



Setting Clear Boundaries

ETHICS IN TECHNOLOGY

Why are we here?

- Student network comprises sixty computers dispersed throughout the classroom and lab environments
- Routine maintenance is performed on these machines by a group of volunteers and one staff member.
- During a recent maintenance period, several hacking tools were discovered on a few machines in two different classrooms.
- Unauthorized user accounts were found as well.

FBA Computer Usage Policy

- Students shall treat all equipment with care and report misuse of computers or other technology as soon as the student becomes aware of it.
- Students may not vandalize or intentionally damage FBA computers or software. Students will be responsible for the cost of repairs and/or replacement.
- Students are expected to respect the work of others and not damage, destroy, or copy another person's data without permission.
- Students may not tamper with or attempt to gain access to computer data to which he/she does not have security authorization.
- Students may not load or copy unauthorized software onto FBA computers.
- Network security is a high priority. If a student identifies a security problem or issues on the FBA network and/or internet, he/she must notify a staff member.

Why Does it matter?

- What is hacking?
 - Unauthorized access. Just because nothing prevents your access doesn't mean your presence is warranted or legal.
- Why is hacking bad?
 - Hacking is an invasion of privacy
 - Hacking potentially destroys property
 - Hacking potentially destroys information systems
 - Hacking can lead to theft of identity or intellectual property

Legal Ramifications

- IL 720 ILCS 5/16D-3: Computer Tampering
 - Class B misdemeanor for access
 - Class A misdemeanor for retrieval of information / Class 4 felony for repeat offenses
- IL 720 ILCS 5/16D-5: Computer Fraud
 - Class 3, 4 felonies depending on severity of damage, assessed by prosecution and investigative team

FBA Responsibilities

- Provide a safe and secure computing environment for the students
 - URL filtering blocking out inappropriate material
 - Antivirus coverage on the workstations
- Provide educational materials and training to the students on appropriate use of technology on campus
- Audit the FBA infrastructure frequently to look for tampering
- Individual user accounts with limited privileges

Student Expectations

- Use the technology for class assignments only
- Login only with your own credentials
- Do not share passwords
- Do not give your personal information while researching
- Lock or log out of your machine when you walk away, don't leave machines unattended when logged in
- Ask for software if it's necessary for a class project, don't attempt to download and install on your own
- Report misuse or abuse to your teachers, or send an anonymous note to the office

Ethical Behavior at Home

- Theft is wrong, this includes copyright violations
 - Ripping CD's is OK if you purchase the music and listen to it on your iPod. It's Not OK to share this music with others, you are preventing the artist's ability to make a profit off their work
 - Same is true of pirated software, such as Windows, Office, etc.
 - File sharing is ok if you are the creator/owner or the licensing is clear that it can be redistributed by you.

Protecting Students at Home

- www should stand for wild wild west, not world wild web, there is a lot of nasty, bad stuff out there, not just pornography
- URL filtering at home should be a must—NetNanny is the best
- Don't put PC's in your children's rooms, keep them in common areas and require at least another person in the room when the computer is in use
- Create restricted permission accounts for your kids that prevent installation privileges if you can't be around when they are online
- Know the social media sites/software and follow your children's usage (chat, Facebook, MySpace, Twitter, etc)
- Cell phone with Data plan? This is another avenue in which you'll need oversight

For the technically-inclined student...

- The creativity should be channeled, not stifled, maybe a home lab that is isolated from the world (and your home network)
- FBA may have a use for these skills, as the volunteer hours are never enough. We'll just need to work out an accountability system

Online Resources

- <http://www.netsmartz.org>
- <http://www.cybercrime.gov/rules/kidinternet.htm>
- <http://www.cybercitizenship.org/index.html>

Utilities

- KeePass - <http://keepass.info/>
 - This is a password database that will generate unique passwords and store them for each site you visit. If you install this on a thumb drive and carry it with you, you can keep unique usernames and passwords for each site so if one is compromised, not all is lost.
- AxCrypt - <http://www.axantum.com/AxCrypt/Default.html>
 - This is a file encryption application that installs to your right-click menu. This is good for any personal/financial data that you store on your computer.



Questions?

- jason.rahm@fbcofallon.org
 - richard.tippett@fbcofallon.org
 - jeremey.mayfield@fbcofallon.org
 - THANK YOU!
- 