TET1 Task 1: Ethics

Melinda Gillette
Student ID: 000943219
Program Mentor: Robbyn Michaels
Assessment Code: TET1 - Task 1
August 2, 2018

A Written Project Presented to the Faculty of the Teachers College of Western Governors University
TET1 Task 1: Ethics

This paper will discuss possible threats and their corresponding safeguards for electronic resources for learners.

**Instructional Setting**

For the math classes at the urban high school (grades 9 to 12) students are grouped by ability and not by age/grade. In total, the high school has approximately 800 students. For this task, the focus will be on the students in the college prep Algebra 1 classes (2 sections). College prep level classes are meant to prepare students who will continue onto to college after high school. With that, there comes varying degrees of motivation ranging from students who are very motivated (should have been in Honors/Advanced level) to students who are not motivated at all (should have been placed in the lower general level class).

**Learners in the Instructional Setting**

The learners are the high school college prep level math students. This 27-member audience is from an urban setting and has 13 boys and 14 girls. The 27 students are made up of 17 freshman, 8 sophomores, and 2 juniors. In this small target population there are 14 (52%) students who are white, 9 (33%) students who are Hispanic, and 4 (15%) African American students. Another unique characteristic of the target population is that there are three students (11%) who receive special education services (either through an IEP or a 504 Plan). The third unique characteristic of this group is that there are five students (19%) who are bilingual, one of whom is enrolled in the English as a Second Language classes at the high school.

**Protective Measures for Safeguarding Electronic Resources**

Electronic resources are abundant in today’s world, both in and out of the classroom. There are many pros and cons about using electronic resources. The pros far outweigh the cons, and the
risks associated with many of the threats can be minimized. In the brief discussion that follows, three threats will be discussed as well as ways to safeguard and minimize the risks that comes along with each threat.

The first threat that will be discussed is viruses. If there a computer acquires a virus, the results can be disastrous. There are many different types of viruses, but none of them are good. Viruses can attach themselves to files and can either be sent through email or downloaded attached to a file or program. (Roblyer, 2012, p. 219) They can either be sent with the purpose to destroy or be attached accidently. There are a few safeguards a person can take to minimize the risk of their computer catching a virus. The first of these safeguards is the most obvious; keep virus and malware/spyware software on your computer up-to-date and scan your computer often for threats. Another safeguard to minimize your computer’s risk of being infected by a virus is to not open emails or email attachments from unknown sources, as these often contain a virus that will automatically infect the computer. Before opening email attachments even from a familiar source, make sure that the person intended to send an attachment. There are viruses that will add attachments without the original user knowing, trying to infect as many computers as possible. When it comes to downloading files and programs, only download from reputable sources. Stay away from shareware, as many times viruses thrive in environments like that.

Another threat, especially to children and the elderly are online predators. These predators manipulate vulnerable people into giving them things like money and doing illegal things. This issue has been in the headlines a lot and is a huge issue in technology. There are many safeguards that a person can take to minimize the risk of being manipulated by a predator. The first and most obvious is to never ever give out personal information (name, address, phone number, social media information, and for a child where they attend school). The vulnerable populations (children and the elderly) need to understand that the people they are talking to online, may not actually be who
they say they are. Predators will often lie to gain the person’s trust and luring them into a false sense of security. Teens often post a lot of pictures on their social media sometimes with personal information, such as a location tag. This allows predators to ‘get to know’ their victim before they contact them, so they sound like a familiar person to the victim. Additionally, pictures can easily be misused and altered for other purposes by anyone. So, another safeguard, is to be aware of what is being posted on social media and the risks that comes along with potentially ‘over-sharing.’

Predators will also try to alienate the child from their family and try to get their victims to meet in person. (Education, 2007, p. 8) If a person feels that they are in a potentially dangerous chat or situation, they need to tell an adult or appropriate law enforcement.

The third threat to be discussed is accessing inappropriate content i.e. violent images/videos, pornography, etc. There are many safeguards to prevent students from accessing, either purposefully or accidentally, inappropriate material. Most schools have installed firewalls which prevents a computer for unauthorized users to gain access and prevents certain sites and filtering software which protects a computer from going to certain sites based on keywords, a list of specific sites or a combination of both. (Roblyer, 2012, p. 217) If children are using electronic resources at school, teachers should monitor what the students are doing by either walking around the room and/or use software to remotely monitor what the students are doing on their computers. When at home, parents can use the parental controls on their computer at home to restrict access to inappropriate materials. Online video games also may have inappropriate material in them, so parents and children need to be clear on what is appropriate and what is not. (Education, 2007, p. 9)

**Safe Practices for Use of Instructional Technology Tools**

There are many ways that technology can be used in instruction, including some very specific instructional technology (websites, programs, etc.) To safeguard against possible threats,
including those aforementioned, in addition to others, districts, schools, teachers and students should follow the following procedures to minimize risk of the threats.

The district and the school should have firewalls and/or filtering software installed on all computers to block access to unwanted and undesirable sites. These entities should also ensure that there is anti-virus and malware software installed on all computers and all computers should be scanned often for these types of threats. This is in addition to having a strong media usage policy, which parents and students sign, informing them of appropriate media use and that the policy will be strictly enforced.

Students should listen to their teachers when using instructional technology and precisely follow their directions. When on the internet, students should only navigate to the directed site or if they are conducting research they should only navigate to trusted sites. If students are unsure of a direction or the content on the site, they should ask their teacher, instead of just clicking on it. Students (and teachers) should also not open email attachments from unknown senders and not share any personal information. When using technology instructional technology teachers should be monitoring the students by circulating throughout the room/lab and/or by using monitoring software installed on their computer to remotely check in on what the students are doing. Some monitoring software allows the user to record what students are doing, so a teacher can go back and check on anything s/he thinks is suspicious activity on the students’ part. (Dove, n.d.)

Establishing Behavioral Expectations in a Technology Environment

To establish behavioral expectations when using electronic resources starts with a strict policy which is signed by both the student and their parent/guardian. This policy needs to be clear and concise. Students need to be held accountable for the policy, i.e. if a student disobeys the policy, then appropriate consequences need to be issued and followed through with. Teachers can instruct students about what the behavioral expectations are through scenarios, they should make it
fun and maybe a bit silly so the experience is memorable. Teachers can also give a presentation about the expectations. (Dove, n.d.)

References


