Academic Honesty Through Technology

Mark Lecher
Information Technology Services
Franklin College
101 Branigin Boulevard
Franklin, IN 46131
317.738.8148
mlecher@franklincollege.edu

Over the past two decades, technology use has increased in the classroom. What started out as a single computer in a classroom has evolved into a laptop or handheld for every student, with a wireless connection to the Internet and other network resources. Cell phones, PDAs, and other electronic tools have opened up new horizons for utilizing technology in the classroom to better educate students. With these advancements have also come the inevitable drawbacks. With ubiquitous connections to the outside world, students have even more resources to share information, knowledge, and work with each other. These same connections also allow students to access unprecedented means for plagiarism and cheating.

Today's students are in a "always connected" or "always on" mode where they have access to many different methods of communication. On most college campuses, there is an ever-present wireless network that students can use to access Internet resources. Students also use cellphones, PDAs, and PIMs to converse and communicate. With these different ways of communicating, they have the responsibility to use these resources wisely. Many times, students continue to use these tools during class time, even though they should be focusing on class work. The larger issue is using these communication devices during a test or quiz. How do educators keep students from sharing questions and answers?

This problem can be resolved in many different ways. It is difficult to say that any particular method will completely resolve these issues, but there are many steps to be taken that will mitigate these issues. Even though technology can play a big part in this process, standard, procedural methods can help also. If a student brings in a cell phone or a PIM, usually there is not an academic use for that equipment in the classroom, especially during a test or quiz. By banning those types of gadgets, and doing a spot check during an assessment, this issue can be quickly resolved. The larger issue, then, is keeping students honest when you don't have control over the situation.

Many times, it is beneficial to have access to word processing programs, in order for the students to submit good work. By using a word processor, students are usually able to work quicker, turn in multiple drafts of work, plus have the ability to spell check. The final result from a word processor is a much better product for both the student and the professor, in terms of readability and clarity. This becomes an issue in a classroom with desktop or laptop computers. The same tool used to word process also has access to outside resources (the Internet, local network, etc.) that can be used to dishonestly pull in previous work from various sources. While it is relatively easy to stop a student from using a cell phone in a classroom, it is hard to track a students' work on individual machines, especially when it is very easy to open a browser and gather information

from the Internet. It is not very obvious when students are cheating in this situation, which further complicates the matter.

In the summer of 2004, we faced this issue at Franklin College. There had been some demand over several previous semesters to find a solution to these issues. We discussed several possibilities, and originally had a difficult time finding a solution. One of the first requests was to turn off the network (wireless for the laptops, and wired connections for the desktop lab) in the classroom areas, so that students taking tests wouldn't be able to access outside resources. This was quickly dismissed, due to the overhead and time involved. Also, this had the added side effect of stopping legitimate network services. (Login, storage for backup, printing, access to others not in that class.)

The next idea was to create a solution using Linux or other open source software. The idea was to create a proxy server that would stop a particular lab from accessing the Internet and network drives, so students wouldn't be able to cheat in that manner. This was dismissed due to the complexity of setting up the proxy solution, and the added disadvantages of limiting network drive access for backup and long term storage for the files. Also, students would still be able to keep files on the local machines, which would still allow them to cheat.

A third solution was to look at using Perfigo, which we already had in place at Franklin College. This would function in a similar manner to the proxy – allow students access to certain services, but limit others. This still had the drawbacks of local storage ability, plus had some management overhead. (We were only able to lock out certain students, not physical machines. This was a problem for those students done early, as they would not have network access until the end of class time.)

In the fall of 2004, during a conversation with an adjunct professor, this issue came up again. The professor (who coincidentally is the Chairman of the Board of Trustees for the College) mentioned that he had heard of software called Securexam that would essentially lock down the computers and keep students honest. We did a quick evaluation and rollout to students to see how the software worked.

Securexam is a product released by Software Secure (http://www.softwaresecure.com). This product locks down Microsoft Word in such a way that the user is unable to access ANY resources on the computer, except for the MS Word program. The end user still has full capabilities of the word processor, but cannot access the Internet or any local files, until the student is finished. When the student is finished, the Word file is encrypted. The student cannot later open the file and make changes, since the file is encrypted. Once you exit Securexam, full capabilities are restored to the computer. The encrypted file can then be transferred to the instructor through any traditional file transfer means. Once the instructor has the file, there is a secondary program that decrypts the file back into a standard Word file. Along with the student's work, there is a header on each page that has the student's information, date, and time. There is a final page added on that gives usage statistics to show how long the student was using the program, and if the student tried to exit the program and re-enter later.

This solution proved to be very successful. Students were able to use word processing software to type their responses to a test, and professors could ensure that the students did not have access to resources typically found on a computer. The software is very robust, and even has built in features to help recover the file if something happens to kick the student out of the program. (This happened two or three times, and the student was able to fully recover every time.) The software will automatically save a copy every minute, which ensures that there will only be minimal data loss in the event of a power outage.

The software turned out to be relatively user-friendly, and students were able to quickly learn how to start and end the program. To collect the files, we had students submit the finished files to Blackboard, where the professor could later retrieve them. Then, the professor would de-crypt the files, and be able to print them or grade on-screen. This solution turned out to work well for faculty, since they were able to reliably control the resources available to the students, while still getting papers from students that were easy to read and retain.

This solution takes care of issues of academic honesty during an in-class test or quiz, but what about writing assignments outside of class time? Students still have access to the Internet and other sources. Students may be tempted to loosely copy other's work, or even plagiarize entire papers. Many times, professors can catch plagiarism through standard methods of comparing student work, but this doesn't always catch copied work, especially over time. Once again, technology can assist with this issue.

There are many resources and solutions for this issue on the market. At Franklin College, we have used the Wcopyfind program over the last several years. This is a free program provided by Lou Bloomfield at the University of Virginia (http://www.plagiarism.phys.virginia.edu/). This software does a great job of comparing files that you have access to on your computer, and it is free. However, it will only search local files (network drives, removable drives, or hard drives) on that specific computer. There are several other options that will scan against larger pools of work to detect plagiarism. One of the most popular is turnitin.com (http://www.turnitin.com). This program is web based, and allows professors to scan works submitted by students to check for plagiarism. At Franklin College, we evaluated this, but found it to be too expensive and harder to manage since it required a separate username and password. A resource that we are currently evaluating is called SafeAssignment (http://www.mydropbox.com) which is an add-in to Blackboard. This will allow students to use their current usernames and passwords to submit work, while still allowing the professor to compare the files to a large pool of work. The pricing for this solution is cheaper than turnitin.com, and is easier to use and administer than some of the other solutions. We are still in the process of evaluating this solution.

Technology continues to give new ways of teaching and learning. By implementing some of the above methods, it is possible to make sure that technology is used in a beneficial manner, and not in a way to further academic dishonesty.

Web sites:

Securexam – http://www.softwaresecure.com

Wcopyfind - http://www.plagiarism.phys.virginia.edu/

turnitin.com - http://www.turnitin.com

SafeAssignment - (http://www.mydropbox.com