**Guidelines for Responsible Use of College Computing Resources**

*Reprinted with permission from author Steve McDonald\**

The ubiquitous nature of the Internet, the propagation of intelligent wireless devices, and the development of social media communications networks are transforming communications at the local, state, regional, national and global levels. In one way, these trends render geography irrelevant –

electronic commerce and social media communications have no capitals or headquarters – and in another way make geography extremely pertinent, as demonstrated by real-time pictures and reports from many Middle East countries in which significant uprisings or political movements have occurred in recent years. By establishing a webpage or Twitter account, for example, an Internet user can speak to a larger and wider audience than does the New York Times, NBC, or National Public Radio. Celebrity Twitterati publish to communities with larger print circulations than the Wall Street Journal or The Financial Times.

The Internet’s powerful and revolutionary potential for good also presents serious opportunities for misuse. Such misuse can be particularly prevalent on college and university campuses, where free *access* to computing resources is often mistakenly thought to be the equivalent of *free speech*, and where free speech rights are in turn often mistakenly thought to include the right to do whatever is technically possible.

The rights of academic freedom and freedom of expression apply to the use of College computing resources, as do the responsibilities and limitations associated with those rights. Thus, legitimate use of College computing resources does not extend to whatever is technically feasible. In addition, while certain restrictions are incorporated into the College’s computer operating systems and networks, those restrictions are not the only restrictions on what is permissible. Users of College computing resources must abide by all applicable restrictions, whether or not built into an operating system or network and capable of circumvention by technical means. The College is not responsible for preventing computer users from avoiding those restrictions; responsibility for knowledge and compliance lies with the computer user.

The Web is not governed by a single legal regime and is not exempt from the normal requirements of legal and ethical behavior within and by the College community. If conduct would be illegal or a violation of College policy in the physical realm, it will almost certainly be so in an online world. Computer users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those other states and countries and the rules or policies of those other systems and networks. When a computer user sends an email to another jurisdiction, that other jurisdiction’s laws are implicated in the same way that a New York State driver is subject to the traffic laws of Ohio while traveling through that state. Effectively, one has consented to jurisdiction.

*It is impossible and arguably of little utility to list and describe every law and policy that applies to the use of College computing resources and in particular to use of the Internet through those resources. The following broad categories serve as an illustrative guide to those areas typically causing the most or most severe problems.*

**Copyright**

Copyright law generally gives authors, artists, composers, and other such creators the *exclusive* right to copy, distribute, modify, and display their works or to authorize other people to do so. Moreover, their works are protected by copyright law from the very moment they are created – whether or not they are registered with the Copyright Office and whether or not they are marked with a copyright notice or symbol ©. Virtually every e-mail message, webpage, or other computer work you have ever created – or seen – is copyrighted. Unless you are the copyright owner of the work, you may not distribute copy, display, or modify that work unless one of the following circumstances applies:

* The copyright owner has given you permission to do so; *or*
* The work is in the public domain; *or*
* Doing so would constitute fair use; *or*
* You have an implied license to do so.

If none of these exceptions applies, your use of the work constitutes copyright infringement, and you could be liable for as much as $100,000 in damages for *each* use. In addition, if you reproduce or distribute copies of a copyrighted work having a total retail value of at least $1000 (which could include, for example, posting a $50 software program on a webpage or newsgroup from which it is downloaded 20 times), your actions may also be *criminal* – even if you do it for free.

It’s typically easy to determine if you have permission to make a particular use of a work – the copyright owner will have assented expressly, either in writing or orally – but it’s not always so easy to tell whether the work is in the public domain or whether what you want to do constitutes fair use or is covered by an implied license.

Placing a work on the Internet is not the same thing as granting the work to the public domain. Generally speaking, a work found on the Internet, like a work found anywhere else, is in the public domain only if (a) its creator has expresslydisclaimed any copyright interest in the work, (b) it was created by the federal government, or (c) it is very old. Sharing a music file containing medieval chanted composed by an anonymous artist or one whose composition has been contested *may* not constitute copyright infringement. Sharing the Beatles’ White Album *is* copyright infringement. Unfortunately, just how old a particular work must be to be in the public domain depends in part upon when the work was created, in part upon whether and when it was formally published, in part upon whether and when its creator died, and in part on still other factors, so there is no one specific cutoff date for all the works to determine whether or not they are in the public domain.

In very general terms, a particular use of a work is “fair” if it involves only a relatively small portion of the work, is for educational or other noncommerical purposes, and is unlikely to interfere with the copyright owner’s ability to market the original work. A classic example is quoting a few sentences or paragraphs of a book in a class paper or, of more recent vintage, using a portion of streaming vidceo or video clips. Other uses may also be fair, but it is almost neverfair to use the entire work, and it is not enough that you aren’t charging anyone for your particular use. It also is not enough simply to cite your source (though it may be plagiarism if you don’t).

An implied license may exist if the copyright owner has acted in such a way that it is reasonable for you to assume that you may make a particular use. For example, if you are the moderator of a mailing list and someone sends you a message for that list, it’s reasonable to assume that you may post the message to the list, even if its author didn’t expressly say that you may do so. The copyright owner can always “revoke” an implied license, however, simply by saying that further use is prohibited.

In addition, facts and ideas *cannot* be copyrighted. Copyright law protects only the *expression* of the creator’s idea – the specific words or notes or brushstrokes or computer code that the creator used – and not the underlying idea itself. Thus, for example, it is not copyright infringement to argue in an American politics paper that Richard Nixon in today’s Republican Party would be viewed more as a liberal pariah than a staunch opponent of Communism even though someone else has already done so, as long as you use your own words. (The risk of plagiarism applies here as well even if you paraphase.)

Copyright law as applied to the Internet is dynamic. There are few static rules and the following general rules of thumb:

* You ***may*** look at another person’s webpage, even though your computer makes a temporary copy when you do so, but you may not redistribute it or incorporate it into your own webpage without permission, except as fair use may allow.
* You ***probably may*** ***not*** copy and redistribute a private e-mail message you have received without the author’s permission, except as fair use may allow.
* You ***probably may***print out a single copy of a webpage or of a listserv, or private email message for your own, personal, noncommerical use.
* You ***may not*** post another person’s book, article,graphic, image, music, or other such material on your we page or use them in your listserve, or private e-mail messages without permission, except as fair use allows.
* You ***may not*** download materials from a news service and copy or redistribute them without permission, unless the applicable license agreement expressly permits you to do so or unless your particular use would constitute fair use.
* You ***may not*** copy or redistribute software without permission, unless the applicable license agreement expressly permits you to do so. web page, even though your

**Libel**

Libel is the “publication” of a false statement of fact that harms another person’s reputation – for example, saying that “John beat up his roommate” or “Mary is a thief” – if it isn’t true. If a statement doesn’t harm the other person’s reputation – for example “Joe got an ‘A’ on the test” – it’s not libel even if it’s false. In addition, a statement of pure opinion cannot be libelous – for example, “I don’t like John” – but you can’t turn a statement of fact into a opinion simply by adding “I think” or “in my opinion” to it. “IMHO, John beat up his roommate” is still libelous if John didn’t beat up his roommate. If you honestly believed that what you said was true, however, you might not be liable if it later turns out that you were wrong.

A libel is “published” whenever it is communicated to a third person. In other words, if you say “Mary is a thief” to anyone other than Mary, you have “published” that libel. That means that almost anything you post or send on the Internet, except an email that you send only to the person about whom you are talking, is “published” for purposes of libel law.

A person who has been libeled can sue for whatever damages are caused by the publication of the libel. Since a libel on the Internet could potentially reach millions of people, the damages could be quite large.

A good rule of thumb to follow: If you would be upset if someone else made the same statement about you, think carefully before you send or post that statement to the Internet, because it might be libelous.

**Invasion of Privacy**

There are a number of different laws that protect the “right to privacy” in a number of different ways. For example, under the Electronic Communications Privacy Act, a federal statute, it generally is a *crime* to intercept someone else’s private email message or to look into someone else’s private computer account without appropriate authorization. The fact that you may have the technical ability to do so, or that the other person may not have properly safeguarded his or her account, does *not* mean that you have authorization. If you don’t know for sure whether you have authorization, you probably don’t.

Invasion of privacy, like libel, is also a “tort”, which means that you can also be sued for monetary damages. In addition to the sorts of things prohibited by the Electronic Communciation Privacy Act, it can be an invasion of privacy to disclose intensely personal information about another person that that person has chosen not to make public and that the public has no legitimate need or reason to know – for example, the fact that someone has AIDS -- if he or she has not revealed that information publicly. Unlike with libel, a statement can be an invasion of privacy even if it is true.

**Obscenity, Child Pornography, and “Indecency”**

Under both state and federal law, it is a *crime* to publish, sell, distribute, display, or, in some cases, merely to possess obscene materials or child pornography. These laws also apply equally to the Internet, and a number of people have been prosecuted and convicted for violating them in the context.

The line between what is obscene and what is not is hard to draw with any precision. A U.S. Supreme Court Justice said, “I could never succeed in intelligibly” defining obscenity, “[b]ut I know it when I see it” – but the term basically means hard-core pornography that has no literacy, artistic, political, or other socially redeeming value. One reason that it is so hard to define obscenity is that it depends in part on local community standards; what is considered obscene in Portland, Oregon may not be considered obscene in Poland, New York. That makes it particularly difficult to determine whether materials on the Internet are obscene, since such materials are, in a sense, everywhere, and it is therefore not enough that the materials are legal wherever you are. The operators of a website in California containing materials that night not be considered obscene there could conceivably still be found to have violated Alabama’s obscenity laws if downloadeded there.

Child pornography is the visual depiction of minors engaged in sexually explicit activity. Unlike obscenity, child pornography is illegal *regardless* of whether it has any literary, artistic, political, or other socially redeeming value.

Sexually oriented materials that do not constitue either obscenity or child pornography *generally*

are legal. Still, it is illegal in most cases to provide such materials to minors, and displaying or sending such materials to people who do not wish to see them will almost certainly be a violation of the College’s Sexual Harassment policy.

**“Hacking” and Similar Activities**

Under the federal Computer Fraud and Abuse Act and similar other state and federal statutes, it can also be a crime to access or use a computer without authorization, to alter data in a computer without authorization, to transmit computer viruses and “worms” over computer networks, to conduct “email bombing”, and to engage in other such activities. Engaging in such activities can also make you liable for monetary damages to any person who is harmed by your activities. Again, the fact that you may have the technical ability to do any of those things, or that another computer owner may not have properly safeguarded his or her computer, does *not* mean that you have authorization. If you don’t know for sure whether you have authorization, you probably don’t.

**Peer-To-Peer File Sharing**

The music and entertainment industries have luanched federal and state lobbying campaigns in recent years to prohibit, limit, and in many cases, criminalize unlawful file sharing. The progenitor of this issue in the music industry was Napster, which enabled massive file-sharing to occur without payment of any royalties to creators or performers of music. The entertainment industry lobbied successfully for enactment of the Digitial Millenium Copyright Act, a federal statue requiring, among other things, that higher education institutions adopt policies that prohibit peer-to-peer filing sharing. It’s tempting, but dangerous, to adopt the Robin Hood approach: that stealing from big bad Disney to allow your little cousin to enjoy a pirated version of an animated classic is legal. It is NOT.

**Harassing Behavior**

It’s best to think of harrassing behavior in two ways. First, you can never text or tweet what you can’t say. So, sending an irate, all-caps I WILL GET YOU! message is just as threatening, and perhaps moreso, if deliered in text form rather than verbally. Simply put, anything that is unacceptable and violative of a harrassment policy in the physical realm is equally violative in the cyber realm. Moreover, computing resources enable harrassment in ways that might not be considered harassment in a physical environment. If college freshman Ned were to wave at classmate Nina every one of the six times he typically saw her walking with her friends on campus and scream out “Marry me!”, Ned would come off as silly and a pest but probably little more. Ned’s behavior would not be so sophomoric if he texted Nina multiple times during all hours of the day and night with the same entreaty.

\*Office of the Chief Information Officer. (2000, May 10). Responsible Use of Computing Equipment. Retrieved October 28, 2010, from Ohio State: http://cio.osu.edu/policies/responsible\_use.html