

Brian Martel  
EDU 624

## The Appropriate Use Policy

The Pomfret Board of Education's appropriate use policy (AUP) is for the most part thorough and clearly defined in the staff handbook. It spells out the responsibilities and privileges of the students and faculty. The document includes a copy of the contract accepting the terms and conditions for grade 5-8 students associated with using technology. This contract requires the signature of the parent, student, and a sponsoring teacher. This contract is a real strength of the policy because it ensures that the student, parent, and teacher are all aware of the policy's regulations. I am of course assuming that care is given to provide parents with ample explanation of the AUP. Realistically, this does not always happen.

With respects to the Board of Education, however, the policy is left to much more interpretation. There are two things that trouble me with that. First, the policy states that "the Board of Education intends to monitor the use of computer systems to ensure that they are being used only for appropriate business and education purposes. To ensure proper use of the computer network and of the Internet and e-mail, private correspondence and/or files may be accessed at any time." (Pomfret BOE) In this day and age, privacy laws entitle many children the most extreme secrecy with regards to many different situations. I question as to the legality of checking a teacher's e-mail that includes such information about a student. The second issue I have is that disciplinary action, "up to and including termination of employment," is left completely up to the Board of Education. (Pomfret BOE)

That being said, there is a blatant infraction that happens at least 3 times a week by the administration alone. Faculty and staff are prohibited from "using e-mail for personal use not related to the business of the Board of Education." (Pomfret BOE) At least once a day, e-mails are sent from within our district, to our entire district, that contain personal stories not related to school or forwards of forwards. I have approached members of the administration about the inappropriateness of this practice with no success. In this

circumstance, I would say that violating policy is not enforced, and is actually encouraged by the administration.

### Public Access of District E-mail

The e-mail system can only be accessed by district employees, with a log on id and a password. What may be a weakness of the system, but is also of immeasurable benefit to teachers, is that e-mail can be accessed through an exchange from outside the school. If a teacher is sick or at a conference, etc. they can access school e-mail to stay in the know about what is going on at school. Although I could see disaster e-mails being forwarded to home addresses, not all e-mails can be scanned for their priority level. E-mails from parents can should not be assessed by anyone but the teacher nor forwarded to a teacher's home address.

All direct links to e-mail have been removed to discourage web crawlers, programs that scour the internet for direct links to e-mail. When these links are found they are subsequently spammed with e-mail. Instead teachers e-mails are spelled out with "AT" instead of "@", to prevent this.

Teachers often communicate with parents via e-mail. A number of teachers have created lists of parents that they send mass e-mails to with updates about field trips, class projects, and special events. This practice peaked the Board of Ed's curiosity about broadcast e-mail. They were quoted a cost of roughly \$1800 by a company to provide the school with mass information sharing (like snow days, early dismissals, and hopefully not disaster situations) to the parents via e-mail, text, and pre-recorded phone messages. The Board of Ed has since removed this program from the budget. The Board of Ed is also considering adding a banner to the school website that would inform parents of the same types of information.

### Protection from Contamination

Our new tech person has put a bit of work into tightening up security on our system. Before e-mails enter our e-mail's spam filter, they are run through a separate spam filter. Peckham, our tech person, reports that the school receives 2 legitimate e-mails for every

94 that come through the system. She reports that 20-50 viruses are filtered out of e-mails every day. Most of these viruses are Trojan viruses.

Our content filtering is provided by our ISP, the Connecticut Education Network (CEN). This operates on the N2H2 software interface. Administrative users in our school can access the N2H2 interface to add custom blocks, and allow access to a blocked site if necessary. This feature is utilized through a https browser authentication process.

Despite the administration's attempt to block "youtube" and "image" searches, the blocks have been easily maneuvered around. As I mentioned earlier in the semester, I have seen several staff members enjoying the UK version of youtube, and successfully searching the internet for "pics" or "jpgs". If the government can't stop illegal music downloads, can our school realistically stop picture and youtube searches?

Our information system is protected first by user log ins and passwords on the system drive where the data is located, then secondary log ins and passwords on the software. There are also firewalls that limit access to the server from outside the school. To access student information the Student Information System (SIS) the user must be inside the school.

Last but not least, a back up file is created every night, so that the system can be restored if contamination occurs. This has proved to be a lifesaver because access to our school web pages has been granted, against the request of our tech person, to many untrained users who have "unknowingly" altered and or erased portions and even the entire school web page.

## Conclusion

I am impressed, and in truth, unsure of what more can be done to protect our system any further by means of technology. However, human error and disregard for the AUP are problems that need to be addressed to maintain our system's integrity. It is painfully obvious from day to day how technologically inept some are, and how technologically deviant others are.