DIGITAL ETHICS Q&A

A RESOURCE FOR TEACHERS & PARENTS

What are Ethics?

Simply put, it's the set of acceptable behaviors in a given culture. It's a well-taught code of conduct by which a society chooses to survive long-term.

- It's doing the right thing, trying to avoid hurting others.
- It's considering what's good for others before the self.
- It's taking responsibility for one's actions.

What are Cyber Ethics?

It's the code of behavior that governs the Internet and other forms of electronic communication in the "cyber-world."

What are some types of cybercrime?

General Intrusions (equivalent to breaking and entering in the real world)
- Hacking, spyware, phishing, pharming,
- Sending computer viruses & worms to invade computers
- Causing denial of service attacks
- Creating bots, Trojan horses, zombie machines

Nuisances (usually non-violent activities)
- Sending spam
- Changing web page text and images
- Redirecting websites

Personal (using someone else's name or credit)
- Phishing for private information, passwords, code numbers
- Making unauthorized purchases with stolen credit cards or ID
- Destroying personal reputation
- Damaging personal credit ratings

Theft of Intellectual Property (stealing ideas or creations of others)

- Downloading copyrighted music & videos
- Software piracy
- Plagiarism, cheating

Physical or Mental Damage

- Cyber-bullying, harassment
- Cyber stalking
- Sexual exploitation of minors, child pornography
- Terrorism
- Stealing military and private industry secrets - espionage
- Brainwashing and recruiting new followers
- Building terrorist communications network

What can parents do to promote safety in the home?

- Talk with the family about cyber-privacy & safety — financial, individual and family, emotional, physical.
- Talk explicitly about ethics with the family.
  Discuss with your family the need to keep information private and with whom and how it should be shared.
- The following information should never be shared online: (name, address, phone, cell numbers, home alarm password, combination to locks, code-names, location of sister's diary, etc.).
- Increase security on your home computers and lock files.
- Don’t open emails or attachments from unknown senders.
- Make your wireless network accessible only by password.
- Install firewall hardware and software.
- Use virus protection software and update it regularly.
- Discuss consequences of illegal online behavior. Some juveniles are being tried as adults, even in federal courts, and are being fined thousands of dollars. They are being given actual prison sentences for cyber-crimes, and are being barred from using the Internet. Parents are being held responsible for the crimes, must pay restitution, keep children under house arrest, etc.
- Monitor computer use. Have the computer in the family room, if possible. There is software so that you can see every keystroke they make from another room. Do surprise spot checks if necessary.
- Use difficult-to-guess, alpha-numeric passwords and change them frequently. They should be 8 characters in length. Mix numbers and letters randomly, and avoid using birth dates. Do not write the password down in accessible locations and do not give it to anyone. Use different passwords for different accounts. Do keep track of your children's passwords.