individuals by the Constitution and the Code of Virginia and to educating students relative to their responsibilities. Students' rights are listed in The Undergraduate Record (http://records.ureg.virginia.edu/index.php?catoid=7) and its graduate counterpart (http://records.ureg.virginia.edu/index.php?catoid=9) .

The University's Standards of Conduct (http://scs.student.virginia.edu/~judic/soc.php) include the expectation that students understand and abide by the all University information technology-related policies (http://www.itc.virginia.edu/policy) . Any student alleged to violate such policies will be subject to full disciplinary action within the Undergraduate and Graduate Student Judicial System (http://scs.student.virginia.edu/~judic/index.php) , up to and including loss of computing accounts and

access, suspension and/or expulsion.

Standards of Conduct

The University of Virginia is a community of scholars in which the ideals of freedom of inquiry, freedom of thought, freedom of expression, and freedom of the individual are sustained. It is committed to preserving the exercise of any right guaranteed to individuals by the Constitution. However, the exercise and preservation of these freedoms and rights require a respect for the rights of all in the community to enjoy them to the same extent.

It is clear that in a community of learning willful disruption of the educational process, destruction of property, and interference with the orderly process of the University or with the rights of other members of the University cannot be tolerated. Students enrolling in the University assume an obligation to conduct themselves in a manner compatible with the University's function as an educational institution. To fulfill its functions of imparting and gaining knowledge, the University retains the power to maintain order within the University and to exclude those who are disruptive of the educational process.

When it is possible for the student Standards of Conduct (http://scs.student.virginia.edu/~judic/soc.php) to be applied to conduct related to computing at the University, you should expect that they will be. Read them at the University Judiciary Committee's website (http://scs.student.virginia.edu/~judic/index.php), and you will understand how several are particularly relevant to the computing environment.

How ITC Handles Student Computer Policy Violations

The procedures for handling alleged student abuse of computing resources are detailed in various University publications and websites, including The Undergraduate Record (http://records.ureg.virginia.edu/index.php?catoid=7) and its graduate counterpart (http://records.ureg.virginia.edu/index.php?catoid=9). Such resources describe the Honor System (http://www.virginia.edu/honor/) and the University Judicial system (http://scs.student.virginia.edu/~judic/index.php), as well as the University's policies, all of which form the context for ITC's procedures.
Briefly:
Step 1:
When ITC is notified (usually through abuse@virginia.edu) that a student appears to be abusing computing resources, all of his or her computing privileges may be suspended immediately when such an action is warranted to protect the computing resources and to assure reliable service to the rest of the community.
Step 2:
Often, ITC staff will notify the student through phone contact, electronic or U.S. mail of the apparent violation. Frequently, the matter is resolved at that step by explanation from the student and, in the case of minor issues, assurance from the student that the behavior will not continue. If computing access has been suspended, it is usually restored at successful conclusion of this step.
Step 3:
If the abuse of computing resources cannot be resolved at Step 2, ITC may refer the matter through the Division of Student Affairs for disciplinary processes (including those that may involve the Honor or Judiciary systems) or through law enforcement officials if the matter involves an apparent violation of law. Computing access may remain suspended during these processes. Sometimes, individuals in the University community who are complaining about the behavior take the matter directly to Student Affairs, the Honor or Judiciary systems, or law enforcement.

XI. UVa Computing Policy Digest

It is your responsibility as a user of the University of Virginia's computers and networks to be familiar with the policies that govern their use. By using your computing ID at UVa, you automatically agree to abide by all of the policies, terms, and conditions, including but not limited to the information in this publication and the University's Information Technology policies website (http://www.itc.virginia.edu/policy) .

Have further questions? Please call the ITC Help Desk at (434)924-3731 or send electronic mail to consult@virginia.edu (mailto:consult@virginia.edu) .

If you're a new student, and following the "New Student Account Access" checklist, continue on with:

- Step 2. (optional) Check out the video! "When I go to UVa..." (http://www.itc.virginia.edu/pubs/docs/RespComp/videos/home.html)
- Step 3. Take the quiz: Responsible Computing Quiz for Students (Required for Account Activation) (https://quiz.people.virginia.edu/rcq.fcgi)