Policies Governing Use of Computing Technology in Academic Libraries

Jason Vaughan

The networked computing environment is a vital resource for academic libraries. Ever-increasing use dictates the prudence of having a comprehensive computer-use policy in force. Universities often have an overarching policy or policies governing the general use of computing technology that helps to safeguard the university equipment, software, and network against inappropriate use. Libraries often benefit from having an adjunct policy that works to emphasize the existence and important points of higher-level policies, while also providing a local context for systems and policies pertinent to the library in particular. Having computer-use policies at the university and library level helps provide a comprehensive, encompassing guide for the effective and appropriate use of this vital resource.

For clients of academic libraries, the computing environment and access to online information is an essential part of everyday service—every bit as vital as having a printed collection on the shelf. The computing environment has grown in positive ways—higher-caliber hardware and software, evolving methods of communication, and large quantities of accurate online information content. It has also grown in many negative ways—the propagation of worms and viruses, other methods of hacking and disruption, and inaccurate informational content. As the computing environment has grown, it has become essential to have adequate and regularly reviewed policies governing its use. Often, if not always, overarching policies exist at a broad institutional or even larger systemwide level. Such policies can govern the use of all university equipment, software, and network access within the library and elsewhere on campus, such as campus computer labs. A single policy may encompass every easily conceivable computing-related topic, or there may be several individual policies. Apart from any document drafted and enforced at the university level, various public laws exist that also govern appropriate computer-use behavior, whether in academia or on the beach. Many institutions have separate policies governing employee use of computer resources; this paper focuses on student use of computing technologies.

In some cases, the library and the additional campus student-computer infrastructure (for example, campus labs and dormitory computer access) are governed by the same organizational entity, so the higher-level policy and the library policy are de facto the same. In many instances, libraries have enacted additional computer-use policies. Such policies may emphasize or augment certain points found in the institution-level policy(s), address concerns specific to the library environment, or both. This paper surveys the scope of what are most commonly referred to as "computer-use policies," specifically, those geared toward the student-client population. Common elements found in university-level policies (and often later emphasized in the library policy) are identified. A discussion on additional topics generally more specific to the library environment, and often found in library computer-use policies, follows. The final section takes a look at the computer-use environment at the University of Nevada, Las Vegas (UNLV), the various policies in force, and identifies where certain elements are spelled out—at the university level, the library level, or both.

Policy Basics

Purpose and Scope

Policies can serve several purposes. A policy is defined as:

> a plan or course of action . . . intended to influence and determine decisions, actions, and other matters. A course of action, guiding principle, or procedure considered expedient, prudent, or advantageous.[1]

Any sound university has a comprehensive computer-use policy readily available and visible to all members of the university community—faculty, staff, students, and visitors. Some institutions have drafted a universal policy that seeks to cover all the pertinent bases pertaining to the use of computing technology. In some cases, these broad overarching policies have descriptive content as well as references to other related or subsidiary policies. In this way, they provide content and serve as an index to other policies. In other cases, no illusions are made about having a single, general, overarching policy—the university has multiple policies instead. Policies can define what is permitted (use of computers for academic research) or not permitted (use of computers for nonacademic purposes, such as commercial or political interests). A policy is meant to guide behavior and the use of resources as they are meant to be used. In addition, policies can delve into procedure. For example, most policies contain a section on how to report suspected abuse and how suspected abuse is investigated, and outlines potential penalties. Policies buried in legalese may serve some purpose, but they may not do a good job of educating users on what is acceptable and not acceptable. Perhaps the best approach is an appropriate

Jason Vaughan (jvaughan@ccmail.nevada.edu) is Head of the Library Systems Department at the University of Nevada, Las Vegas.

balance between legalese and language most users will understand. In addition, policies can also serve to help educate individuals on important topics, rather than merely stating what is allowed and what will get one in trouble. For example, a general policy statement might read, "You must keep your password confidential." Taken a step further, the policy could include recommendations pertaining to passwords, such as the minimum password length, inclusion on nonalphabetic characters, the recommendation to change the password regularly, and the mandate to never write down the password.

Characteristics of a Policy—Visibility, Prominence, Easily Identifiable

A policy is most useful when it is highly visible and clearly identified as a policy that has been approved by some authoritative individual or body. Students often sign a form or agree online to terms and conditions when their university accounts are established. Web pages may have a disclaimer stating something to the effect of "use of (institution's) resources is governed by . . . ." and provide a hyperlink to the various policies in place. Or, a simple policies link may appear in the footer of every Web page at the institutional site. Some universities have gone a bit further. At the University of Virginia, for example, students must complete an online quiz after reviewing the computer-use guidelines.[2] In addition, they can choose to view the optional video. Such components serve to enhance awareness of the various policies in place.

A review of the library literature failed to uncover any articles focusing on computer-use policies in academic libraries. The author then selected several similar-sized (but not necessarily peer) institutions to UNLV—doctoral-granting universities with a student population between twenty thousand and thirty thousand—and thoroughly examined their library Web sites to see what, if any, policy components were explicitly highlighted. It quickly became evident that many libraries do not have a centrally visible, specifically titled, inclusive computer-use policy document. Most, but not all, of the library Web sites provided a link to the institutional-level computer-use policy. In some cases, library policies were not consolidated under a central page titled "Policies and Procedures," or "Guidelines," and, where they did appear, the context did not imply or state authoritatively that this was an official policy. There was no statement of who drafted the policy (which can lend some level of authority or credence), as well as no indicated creation or revision date. Granted, many libraries have paper forms one must sign to obtain a library card, or they may state the rules in hardcopy posted within prominent computer-dense locations. Still, with so much emphasis given to licensed database and Internet resources, and with such heavy use of the computing environment, such policies should appear online in a prominent location. Where better to provide a computer-use policy than online? Perhaps all the libraries reviewed did have policies posted somewhere online. If the author could not easily find them, chances are a student would have difficulties as well. In sum, the location of the policy information and how it is labeled can make a tremendous difference.

Revisions

Policies should be reviewed on a regular basis. Often, the initial policy likely goes through university counsel, the president's administrative circles, and, perhaps, a board of regents or the equivalent. Revisions may go through such avenues, or may be more streamlined. A frequent review of policies is mandated by evolving information technology. For example, cell phones with built-in cameras or Internet-browsing capabilities, nonexistent a few years ago, are now becoming mainstream. With such an inconspicuous device, activities such as taking pictures of an exam or finding simple answers online are now possible. Similarly, regularly installed critical updates are a central concept within Windows' latest version of operating-system software. Such functionality failed to attract much attention until the increase in security exploits and associated media coverage. Some policies, recently updated, now make mention of the need to keep operating systems patched.

Why Have a Library Policy?

While some libraries link to higher-level institutional policies and perhaps have a few rules stated on various scattered library Web pages, other libraries have quite comprehensive policies that serve as an adjunct to (and certainly comply with) higher-institutional policies. There are several reasons to have a library policy. First, it adds visibility to whatever higher-level policy may be in place. A central feature of a library policy is that it often provides links (and thus, additional visibility) to other higher-level policies. A computer-use policy can never appear in too many places. (Some libraries have the link in the footer of every Web page.) A computer-use policy can be thought of as a speed limit sign. Presumably, everyone knows that unless otherwise posted, the speed limit inside the city is thirty-five miles per hour, and outside it is fifty-five miles per hour. Nevertheless, numerous speed-limit signs are in place to remind drivers of this.

Higher-level institutional policies often take a broad stroke, in that they pertain to and address computing technology in general, without addressing specific systems in detail. A second reason to have a local-library policy is to reflect rules governing local-library resources that are housed and managed by the library. Such systems often include virtual reference, electronic reserves, laptop–checkout privileges, and the mass of electronic databases and full-text resources purchased and managed by libraries. Such library-based systems do not necessarily make the radar of higher-level policies, yet have important considerations, such as copyright issues in the electronic age or privacy as it relates to e-mail and chat reference. In addition, libraries often have two large user groups that other campus entities do not have—university affiliates (faculty, staff, students) and nonuniversity affiliates (community users). While broader university policies generally apply to all users of computing technology, local-library policies can work to address all users of the library PCs, and make distinctions as to when, where, and what each group can use.

Common Computer-Use Policy Elements

The following section outlines broad topics that are usually addressed within high-level, institutional policies. Often, some or many of these same elements are later reemphasized or adapted by libraries, focusing on the library environment. In many cases, the policy is presented in a manner somewhat like breaking the seal on a new piece of software packaging. Essentially, if someone is using the university equipment or network, that person agrees to abide by all policies governing such use. An overarching policy frequently may end with a bulleted summary of the important points in the document. An important first part of the policy is a clear indication of who the policy applies to. This may be as broad as "anyone who sits down in front of university equipment or connects to the network," or as specific as spelling out individual user groups (undergraduates, graduates, alumni, K–12 students). Appendix A summarizes elements found in the various end-user computer policies in force at UNLV and the UNLV university Libraries.

Network and Workstation Security

Network security is a universal topic addressed in computer-use policies. Under this general aegis one often finds prohibitions against various forms of hacking, as well as recommendations for steps individual users should take to help better secure the overall network. There are also such policies as the prohibition of food and drink near computer workstations or on the furniture housing computer workstations. Typical components related to network and workstation security include:

1. Disruption of other computer systems or networks; deliberately altering or reconfiguring system files; use of FTP servers, peer-to-peer file sharing, or operation of other bandwidth-intensive services
2. Creation of a virus; propagation of a virus
3. Attempts at unauthorized access; theft of account IDs or passwords
4. Password information—individual users need to maintain a strong, confidential password
5. Intentionally viewing, copying, modifying, or deleting other users' files
6. A requirement to secure restrictions to files stored on university servers
7. Recommendation or requirement to back up files
8. Statement of ownership regarding equipment and software—the university, not the student, owns the equipment, network, and software
9. Intentional physical damage: tampering, marking, or reconfiguring equipment or infrastructure—such as unplugging network cables
10. Food and drink policies

Personal Hardware and Software

Many universities allow students to attach their own laptops to the campus wired or wireless network(s). In addition to network connections, a growing number of consumer devices such as floppy disks, zip disks, and rewritable CD/DVD–media have the potential to connect to university computers for the purpose of data transfer. Today, the list has grown to include portable flash drives, digital cameras and camcorders, and MP3 players, among others. The attaching of personal equipment to university hardware may or may not be allowed. Similarly, users may often try to install software on university-owned equipment. Typical examples may include a game brought from home or any of the myriad pieces of software easily downloaded from the Internet. Some of the policy elements dealing with the use of personal hardware and software include:

1. Connecting personal laptops to the university wired or wireless network(s)
2. Use of current and up-to-date patched operating systems and antivirus programs running on personal equipment attached to the network
3. Connecting, inserting, or interfacing such personal hardware as floppy disks, CDs, flash drives, and digital cameras with university-owned hardware; liability regarding physical damage or data loss
4. Limit access to and mandate immediate reporting of stolen personal equipment (to deactivate registered MAC addresses, for example)
5. Downloading or installing personal or otherwise additional software onto university equipment
6. Use of personal technology (cell phones, PDAs) in classroom or test-taking environments

E-mail

E-mail privileges figure prominently in computer-use policies. Some topics deal with security and network performance (sending a virus), while many deal with inappropriate use (making threats or sending obscene e-mails). Other topics deal with both (such as sending spam, which is unsolicited, annoying, and consumes a lot of bandwidth). Among the activities covered are prohibitions or statements regarding:

1. Hiding identity, forging an e-mail address
2. Initiating spam
3. Subscribing others to mailing lists
4. Disseminating obscene material or Weblinks to such material
5. General guidelines on e-mail privileges, such as the size of an e-mail account, how long an account can be used after graduation, and e-mail retention
6. Basic education regarding e-mail etiquette

Printing

With the explosion of full-text resources, libraries and other student-computing facilities have experienced a tremendous growth in the volume of pages printed on library printers. At UNLV Libraries, for example, the printing volume for July 2002 to June 2003 was just shy of two million pages; the following year that had jumped to almost 2.4 million pages. Various policies helping to govern printing may exist, such as honor-system guidelines ("don't print more than ten pages per day"). Some institutions or libraries have implemented cost-recovery systems, where students pay fixed amounts per black-and-white and color pages printed through networked printers. Standard policies regarding printer-use cover:

1. Mass printing of flyers or newsletters
2. Tampering with or trying to load anything into paper trays (such as trying to load transparencies in a laser printer)
3. Per-sheet print costs (color and black-and-white; by paper size)
4. Refund policies
5. Additional commonsense guidelines, such as "use print preview in browser"

Personal Web Sites

Many universities allow students to create personal Web sites, hosted and served from university-owned equipment. Customary policy items focusing on this privilege include:

1. General account guidelines—space limitations, backups, secure FTP requirements
2. Use of school logo on personal Web pages
3. Statement of content responsibility or institutional disclaimer information
4. Requirement to provide personal contact information
5. Posting or hosting of obscene, questionable, or inappropriate content

Intellectual Property, Copyright, or Trademark

Abuse of copyright, clearly a violation of federal law, is something that libraries and universities were concerned about long before computers hit the mainstream. Widespread computing has introduced new avenues to potentially break copyright laws, such as peer-to-peer file sharing and DVD-movie duplication, to mention only two. A computer-use policy covering copyright will generally include:

1. General discussion of copyright and trademark law; links to comprehensive information on these topics
2. Concept of educational "fair use"
3. Copying or modification of licensed software, use of software as intended, use of unlicensed software
4. Specific rules pertaining to electronic theses and dissertations
5. Specific mention of the illegality of downloading copyrighted music and video files

Appropriate- and Priority-Use Guidelines

Appropriate use is often covered in association with topics such as network security or intellectual property. However, appropriate- and priority-use rules can be an entire policy and would include:

1. Mention of federal, state, and local laws
2. Use of resources for theft or plagiarism
3. Abuse, harassment, or making threats to others (via e-mail, instant messaging, or Web page)
4. Viewing material that may offend or harass others
5. Legitimate versus prohibited use; use for nonacademic purposes such as commercial, advertising, political purposes, or games
6. Academic freedom, Internet filtering

Privacy, Data Security, and Monitoring

Privacy and data security are tremendous issues within the computing environment. Networking protocols and components of many software programs and operating systems by default keep track of many activities (browser history files and cache, Dynamic Host Configuration Protocol logs, and network account login logs, to mention a few). Additional specialized tools can track specific sessions and provide additional information. Just as creditcard companies, banks, and hospitals provide a privacy policy to their clients, so do many academic computer-use policies. Such statements often address what logs are kept, how they are maintained, how they may be used, and who has access. In addition to the legitimate use of maintaining information, there is the general concept of questionable or outright malicious collection of information, through cookies, spybots, or browser hijacks. The following are concepts often addressed under the general heading of privacy:

1. Cookies, spybots, other malicious software
2. What information is collected for evaluative system management and/or statistical purposes; use of cookies for this; how such information is used and reported
3. Statement on routine monitoring or inspection of accounts or use; reasons information may be accessed (routine system maintenance, official university business, investigation of abuse, irregular usage patterns)
4. Security of information stored on or transmitted by various campus resources
5. Statement on general lack of security of public, multiuser workstations (browser cache, search history, recent documents)
6. Disposition of information under certain circumstances (for example, if a student dies while enrolled, any personal university e-mail and stored files can be turned over to executor of will or parents)

Abuse Violations, Investigations, and Penalties

As policies generally are a statement of what is or is not permitted, or what is considered abuse, a clearly defined mechanism for reporting suspected abuse and policy violations can often be found. Obviously, some abuse issues violate not only university policy, but also local, state, or federal law. Investigations of suspected abuse are by their nature tied into the privacy and monitoring category. Policy items detailing suspected abuse usually include:

1. How one can report suspected abuse
2. How requests for content, logging, or other account information are handled; how and by what entities abuse investigations are handled
3. Potential penalties
4. How to appeal potential penalties; rights and responsibilities one may have in such a situation

Other Computer or Network-based Services Affecting the Broad Student Population

Universities operate any number of other computer or network-based services for the broad academic community. Such services may include provisioning of ISP accounts, courseware, online registration, and digital institutional repositories. Depending on the broad nature of these services, policy information particular to such systems can be specified at the broad policy level, especially if they have unique avenues of potential exploitation or abuse not covered in the general topics included elsewhere in the policy.

Additional Library-Specific Computer-Use Policy Elements

Many libraries elect to have their own, additional computer-use policies that serve as an adjunct to the larger university-level policy that generally governs the use of all computing resources on campus. Libraries that have a formalized library computer-use policy often start with a statement of other policies governing the use of the library equipment and network—references to the university policies in place. The library policy may choose to include or paraphrase parts of the university policy deemed especially important or otherwise applicable to the specific library environment. Important concepts governing university policies apply equally to library policies—purpose and comprehensiveness, visibility, and frequent review. Libraries that have formalized computer-use policies often link them under library common Web-site sections such as "information about the libraries," or "about the libraries." Library policies can help address items unique, special, or otherwise worthy of elaboration, such as specific systems in place or situations that may arise. They can also help provide guidelines and strategies to aid staff in policy enforcement. As an example of a library computer-use policy, appendix B provides the main UNLV Libraries computer-use policy.

Public versus Student Use—Allowances and Priority Use

Many of the other entities on a university campus do not daily deal with the community at large (the non-university affiliates) as do academic libraries. This applies to most if not all public institutions, as well as many private institutions. The degree to which academic libraries embrace community users varies widely; often, a statement on which user groups are the primary clients is stated in a policy. Such policy statements may discuss who may use what computers, what software components they have access to, and when access is allowed. In some cases, levels of access for students and the community are basically the same. Community users may be allowed to use all software installed on the PC. More often, separate PCs with smaller software sets have been configured for community users or for specific access to government documents. In some cases, libraries allow some or all PCs to be used by anyone, student or nonstudent, but have technically configured the PC or network to prevent the community at large from using the full software set (such as common productivity suites).

However, community users may be limited from using the productivity software (such as Microsoft Word) found on these PCs. The may be restricted from using PCs on upper floors, or those reserved for special purposes, such as high-end graphics-development workstations. In addition, during crunch time—midterms and final exams—community users are often restricted to the few PCs set up and configured to allow access only to the library Web page (not the Web at large) and the online catalog. In addition, only students and staff can plug in their personal laptops to the library and campus network. Regardless of whether it is crunch time, nonstudent users can be asked to leave if all PCs are in use and students are waiting. An in-house–authored program identifies accounts and whether particular users are students or nonstudents. In 2005, the UNLV Libraries will begin limiting full web access to community users; they will only be permitted access to a limited set of Web-based resources, such as government document websites and library licensed databases.

More and more government information is available online. For libraries serving as government document repositories, all users have the right to freely access information distributed by the government. In 2005, the UNLV Libraries will begin limiting full Web access to community users; they will only be permitted access to a limited set of Web-based resources, such as government document Web sites and library licensed databases. On another note, many libraries have special adaptive workstations with additional software and hardware to facilitate access to library resources by disabled citizens. Disabled individuals, enrolled at the university or not, are allowed to use these adaptive workstations.

Laptop Checkout Privileges

Many libraries today check out laptops for student use. At UNLV Libraries, faculty, staff, and students may check out LCD projectors and library-owned laptops and plug them into the network at any of the hundreds of available locations within the main library. More details on these privileges can be found in the article "Bringing Them In and Checking Them Out: Laptop Use in the Modern Academic Library."[3] As the university does not otherwise check out laptops to users or allow students to plug in their own laptops to the wired university network, the Libraries had to come up with these additional specific policies.

Licensed Electronic Resources—Terms and Conditions

Academic libraries are generally the gatekeepers to many citation and full-text databases and electronic journals. Each of the myriad subscription vendors has terms of use, violations of which can carry harsh penalties. For example, the UNLV Libraries had an incident where a vendor temporarily cut off access to its resource due to potential abuse detected from a single student. In this case, the user was downloading multiple PDF full-text files in an automated manner. This illustrates the need to have some statement in a library policy outlining the existence of such additional terms of use. Vendors generally place a link at the top page of each of their resources related to this. For greater visibility, libraries should at least point out the existence of such terms of use for better exposure and potential compliance. In addition, some electronic resources have licensing agreements that simply do not permit community-user access. In these cases, library policy can simply state that some licensed resources may be accessed only by university affiliates.

Electronic Reserves

Many libraries have set up electronic reserves systems to help distribute electronic full-text documents and streaming media content, among other things. Additional policies may govern the use of such systems, such as making the system available only to currently enrolled students, and providing some boundaries in terms of what is acceptable for mounting on such a system. In addition, there is the whole area of copyright. E-reserve systems often have built-in methods to help better enforce copyright compliance in the electronic arena. Additional policy statements can help educate faculty members on particulars related to copyright and e-reserves.

Offsite Access to Licensed Electronic Resources

Many libraries provide offsite access to their licensed resources to legitimate users via proxy servers or other methods. The policy regarding such access may address things such as who is permitted to access resources from offsite (such as students, staff, and faculty), and the requirement that the user be in good standing (such as no outstanding library-book fines). In some instances, universities have implemented broad authentication systems that, once logged on from an offsite location, allow the user into a range of university resources, including, potentially, library-licensed electronic resources. If such is the case, information pertaining to offsite access may be found in a higher-level policy.

Electronic Reference Transactions

Many libraries have installed (or plan to install) virtual-reference systems, or, at a minimum, have a simple e-mail reference service ("Ask a Librarian"). In addition, many collect library feedback or survey information through simple forms. In all cases, a record exists of the transaction. With virtual-reference systems, the record can include chat logs, e-mail reference inquiries, and URLs of Web pages accessed during the transaction. A policy governing the use of electronic-reference systems may address such things as which clientele may use the system; a statement on the confidentiality of the transaction; or a statement on whether the library maintains the electronic-transaction details. Items such as hours of operation and response time to an e-mail question could be considered more procedural or informational than a policy issue.

Statements on Information Literacy

While perhaps not a policy per se, many libraries have a computer-use policy statement to the effect that while the library may provide links to certain information, this does not serve as an endorsement or guarantee that the information is accurate, up-to-date, or has been verified. (Such a statement posted on the library Web site may provide additional exposure to the maxim that all that glitters is not gold.) Statements that libraries do not regulate, organize, or otherwise verify the general mass of information on the Internet may be included. Obviously, many libraries have separate instruction sessions, awareness programs, and overall mission goals geared toward information literacy.

Principles on Intellectual Freedom and Internet Filtering

Statements by the American Library Association (ALA) on intellectual freedom and Internet filtering may well appear in an institutional policy and often are included in library policies. Filtering is something more likely to affect public and school libraries as opposed to academic libraries. Still, underage children can and do use academic libraries. In such an environment, they may be intentionally or unintentionally exposed to questionable or obscene material. Thus, a library computer-use policy can express the general concept behind the following:

1. intellectual freedom (freedom of speech; free, equal, unrestricted access);
2. the fact that academic libraries provide a variety of information expressing a variety of viewpoints;
3. the fact that this information is not filtered; and
4. the responsibility of parents to be aware of what their children may be viewing on library PCs.

Some libraries have provided policy links to various sets of information from the Office of Intellectual Freedom at ALA's Web site, such as:

1. ALA Code of Ethics
2. ALA Bill of Rights
3. Intellectual Freedom Principles for Academic Libraries: An Interpretation of the Library Bill of Rights
4. Access to Electronic Information, Services, and Networks: An Interpretation of the Library Bill of Rights

Some libraries also provide references to ALA information pertaining to the USA Patriot Act and how law-enforcement inquiries are handled.

Summary

Computing is a vitally important tool in the academic environment. University and library computing resources receive constant and growing use for research, communication, and synthesizing information. Just as computer use has grown, so have the dangers in the networked computing environment. Universities often have an overarching policy or policies governing the general use of computing technology that help to safeguard the university equipment, software, and network against inappropriate use. Libraries often benefit from having an adjunct policy that works to emphasize the existence and important points of higher-level policies, while also providing a local context for systems and policies pertinent to the library in particular. Having computer-use policies at the university and library level help provide a comprehensive, encompassing guide for the effective and appropriate use of this vital resource.

References

1. *The American Heritage College Dictionary*, 3rd edition. (Boston: Houghton, 1997), 1058.

2. Board of Visitors of the University of Virginia, "Responsible Computing at U.Va.: A Handbook for Students." Accessed June 2, 2004, www.itc.virginia.edu/pubs/docs/RespComp/rchandbook03.html.

3. Jason Vaughan and Brett Burnes, "Bringing Them In and Checking Them Out: Laptop Use in The Modern Academic Library," *Information Technology and Libraries* 21 (2002): 52–62.

Appendix A. Systemwide, Institutional, and Library Computing Policies at UNLV

	SCS NevadaNet Policy*	UCCSN Computing Resources Policy**	UNLV Student Computer-Use Policy***	UNLV Policy for Posting Information on the Web†	UNLV Libraries Guidelines for Library Computer Use††	UNLV Libraries Additional Policies†††
General						
Direct Evident Link or References to Higher-Level Institutional/System Computer Use Policy	-	-	x	x	x	-
Author/Authority Information Included	-	-	-	x	x	x
Approved/Revised Date Included	-	x	-	x	x	x
Network and Workstation Security						
Disruption of other computer systems/networks; deliberately altering or reconfiguring system files; FTP Servers/Peer-to-Peer File Sharing/Operation of other bandwidth intensive services	x	x	-	x	-	-
Creation of a virus; propagation of a virus	x	x	x	-	x	-
Attempts at unauthorized access/Theft of account IDs or passwords	x	x	x	x	x	-
Password Information—individual user's need to maintain a strong, confidential password	-	-	-	-	-	-
Intentionally view, copy, modify, or delete other users' files	-	x	x	x	x	-
Requirement to secure restrictions on stored files						
Recommendation/requirement to back up files	-	-	-	-	-	-
Statement of ownership regarding equipment/software	-	x	-	-	-	-
Intentional physical damage: tampering with or marking, reconfiguring equipment or infrastructure	-	x	x	-	x	-
Food and drink policies	-	-	-	-	-	x

Appendix A. Systemwide, Institutional, and Library Computing Policies at UNLV (cont.)

	SCS NevadaNet Policy*	UCCSN Computing Resources Policy**	UNLV Student Computer-Use Policy***	UNLV Policy for Posting Information on the Web†	UNLV Libraries Guidelines for Library Computer Use††	UNLV Libraries Additional Policies†††
Personal Hardware and Software						
Connecting personal laptops, etc. to university wired or wireless network(s)	-	-	-	-	x	-
Use of current and up-to-date patched operating systems and antivirus programs running on personal equipment attached to network	-	-	-	-	-	-
Connecting/inserting/interfacing personal hardware with existing university equipment; liability regarding physical damage or data loss	-	-	-	-	x	-
Limiting access to personal equipment/report immediately if stolen	-	-	-	-	x	-
Downloading or installation of personal or otherwise additional software onto university equipment	-	x	x	-	x	-
Use of personal technology in classroom/test-taking environments	-	x	x	-	x	-
Printing						
Mass printing of flyers or newsletters	-	-	-	-	x	-
Tampering with or trying to load anything into paper trays	-	-	-	-	-	x
Per-sheet print costs	-	-	-	-	-	x
Refund policies	-	-	-	-	-	-
Additional common-sense guidelines	-	-	-	-	x	-
E-mail						
Hiding identity/forging an e-mail address	-	x	-	-	-	-
Initiating spam	x	x	-	-	-	-

Appendix A. Systemwide, Institutional, and Library Computing Policies at UNLV (cont.)

	SCS NevadaNet Policy*	UCCSN Computing Resources Policy**	UNLV Student Computer-Use Policy***	UNLV Policy for Posting Information on the Web†	UNLV Libraries Guidelines for Library Computer Use††	UNLV Libraries Additional Policies†††
E-mail (cont.)						
Subscribing others to mailing lists	-	-	-	-	-	-
Dissemination of obscene material or Web links to such material	-	-	x	-	x	-
General guidelines on e-mail privileges, such as the size of an e-mail account, how long an account can be used after graduation, etc.	-	-	-	-	-	-
Personal Web Site Specific						
General account guidelines	-	-	-	x	-	-
Use of school name and logo	-	-	-	-	-	-
Statement of content responsibility/institutional disclaimer information	-	-	-	x	-	-
Requirement to provide personal contact information	-	-	-	x	-	-
Posting and hosting of obscene, questionable, or inappropriate material	-	-	-	x	-	-
Intellectual Property, Copyright, and Trademark						
General discussion of copyrights and trademark law; links to comprehensive information on these topics	-	-	-	x	x	x
The concept of educational fair use	-	-	-	-	-	x
Copying or modifying licensed software/use of software as intended/use of unlicensed software	-	x	x	-	x	-
Specific rules pertaining to electronic theses and dissertations	-	-	-	-	-	-

Appendix A. Systemwide, Institutional, and Library Computing Policies at UNLV (cont.)

	SCS NevadaNet Policy*	UCCSN Computing Resources Policy**	UNLV Student Computer-Use Policy***	UNLV Policy for Posting Information on the Web†	UNLV Libraries Guidelines for Library Computer Use††	UNLV Libraries Additional Policies†††
Appropriate- and Priority-Use Guidelines						
Mention of federal, state, and local laws	x	x	x	-	-	-
Use of resources for theft/plagiarism	-	x	-	-	-	-
Abuse, harassment, or making threats to others (via e-mail, instant messaging, Web page, etc.)	-	x	x	x	x	-
Viewing material which may offend others	-	-	-	-	x	-
Legitimate versus prohibited use; use for nonacademic purposes (commercial; advertising; political purposes; games; etc.)	x	x	x	x	x	-
Academic Freedom; Internet filtering	x	x	-	x	x	-
Privacy						
Cookies, spybots, other malicious software	-	-	-	-	-	-
What information is collected for evaluative/system management/statistical purposes; use of cookies for this	-	-	-	-	-	-
Statement on routine monitoring or inspection of accounts or use; reasons information may be accessed	x	x	-	-	-	-
Security of information stored on or transmitted by various campus resources	x	-	-	-	-	-
Statement on general lack of security of public, multi-user workstations	-	-	-	-	-	-
Disposition of information under certain circumstances	-	-	-	-	-	-

Appendix A. Systemwide, Institutional, and Library Computing Policies at UNLV (cont.)

	SCS NevadaNet Policy*	UCCSN Computing Resources Policy**	UNLV Student Computer-Use Policy***	UNLV Policy for Posting Information on the Web†	UNLV Libraries Guidelines for Library Computer Use††	UNLV Libraries Additional Policies†††
Abuse Violations, Investigations, and Penalties						
How one can report suspected abuse	x	-	-	x	-	-
How requests for content, logging, or other account information are handled; how and by what entities abuse investigations are handled	x	x	-	x	-	-
Potential penalties	x	x	x	x	x	-
How to appeal potential penalties; rights/ responsibilities you may have in such a situation	-	-	-	-	-	-
Other Computer/ Network-based Services Affecting the Broad Student Population						
Library-Specific						
Public versus student use —allowances and priority use	-	-	-	-	x	-
Right to access government information	-	-	-	-	-	-
Assistance for person with disabilities	-	-	-	-	-	x
Laptop, LCD projector, etc. checkout privileges	-	-	-	-	-	x
Licensed electronic resources—terms and conditions	-	-	-	-	-	-
Offsite access to licensed electronic resources—who can access from offsite	-	-	-	-	-	x
Electronic reference transactions	-	-	-	-	-	-
Statements on information literacy	-	-	-	-	x	-

Appendix A. Systemwide, Institutional, and Library Computing Policies at UNLV (cont.)

	SCS NevadaNet Policy*	UCCSN Computing Resources Policy**	UNLV Student Computer-Use Policy***	UNLV Policy for Posting Information on the Web†	UNLV Libraries Guidelines for Library Computer Use††	UNLV Libraries Additional Policies†††
ALA principles on academic freedom/Internet filtering	-	-	-	-	x	-
Electronic reserves; copyright as it pertains to electronic reserves	-	-	-	-	-	x

Notes

* The Systems Computing Services NevadaNet Policy. Among other responsibilities, SCS provides and maintains the general Internet connectivity for Nevada's higher education institutions, including UNLV. The complete document can be accessed at www.scs.nevada.edu/nevadanet/nvpolicies.html.

** The University and Community College System of Nevada Computing Resources Policy. UCCSN is the system of higher education institutions in the state of Nevada, governed by an elected board of regents. The complete document can be accessed at www.scs.nevada.edu/about/policy061899.html

*** The complete document can be accessed at www.unlv.edu/infotech/itcc/SCUP.html.

† The complete document can be accessed at www.unlv.edu/infotech/itcc/WWW_Policy.html.

†† The primary UNLV Libraries policy governing student computer use. Provided in Appendix 2, the complete document can also be accessed at www.library.unlv.edu/services/policies/computeruse.html.

††† Various other policies are in effect at the UNLV Libraries. Some of these can be accessed at www.library.unlv.edu/services/policies/computeruse.html.

Appendix B. UNLV University Libraries Guidelines for Library Computer Use

In pursuit of its goal to provide effective access to information resources in support of the university's programs of teaching, research, and scholarly and creative production, the university libraries have adopted guidelines governing electronic access and use of licensed software. All those who use the libraries' public computers must do so in a legal and ethical manner that demonstrates respect for the rights of other users and recognizes the importance of civility and responsibility when using resources in a shared academic environment.

Authorized Users

To gain authenticated access to the libraries' computer network, all users of the university libraries public computers must be officially registered as a library borrower, a library computer user, or a guest user. A photo ID is required. (Exceptions may be made as needed when access to Federal Depository electronic resources is required.) Priority use is granted to UNLV students, faculty, and staff. As need arises, access restrictions may be imposed on nonuniversity users. In accordance with licensing and legal restrictions, nonuniversity users are restricted from using word-processing, spreadsheet, and other productivity and high-end multi-media software. During high-demand times, all users may have time restrictions placed on their computer use. If requested by library staff, all users must be prepared to show photo ID to confirm their user status.

Authorized and Unauthorized Use

Public computers are to be used for academic research purposes only. Electronic information, services, software, and networks provided directly or indirectly by the university libraries shall be accessible, in accordance with licensing or contractual obligations and in accordance with existing UNLV and University and Community College System of Nevada (UCCSN) computing services policies (UCCSN Computing Resources Policy www.scs.nevada.edu/about/policy061899.html;

UNLV Faculty Computer Use Policy www.unlv.edu/infotech/itcc/FCUP.html; Student Computer Use Policy http://ccs.unlv.edu/scr/computeruse.asp).

Users are not permitted to:

1. Copy any copyrighted software provided by UNLV. It is a criminal offense to copy any software that is protected by copyright, and UNLV will treat it as such
2. Use licensed software in a manner inconsistent with the licensing arrangement. Information on licenses is available through your instructor
3. Copy, rename, alter, examine, or delete the files or programs of another person or UNLV without permission
4. Use a computer with the intent to intimidate, harass, or display hostility toward others (sending offensive messages or prominently displaying material that others might find offensive such as vulgar language, explicit sexual material, or material from hate groups)
5. Create, disseminate, or run a self-replicating program ("virus"), whether destructive in nature or not
6. Use a computer for business purposes
7. Tamper with switch settings, move, reconfigure, or do anything that could damage terminals, computers, printers, or other equipment
8. Collect, read, or destroy output other than your own work without the permission of the owner
9. Use the computer account of another person with or without their permission unless it is designated for group work
10. Use software not provided by UNLV
11. Access or attempt to access a host computer, either at UNLV or through a network, without the owner's permission, or through use of log-in information belonging to another person

Internet and Web Use

The university libraries cannot control the information available over the Internet and are not responsible for its content. The Internet contains a wide variety of material, expressing many points of view. Not all sources provide information that is accurate, complete, or current, and some may be offensive or disturbing to some viewers. Users should properly evaluate Internet resources according to their academic and research needs. Links to other Internet sites should not be construed as an endorsement by the libraries of the content or views contained therein.

The university libraries respect the First Amendment and support the concept of intellectual freedom. The libraries also endorse ALA's Library Bill of Rights, which supports access to information and opposes censorship, labeling, and restricting access to information. In accordance with this policy, the university libraries do not use filters to restrict access to information on the Internet or Web. As with other library resources, restriction of a minor's access to the Internet or Web is the responsibility of the parent or legal guardian.

Printing

Users are charged for printing no matter who supplies the paper. Mass production of club flyers, newsletters, posters is strictly prohibited. If multiple copies are desired, users need to go to an appropriate copying facility such as Campus Reprographics. Contact a staff member when using the color laser printer to avoid costly mistakes. The university libraries reserve the right to restrict user printing based on quantity and content (such as materials related to running an outside business).

Copyright Alert

Many of the resources found on the Internet or Web are copyright protected. Although the Internet is a different medium from printed text, ownership and intellectual property rights still exist. Check the documents for appropriate statements indicating ownership. Most of the electronic software and journal articles available on library servers and computers are also copyrighted. Users shall not violate the legal protection provided by copyrights and licenses held by the university libraries or others. Users shall not make copies of any licensed or copyrighted computer program found on a library computer.

Use of Personal Laptops and Other Equipment

Students, faculty, and staff of the university are welcome to bring laptops with network cards and use them with our data drops to gain access to our network. The laptop must be registered in our laptop authentication system, and a valid library barcode is also required. Users are responsible for notifying the library promptly if their registered laptop is lost or stolen, since they may be held responsible if their laptop is used to access and damage the network. Users taking advantage of this service are required to abide by all UCCSN and UNLV computer policies. The libraries allow the use of the universal serial bus (USB) connections located in the front of the workstations. This includes use with portable USB-based devices such as flash-based memory readers (memory sticks, secure digital) and digital camera connections. The patron assumes all responsibility in attaching personal hardware to library workstations. The libraries are not responsible for any damage done to patron-owned items (hardware, software, or personal data) as a result of connecting such devices to library workstations. As with any use of library workstations, patrons must adhere to all UCCSN, UNLV, and university libraries' computing and network-use policies. Patrons are responsible for the security of their personal hardware, software, and data.

Inappropriate Behavior

Behavior that adversely affects the work of others and interferes with the ability of library staff to provide good service is considered inappropriate. It is expected that users of the libraries' public computers will be sensitive to the perspective of others and responsive to library staff's reasonable requests for changes in behavior and compliance with library and university policies. The university libraries and their staff reserve the right to remove any user(s) from a computer if they are in violation of any part of this policy and may deny further access to library computers and other library resources for repeat offenders. The libraries will pursue infractions or misconduct through the campus disciplinary channels and law enforcement as appropriate.

Revised: March 3, 2004
Updated: Thursday, May 13, 2004
Content Provider: Wendy Starkweather, Director of Public Services