UNIVERSITY OF MARYLAND
University College

Learning Resource

Ethics

Computers, like any other tool, can be used for the best of purposes or manipulated to accomplish outcomes that are dangerous or illegal. There are well-established standards or guidelines that define the appropriate use of information technology (IT) and all the associated systems that support this technology—computers, networks, and so on. These guidelines form the basis of **IT ethics**.

Codes of Conduct: The Particular to the General

We will begin our study of ethics in the information technology setting by looking first at those issues that more immediately affect the employee in the document that describes use of the organization's IT resources: primarily computers and access to the internet. Subsequently, we will investigate the policies and guidelines that define the employee's expected behaviors related to more than just IT use—the employee code of conduct. Finally, we will look at the standards that outline the employee's relationship to the larger world outside the immediate organization.

User Access Agreements

Organizations expect employees to act ethically in all situations related to workplace behavior and use of the employer's resources. To act ethically means to make sound decisions about what is right and wrong and to act accordingly. Every time employees log onto their computers and click to accept the user access agreement, they agree to abide by the rules specified by the user access agreement.

Unauthorized "Surfing"

Rajiv is a new intern in the purchasing department at ABC Corporation. He completed orientation and systems training during the first week at work and is now eager to start working. Every morning Rajiv's manager promises to meet and give him assignments, but his manager just can't seem to fit Rajiv's training time into his

schedule. Day after day, Rajiv comes to work, logs into his computer, clicks "I accept" on the user access agreement, then opens his company-provided email account and the internet browser installed on his work computer.

Rajiv has internet access at work for conducting company business by email and for ordering supplies and services. Since Rajiv doesn't have any work to do, he rationalizes that a little surfing on the computer wouldn't hurt anything, and it would keep him from getting so bored every day. The following week Rajiv's manager asks to speak with him privately. He tells Rajiv that he's been fired for surfing the internet, which violates the company's user access agreement. Each time Rajiv clicked "I accept" on the user access agreement, he agreed to abide by the company's policy.

The user access agreement consists of rules outlining the activities that are acceptable and those that are not when using the employer's computers, network, e-mail system, website, databases, and any other forms of IT-related resources. This agreement is often called an **acceptable use policy**. What type of language might such an agreement contain?

Acceptable Use Policy (adapted from UMUC, 2018):

Though the list here is brief, a well-written user access agreement will contain a longer and more exact list of acceptable and unacceptable behaviors related to use of the company's computers and IT resources. Effective user access agreements will also contain examples of what is considered acceptable and unacceptable use, along with the sanctions or penalties for misusing the company's resources. Generally, you will find specific sections that deal with security, online etiquette, and valid use or misuse of the organization's resources.

1. Employees should use only the computer systems, network accounts, and computer applications and files that they are authorized to use.
2. Employees may not use another employee's network account or attempt to steal or ascertain another employee's password.
3. Employees are responsible for all computer resources assigned to them, including both hardware and software, and shall not enable or assist unauthorized users to gain access to the company's network by using a computer.
4. Employees must not share their passwords with other employees or nonemployees and must take all reasonable steps to protect their passwords and secure their computer systems against unauthorized use.
5. Employees may not attempt to gain access to protected/restricted portions of the company's network or operating system, including security software and administrative applications, without authorization.

6. Employees must not use the company's computer resources to deploy programs, software, processes, or automated transaction-based commands that are intended to disrupt other computer or network users or damage software or hardware components of a system.
7. Employees are responsible to promptly report any theft, loss, or unauthorized access of the company's network system, or illegal disclosure of any proprietary information.

Note: If you conduct additional research on the topics here, you may find differences in how the components or documents are labeled: agreements, policies, guidelines, standards.

An example of a modifiable template for a complete user access agreement (http://www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf) (more commonly called an acceptable use policy), is provided by the SANS Institute (2014).

Rajiv's mistake was that he violated the user access agreement by surfing on the internet when he didn't have any work to do. Clicking "I accept" on the user access agreement is necessary to gain computer access. It is of paramount importance to know and comply with the terms of the agreement to maintain your computer access.

You might argue that Rajiv was never warned that his actions were violating the user access agreement, or that his supervisor was at fault for not finding the time to complete Rajiv's training. The scenario is lacking several critical details as to why this action was taken. The language of the user access agreement must be specific as to the actions to be taken when a violation occurs. For example, Rajiv's employment termination might have been a result of a sanction such as this: "Failure to observe these policies will result in immediate disciplinary action or termination at the discretion of the offending party's supervisor or department head."

Rajiv had completed orientation and system training, and it is assumed that he knew the contents of the user access agreement. And when Rajiv clicked on the "accept" button when logging onto the internet, he was acknowledging that he understood the actions allowed and prohibited by the user access agreement.

The Employee Code of Conduct

Expected Behaviors in an Organization

Compliance with the user access agreement is one of an employee's expected behaviors within the organization. A user access agreement is typically part of a larger document that outlines both the mission of the organization and the organization's approach to employee behavior on the worksite. This document, often called the "employee code of conduct," contains the following (New South Wales Government, Industrial Relations, n.d.):

So the user access agreement previously discussed would be a specific example of a set of guidelines that might be found in such a document.

- policies that outline the principles and practices that enable an organization to meet its stated mission or purpose
- the steps the organization will take in dealing with operational activities and how to respond to requirements to comply with federal and state legislation and regulations
- procedures that explain how to perform tasks and duties, who is responsible for what tasks, and how the duties are to be accomplished
- guidelines listing appropriate behaviors (and sanctions for violation of these behaviors) related to a range of topics: harassment, safety, workplace attendance, drug and alcohol use in the workplace, religious exercise, and computer use, for example

These policies, steps, procedures and guidelines define the "what and when" for running the organization and also define the organization's expectations of all employees collectively. The "what and when" in the organization means what needs to be done and when it needs to be finished.

What's the Difference Between Policies and Guidelines?

In an organization, employees are responsible for complying with both policies and guidelines. Both are binding and are enforced, and both concern the organization's operation. The major differences between the two have to do with the authoring body and specificity. Policies tend to be larger, relatively static documents authored and approved by an organization's governing body, most often its board of directors. Policies are intended to be useful and applicable over time. To that end, they are normally written with some degree of flexibility so that they can be adapted to changing circumstances. Specific penalties and expectations are not usually included in a policy.

Guidelines are based on policy, but they tend to focus on a specific series of steps in the functional area. Guidelines are normally approved and changed by the department or division most affected by them. This approach puts authority in the hands of knowledgeable staff. Because fewer individuals are involved in the drafting and approval process, guidelines can be changed and adapted more quickly than policies. Guidelines are typically much more explicit than policies in defining what's allowed and specifying the penalties for particular violations.

For example, an organization's policy may state that everyone needs to have a user ID and password to access a desktop computer. The organization's guidelines may state that the password must contain eight characters with at least two numeric digits and two uppercase letters.

As a general rule, an employer expects you to behave as a responsible, mature, and ethical person. In day-to-day terms, this means being respectful of your coworkers and of the organization's resources. Be aware that your use of the organization's resources can have an effect on others' use of them. Broadly, it's expected that you will:

As it relates specifically to use of computer resources, the code of conduct outlines the employer's expectation that computers, email, and the internet will be used primarily to conduct the company's business.

- maintain the security and confidentiality of your user ID and password
- take care of any property assigned to you
- use your knowledge of organizational information in a responsible way
- use the organization's supplies and services for official purposes only
- be respectful of others' property and privacy rights

Professional Associations and Codes of Conduct

Codes of Conduct

We've covered the user access agreement and learned about an organization's policies and guidelines as applicable to the employee code of conduct within an organization. Another way to look at what we've covered is that we first described the expected, ethical behavior of the individual as outlined in the user access agreement. Next, we learned that policies and guidelines define the "what and when" for running the organization and also define the organization's expectations of all employees collectively (as found in an employee code of conduct).

Now, we take one step further in our discussion to describe general standards applicable to and the behaviors that are expected of individuals who belong to professional associations or who have obtained certifications in a particular field of expertise. How do these codes of conduct differ from those written for a particular company, business, or institution?

Many professional careers are not regulated by any external bodies such as federal and state governments. Unlike doctors or accountants, for example, IT professionals do not have specific regulations that govern their behavior, outside of established laws regarding any type of illegal activity. Thus, professional organizations like those supporting IT professionals develop a code of ethics, which is intended to guide and govern the behaviors of its members. This, in one sense, is an attempt at self-regulation and ensuring that the members demonstrate behaviors that reflect positively on the organization and that profession as a whole.

When you look at the codes of ethics for such groups such as the Association for Computing Machinery or the SANS Institute, you will find many of the same topics addressed as those found within any single organization's employee code of conduct—being respectful of others' property and privacy rights, using resources only when authorized to do so, using knowledge of organizational information in a responsible way, and the like. The basic elements of the code of ethics in professional associations revolve around members conducting themselves "honorably, responsibly, ethically, and lawfully so as to enhance the honor, reputation, and usefulness of the profession" (NSPE, 2007).

These professional associations provide a collective voice for members who are focused on a particular field of expertise. The associations attempt to promote professional ethical standards among their members. But the code of ethical conduct for a professional association is written with less specificity than an employee code of conduct. The contents are presented as standards of behavior and do not include the details of "who, what, and when" that are found in an employee code of conduct. In a code of ethical conduct for a professional organization, you might find phrases such as:

Of course, these same standards of behavior are part of any employee code of conduct, but in that setting, there are generally specific policies and guidelines to be followed in support of these standards. If we look at one item in all three documents (the ethical code of conduct for a professional association, the employee code of conduct, and the user access agreement), the same topic might be addressed in the following ways:

- "I shall perform with honesty and integrity in all my professional relationships."
- " I shall not use my knowledge and experience in the field to take advantage of others, thereby achieving personal gain."
- " I shall be willing to share my knowledge and expertise with others and always act in such a way that reflects favorably on my profession."

An IT professional with a network engineering certification, faculty members in a university with membership in the Middle States Association of College and Schools, or a union plumber working on a construction site are a few examples of individuals who, by virtue of their membership in a particular professional association, have subscribed to the code of ethical conduct for that organization. Professional certifications and memberships convey an assurance that the individual with the certification or membership has agreed to abide by the established code of conduct.

Ethical Code of Conduct for a Professional Association	Employee Code of Conduct	User Access Agreement

Ethical Code of Conduct for a Professional Association	Employee Code of Conduct	User Access Agreement
"I shall protect the privacy and confidentiality of all information entrusted to me."	"The employee will maintain the security and confidentiality of his/her user ID and password."	"The user ID and password are to be used only by the authorized owner of the account and only for the authorized purpose specified by the owner's job description."

One reason organizations hire certified professionals is to establish themselves as organizations with competent and ethical professional employees. The rapidly changing nature of technology makes a general standards approach very practical—it's much easier for organizations to rely on the credentials established by the certifying professional organizations and boards than to hire employees without knowing their level of expertise or their ethical and moral standing. An organization with a highly ethical and competent staff distinguishes itself because the general standards of competency have a high level of credibility in the workplace.

Standards and Behavior

Jenna is a network engineer and holds a Microsoft Certified Solutions Expert (MCSE) certification. This certification attests to Jenna's ability to design and implement computer network systems. Chad holds several Certified Information Systems Security Professional (CISSP) credentials. These credentials signify that Chad has the experience to handle all issues related to information systems in business environments, particularly those that relate to security of the systems. To obtain these professional certifications and credentials, Jenna and Chad had to agree to act in accordance with high moral and ethical standards in all activities related to that profession. They also had to pass examinations to prove that they had the appropriate subject knowledge. Therefore, a professional certification attests not only to Jenna's and Chad's subject knowledge, but also to their high ethical standards and behavior in their professional lives.

IT Ethical Issues

Software Piracy

Even though you have purchased a legitimate copy of this software for your use, lending it to another person, even for a short time, is a violation of the license agreement you agreed to when you installed the software on your machine. You are not allowed to lend (or borrow) software, and doing so is a violation of copyright law. In general, US copyright law makes it illegal to distribute or reproduce copyrighted work without the consent of the copyright holder. These laws have a long history in the United States, and they are rooted in the idea that strong intellectual property rights encourage invention and creativity.

Legal to Lend?

Jeff is upgrading his computer and has an old version of a document creation/editing program. He asks to borrow your installation CDs for the newer version of the same software application to load onto his machine until he has a chance to purchase his own copy. You give him the CDs, and he loads the program on his machine. But when he attempts to open the program, he gets notification that he needs to register the application. He uses the activation code that is still attached to the back of the set of CDs you lent him. Eventually, Jeff purchases his own copy of the software and loads it on his machine.

It can be difficult to understand that software piracy is theft because the thief isn't taking anything physically, and because retail merchants are not present when the theft occurs. It may seem strange that you can purchase something legally (like an iTunes song or an e-book), and its use will become illegal if you load it more than the allowed number of times. On the other hand, If you purchased a hardcover or paperback book, a music CD, or a movie on a DVD, you can lend that item to as many people as you wish (as long as they do not make copies).

Piracy, a type of software theft, occurs when software is illegally copied, registered, activated, released, or sold. Software includes data files, music files, videos, pictures, game files, e-books, computer applications, and operating system programs.

Software owners register or **copyright** their work to protect it. Software owners specify the method and terms by which the software is distributed or shared with users. So if you purchase a song from the iTunes store, you can load it or sync it with as many Apple devices as you own and up to five computers that you own, but you cannot legally sync or load songs from someone else's computer or Apple device to yours. To do so would constitute an infringement of the copyright on the song and transfer process claimed by Apple. Or you can purchase an e-book and download it to your computer and then transfer it to one or more electronic readers that you own—but you cannot transfer the book legally to someone else's electronic reader.

The victims of piracy are software manufacturers, writers, programmers, and owners of the software. Ultimately, legitimate customers who purchase software are victims of piracy as well, because the purchase price of software must increase in order to cover the losses incurred by theft.

What Is Copyright and Does It Really Apply to Digital Media?

What Is Copyright?

Copyright refers to a series of rights that are granted to the author of an original work. These rights focus on the reproduction and distribution of the work—specifically, "the right to control copying." Copyright owners are essentially given two specific entitlements: the right to exploit their own copyrighted work, and the right to stop others from doing so.

In the United States, copyright is automatically granted to the creator of a work. Copyright protection remains in effect for the life of the author plus an additional 70 years. Although individuals and companies concerned about protecting their copyright will often place an explicit copyright notice on the work (e.g., "© 2010, all rights reserved"), this notice is not required for the work to qualify for copyright protection.

What Can Be Copyrighted?

US law specifies eight general types of works that are copyrighted. These works are specified below:

These include CDs, DVDs, video games, software, songs, poems, movies, plays, books, databases, label designs, photographs, and websites.

- literary works
- musical works
- dramatic works
- pantomimes and choreographic works
- pictorial, graphic, and sculptural works, including fabric designs
- motion pictures and other audiovisual works
- sound recordings
- architectural works

What Cannot Be Copyrighted?

According to the US Copyright Office, "Copyright does not protect facts, ideas, systems, or methods of operation, although it may protect the way these things are expressed."

It's important to point out that as a university student, you are likely going to be creating original work throughout your academic career. Copyright law applies to you not just as a consumer, but also as a creator of original work. In that capacity, copyright can protect the work you own from being used without your permission. Do you think asserting your rights under copyright law in your student work is never worth the time and effort? Consider these cases:

What's Special About Digital Media?

- Student Sues Professors Over Intellectual Theft (http://www.africaresource.com/index.php?option=com_content&view=article&id=448:binghamton-university-doctoral-student-sues-professors-over-intellectual-theft&catid=136:race&Itemid=351)
- Who Owns Your Great Idea? (http://www.nytimes.com/2009/01/04/education/edlife/whoseidea-t.html?_r=1&ref=edlife)

Given that copyright law has more than 300 years of history behind it, why has this issue suddenly become so contentious and prominent in the news? Has copyright law always been as problematic as it is today? For most of its history, the topic of copyright has been reasonably established and settled. It's only recently that the topic has become so newsworthy. Much of this attention is the result of changes in technology that make reproduction and distribution much easier. Think of how much easier it is to distribute a document digitally than in paper form, or to send friends a digital image compared to mailing a printed photograph.

Since that case, technology has continued to lower the cost and burden of reproducing copyrighted work, most particularly media files—text, images, and audio and video recordings. Similarly, advances in telecommunications have reduced the cost of distributing such files. Much of the current controversy stems from the combination of personal computers and the internet. Together, these technologies make reproducing and distributing copyrighted work exceptionally inexpensive. These technologies have enough potential to affect copyrighted works for which laws were put in place in the United States specifically to address the issue.

Current concerns over copyright have their roots in the 1970s, when Sony popularized videocassette recorders (VCRs). Until then, reproducing and distributing most forms of copyrighted work required expensive equipment. The expense of reproduction generally protected copyright holders from easy reproduction of their work. The widespread consumer adoption of the VCR suddenly made reasonably high-quality reproduction of

copyrighted works easy and inexpensive. Concerned movie studios filed lawsuits against Sony, culminating in a Supreme Court case (http://en.wikipedia.org/wiki/Sony_Corp._of_America_v._Universal_City_Studios,_Inc.) that protected the use of potentially copyright-infringing technology when the technology in question had other (noninfringing) uses.

The Digital Millennium Copyright Act (DMCA) of 1998

As advances in technology made copyright infringement easier and less expensive, major copyright owners sought additional protections to make such infringements easier to penalize. At the same time, because the internet plays such a prominent role in this potential infringement, both internet service providers (ISPs) and online service providers (OSPs, those that host websites on the internet) sought limits on their own liability if their networks and systems were used as a conduit to infringe on copyright.

Congress was concerned that without limiting the liability of online service providers, the efficiency and growth of the internet as an important technology would be stifled. The Digital Millennium Copyright Act (DMCA) was the legislative product of this controversy. The law specifically sets out expectations and safe harbors for ISPs. Under the DMCA, ISPs are encouraged to provide and improve online services such as network access (thereby allowing their users to transfer files), but if illegal activity is detected, the ISP is obligated to ensure that these illegal transfers or publications of copyrighted materials do not continue.

So does the DMCA protect the copyright holder or just set the liability limits for OSPs and ISPs? If you find that digital material for which you hold the copyright is appearing on a site owned/managed by an online service provider (OSP) such as Facebook, Twitter, YouTube, etc., you have the right to demand that the OSP remove the material. This is called a "takedown notice," and when an OSP receives such a notice, it is required to remove or disable access to the accused material to avoid being held liable. This portion of the DMCA "gives individual authors more power to protect their rights. At the same time, the DMCA takedown mechanism has certain safeguards in place to protect the rights of those who have a right to publish material that is not infringing" (Liu, 2013).

Under the DMCA, copyrighted works are given specific protections that prohibit the circumvention of technological measures that control access to and prevent unauthorized duplication of copyrighted works. The law also increased penalties for copyright violations.

The DMCA goes beyond penalizing those for reproducing copyrighted software. Under the law, it is illegal to bypass any protection the software manufacturer built into the software. Developing, selling, and owning the tools to carry out the bypass are also illegal under the law.

Prosecutions for copyright infringement and related news coverage of the issues of copyright protection and enforcement have increased dramatically in the past decade. These increases reflect the importance of this issue and the hard line contemporary copyright owners take on copyright violations.

It may seem remote that you'd be caught violating the DMCA because your actions would be on such a small scale. Consider that if you are caught violating these laws, you can be liable for civil penalties of up to $150,000 per violation. You could also face criminal prosecution, with fines and penalties. Is the risk of getting a criminal record and paying a hefty fine worth the reward of having pirated software?

A Specific Issue Related to Software Piracy: File Sharing

File sharing is the process of transferring files across a network (often the internet). Although any type of file can be shared, most file sharing revolves around media files: music, movies, and video games. Many different applications can be used to share files, including FTP, Internet Relay Chat (IRC), operating system sharing capabilities, web pages, and peer-to-peer (P2P) applications.

Any type of file sharing that infringes on copyright is illegal, but most media and legal attention is focused on the use of P2P applications. Although there are legal uses for P2P technology, these applications are especially popular for exchanging files illegally. This popularity stems from their efficiency—many popular P2P applications offer a fast way to download and upload information—and also from a perception of anonymity. Because users are sending or receiving files with other users (peers), many users mistakenly believe that their identities can't be tracked. In reality, computers that use P2P applications to upload or download files can be identified by their IP addresses.

Given all of the risks and possible repercussions, why would anyone ever use P2P to share digital files? Are there any legitimate uses for the technology? In fact, there are. File-sharing applications can be an efficient and effective way to share information. As a mechanism for sharing content that you've created yourself—whether informational, multimedia, or software—P2P applications represent a legal and effective approach.

This same technology can be a useful way to gain access to material that is not copyrighted, or that has licensing such that it's legal to share it. Sometimes it seems as though P2P file sharing is mentioned solely in conjunction with downloading movies and music illegally, but these applications have plenty of legal uses. P2P programs provide an efficient method for obtaining files that are in the public domain or are licensed to allow electronic distribution. If you choose to use file-sharing technologies, the onus is on you to make sure that you are doing so legally and safely.

Social Networking Issues

The Benefits of Social Networking

Social networking is ongoing communication between people, and in that form has existed ever since humans joined together in communities. However, now the term has taken on a particular meaning since it more often refers to groups that communicate on the internet. The reasons for joining these online groups are varied and include sharing of interests, photos, videos, stories, affiliations, and product and service reviews. Such sites are also used as a forum for professional contacts with the purpose of exchanging work-related information, posting jobs, or posting resumes from those seeking jobs. Another use, made possible by the large number of public databases that store information about individuals, is searching for information about persons, including police records, tax records, and other details.

One of the positive outcomes of this new form of social networking is the ability to contact and come to know people from any part of the world, exposing the participant to countries, cultures, languages, and customs that might never be made available in the individual's local community. Some of the most popular networking sites are Facebook, Instagram, Twitter, Flickr, LinkedIn, YouTube, Pinterest, and Meetup. Participation in any of these can lead to an expanded list of friends and a sense of belonging to a community. It can provide a source of information to help with a problem. It gives you a voice for your opinions and a place to connect with people who like the same things.

The Dangers of Social Networking

While conventional social networking follows accepted normal behavior, there are unethical and even criminal uses made of the information that is available on social networking sites. An individual can become the victim of data theft or unwittingly download a virus. One of the more significant dangers involves online predators or those who claim to be someone they are not. We will take a look at two such dangers—cyberbullying and cyberstalking.

Cyberbullying

Cyberbullying is defined as actions that use information and communication technologies—the internet, web pages, discussion groups, instant messaging, or text messaging—to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm another or others. These communications seek to intimidate, control, manipulate, put down, falsely discredit, or humiliate the recipient ("Cyberbullying," 2016).

Although we most often hear about this negative use of social networking among minors, resulting in disastrous actions such as school shootings, suicides, or even murders, adults can be victims of cyberbullying as well. Cyberbullying has an advantage of anonymity. The bully or bullies do not face the victim but communicate from untraceable cell numbers, fake

email accounts, or fake online IDs at popular social networking sites. The online actions can include such content as sexual remarks, hate speech, false accusations, gossip or rumors, online ridicule, or threats of harm or death. Victims often suffer in silence rather than face being ostracized by their peers.

Cyberstalking

Cyberstalking, also called **cyberharassment,** is a pattern of behavior that involves repeated continuous, unwanted communication to an adult. It is the adult version of cyberbullying. In the workplace, it can take place via company websites, blogs, or product reviews. It can escalate to criminal behavior if the stalker's behavior is threatening or invades the privacy of the victim.

This cyberharassment or stalking results from many of the same factors that give rise to cyberbullying: professional or sexual obsession, perceived failure with life or job, wanting to make others feel inferior, a delusional belief that he/she "knows" the target, and the assumption of anonymity. In the workplace, the cyberstalker may also be motivated for economic reasons—perhaps the victim is an affiliate or a competitor ("Cyberbullying," 2016). Under the US federal cyberstalking law, anyone who uses electronic means to repeatedly harass or threaten someone online can be prosecuted.

Whether it is called cyberbullying or cyberstalking, there are several key identifiers for this type of behavior:

Perhaps one of the greatest dangers involves an invitation to a meeting between the victim and the cyberstalker ("Cyberstalking," 2016).

- The perpetrator seeks to damage the reputation of the victim by posting false information about the victim on websites.
- He or she may gather personal information about the victim through the victim's friends, family, and/or coworkers.
- A technically savvy stalker may attempt to trace the victim's IP address to gather more information about the victim's online presence.
- Sometime cyberstalkers involve others; they may even claim that the victim is harassing them to encourage others to join in the harassment of the victim.
- The cyberstalker may try to damage the victim's computer by sending viruses.
- Purchases or magazine subscriptions (often involving pornography) may be made in the victim's name.

There are some elementary steps you can take to keep yourself and the information about you safe. Think about these:

- Look at your postings through the eyes of employers or potential employers. Do not post anything that might be embarrassing in your current or potential employment situations.
- Never post private information (phone numbers, addresses). These details can be used to track you down, possibly by someone who wishes to exploit your identification.
- Control who has access to your postings by adjusting privacy settings.
- Use strong passwords and change them regularly.
- Check to see how visible your name or identity is by "Googling" your name.

References

Cyberbullying. (2016). In *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/Cyberbullying

Cyberstalking. (2016). In *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/Cyberstalking

Liu, K. (2013, March 6). The DMCA takedown notice demystified [Blog post]. Retrieved from http://www.sfwa.org/2013/03/the-dmca-takedown-notice-demystified/

National Society of Professional Engineers (NSPE). (2007, July). Code of ethics. Retrieved from http://www.nspe.org/resources/ethics/code-ethics

New South Wales Government, Industrial Relations (n.d.). Workplace policies and procedures. Retrieved from http://www.industrialrelations.nsw.gov.au/oirwww/Employment_info/Managing_employees/Workplace_policies_and_procedures.page

SANS Institute Consensus Policy Resource Community. (2014). Acceptable use policy. Retrieved from https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy

University of Maryland University College. (2018). *Acceptable use of technology policy*. Used under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license.
