Good Practices In Technology: The K-12 Classroom

Elizabethtown Independent School District

BUILDING ON A TRADITION OF EXCELLENCE

Ver 0909.2

Acceptable Use Policy

- All users must read the Acceptable Use Procedures (AUP) and sign an Individual Use Agreement (IUA).
- EIS electronic resources (Computers, Network, E-mail and Internet, etc.) are available to users for educational purposes.
- Users are solely responsible for their actions on the Internet.
- Use network with same good judgment expected when in the school building.
- Schools will provide reasonable supervision but are not responsible for individual user's actions.

Network, Internet and Email Guidelines

Users are responsible for good behavior on the network

- Electronic assets are not for:
  - Personal business (e.g., Tupperware, Avon, Mary Kay)
  - Political activities
- Use your own login account – do not give it to others
- Do not open others' files, mail, etc.
  - Only Principals can authorize access to student accounts
  - Only Superintendent can authorize access to staff accounts
- Do not use destructive behavior such as sending viruses, deleting files, harassing, etc.
- Do not access network for hate mail, pornography, racist or other objectionable material.
- Obey copyright laws

Cyberbullying – Part 1

- 90% of youth age 12-17 communicate via email; 75% use IM
- Cyberbullying - “willful and repeated harm inflicted through use of computers, cell phones and other electronic devices”; involves a minor
- Children have killed/committed suicide after cyberbullying
- Two types
  - Direct Attacks
  - Via proxy
- Some Examples of Direct Attacks
  - Send threatening messages; create screennames similar to others
  - Steal passwords and send messages, lock out user, hack into comp.
  - Post blogs/videos and create malicious web sites about kids
  - Send degrading pictures of kids
  - Internet polling – “who’s hot/who’s not”
  - Send malicious code, porn, junk e-mail

Cyberbullying – Part 2

- Prevention
  - Educate kids about consequences
  - Use internet and mobile phones carefully
    - Don’t give out personal information
- Victims should:
  - Talk to someone they trust
  - Report the incident (to police if necessary)
  - Block messages/emails
  - Keep offensive messages as evidence

E-mail
Good Practices

- Use email to support the instructional program.
- Open email from those you know- not from strangers.
- Close email when not in use.
- Do not send or forward email that is:
  - "Chain letter" or "spamish" in nature
  - Infected with a virus
  - Offensive in any manner
- Make it a habit to not "bad mouth" anyone/anything

E-mail
Good Etiquette

- Do not use all CAPS…considered shouting.
- Keep messages concise and to the point
  - Several short paragraphs better than longer narrative
- Avoid public "flames" - messages sent in anger.
- Always use a signature.
- Mail systems are not private. Don’t send embarrassing messages.
- Emoticons (☺) can help convey a message.
- Proof e-mail before sending; consider a 5 minute “time-out” before sending emotional responses
- Use “High Priority” sparingly (or risk overuse)

Miscellaneous Musings

- Protect your password
  - Keep PW to yourself, use letters, numbers & special characters
  - Example, password of “sports” could be “5p0rt5” where 5 looks like an s, and a zero replaces the letter o
- Only download educational programs and files from “established” locations
- Obey copyrights (documents, music, etc.)
- Sites/programs to not use from district resources
  - Non KETS email (e.g., Hotmail, AOL mail)
  - Instant Messaging (e.g. AIM0
  - Social Networking sites
    - Facebook, Myspace, Twitter, etc.
    - Note; When using from home, be aware of the risks these sites contain
  - File Sharing sites like Kazaa
- Check with STC before using unauthorized antivirus/registry cleaners on district computers

Scams, Schemes & Such

At home & work – watch for scams

- Advance Fee Scams
  - Nigerian Letter (cheated Americans of $122 mil) & Canadian Lottery Winner: You pay money to get money.
- Internet Schemes
  - Auction web sites that don't deliver, phony emails, verify your account number, etc.
- Cramming
  - Mysterious charges on your phone bill (fine print of agreements)
- Bogus business opportunities
  - Work at home scams, leasing ATMs
- Viaticals
  - Buying life insurance of terminally ill patients

Chain Mail

- Email “chain mail” sounds reasonable – but is designed to overload mail networks
- Topics:
  - Make Money Fast
  - Email Tracking Giveaway
  - Good Luck
  - Follow Directions Carefully
  - Chains of Mourning
  - Charity Chains
  - Urban Myths (Spiders under toilet seats, gang initiations, etc.)
- Forwarding chain mail is a violation of the district’s AUP
- If email says “Forward this to all…” – it is probably chain mail

Chain Mail – Example 1
(Note – spelling errors were built in by author)

Subject: PLEEEEEEASE READ!!!! it was on the news!

To all of my friends, I do not usually forward messages, But this is from my good friend Pearlas Sandborn and she really is an attorney.

For every person that you forward this e-mail to, Microsoft will pay you $245.00 For every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, You will be paid $241.00. Within two weeks, Microsoft will contact you for your address and then send you a check.

I thought this was a scam myself, But two weeks after receiving this e-mail and forwarding it on. Microsoft contacted me for my address and within days, I receive a check for $24,800.00. You need to respond before the beta testing is over.

If anyone can affoard this, Bill gates is the man.
It's all marketing expense to him. Please forward this to as many people as possible.

Chain Mail – Example 2

Chain Prayers

"We all need friends to pray for us!!! When you receive this, say the prayer. That's all you have to do. There is nothing attached. This is powerful. Just send this to four people and do not break this, please. Prayer is one of the best free gifts we receive. (general prayer follows). . . Passing this on to anyone you consider a friend will bless you both. Passing this on to one not considered a friend is something Christ would do."

Some thoughts for home computers

- Must have Antivirus software (Norton's, MacAfee's, etc.)
  - With current AV definitions (weekly updates)
- Must apply Microsoft Windows updates regularly
- Must have a firewall if using DSL, Cable
- Good to have:
  - Spybot
  - Adaware
  - Antispam software

Note – there are free versions of all of these on the Internet. There are many good, safe sources for the free versions – one is:

www.pcworld.com/downloads/

Some Freeware to Consider

- Open Office – almost as good as Microsoft Office
- Firefox – outdoes Internet Explorer browser
- AVG – Antivirus software
- Misc
  - Adaware
  - Spybot
  - Zone Alarm