Washington Township Public School District
206 East Holly Avenue, Sewell, NJ 08080
Telephone 856-589-6644

Joseph A. Vandenberg
Interim Superintendent of Schools

Stephen Altamuro
President, Board of Education

SPAM

The amount of spam on the Internet is increasing EXPONENTIALLY. To fully understand the level of spam, see our spam statistics below.

Email Statistics			
	Inbound		
	Total	Day	Hour
Blocked	103,643,533	36,115	2,443
Blocked: Virus	80,208	11	1
Rate Controlled	2,849,967	2,709	1,586
Quarantined	246,352	183	46
Allowed: Tagged	542,843	185	29
Allowed	6,815,360	12,650	4,276
Total Received	114,178,263	51,853	8,381

Less than 3% of the emails trying to come into the district are legitimate -- the rest are spam.

Spam can be generated by viruses, Trojan horses, or worms that infect a user's computer, invade the address book, and send emails to everyone. That email you received from your aunt in Podunk, Michigan may not have been sent by her. We encourage district staff to keep their home computers up to date with the latest virus signature files.

Unfortunately, some spam will still get through. There is no way to successfully block 100% of all spam. To add to the problem, much of the new spam is now in a graphic format which does not contain text that would trigger the spam protection. The text is embedded in the graphic.

How do I get spam?

- **If you have your email address on any website, you WILL get spammed.** No question about it, no hiding from this fact. It's only a matter of time before a spammer's Harvester finds your address.
- A company you've done business with sells it. Check privacy policies before doing business with any company. Be sure the company never sells or otherwise distributes customer information, including email addresses.

- You or someone you know:
  - gives your email address to an untrustworthy party, such as an online contest or e-card website and that party uses or sells your address.
  - puts your address on a website, like a personal homepage.
  - signs up for a mailing list who shares your information.
  - responds to a spam email asking to be removed from the list - in turn, confirming your email address as a live address.
- Spammers use their computer for "dictionary attacks" to automatically generate addresses by the tens of thousands. For example: johna@xxx.com, johnb@xxx.com, johnc@xxx.com, johnd@xxx.com.
- A virus, Trojan horse, or worm infected someone's computer and your address is in their address book, generating an email from one person in the address book to another. What arrives will look like a legitimate email, but was not actually sent by that person.

You can prevent spam:

- **NEVER respond to unsolicited mail.** Create a "throwaway" email account with Yahoo, Excite, Hotmail, or other service to use when dealing with e-commerce. If you get spam at that address, abandon it and create a new one.
- **Keep your anti-virus software up to date and install a firewall.** Unprotected high-speed Internet connections are vulnerable to infection by viruses that are programmed to open gateways (proxies) to relay spam. If your PC is not secure, you may unwittingly be a courier for spam.
- **Give your primary e-mail address to friends and family only**. Give a secondary e-mail address to commercial entities. It is disposable.
- **Use your secondary e-mail address** in newsgroups, bulletin boards or chat rooms, or "munge" the primary address so that it is not deliverable in the original format. For example, if your e-mail address is joe@somewhere.com you could post it as joe@NOSPAM.somewhere.com. The recipient can understand it but a spammer program cannot.
- **Never post your primary e-mail address on a Web site.** Spiders scan Web sites for e-mail addresses.
- **Do not reply to unsolicited e-mails.** If the email does not appear to be from a trustworthy source, delete it without replying.
- **Use the secondary e-mail address** when signing up for services, filling out forms or taking surveys. Read the privacy policy of these sites.
- **If the spam you receive always comes from the same sender** or has the same subject line, you can set up a rule in Microsoft Exchange to block a sender, a domain, or specific text in the title or body of the email.

Why can't all spam be filtered?

- It is impossible to avoid all spam. Filters can be set so tight that they actually block legitimate email. So where do we draw the line? If we make the filters too tight, legitimate email is blocked; if it is not tight enough, spam gets through.
- Spammers are changing or misspelling common triggers, or using other tactics such as embedding text into a graphic.
- Spammers actually purchase anti-spam software and use it to circumvent the filters.

What else can I do to block spam?

Our email server has the ability to allow you to create RULES to block emails that have common characteristics. Examples could include specific text in the subject line or body of the email, emails coming from the same sender, etc.

Where can I learn more about limiting spam?

Visit: http://help.yahoo.com/sbc/tutorials/mail/otherspam1.html

RULE 1: NEVER REPLY TO A SPAM EMAIL!

Even if you follow the instructions to remove yourself from the spammer's email list, you've just validated your email address and they can sell it to their spammer friends.

RULE 2: NEVER RUN ANY ATTACHMENT THAT ENDS IN ".EXE", ".SCR", OR ".VBS". DELETE IT IMMEDIATELY.

More a virus protection than spam protection, it's an easy way to prevent serious problems. Viruses are contained in attachments named "picture.gif.exe" or similar. Users see the "picture.gif" and assume it's a picture. The ".exe" is an executable file that, when downloaded, runs a program on your computer. You will have no idea what it is doing, and it can do ANYTHING: forward your address book to a spammer; load a monitoring script onto your network; forward itself to everyone you know, or send spam from your email address.

We filter for these extensions with our network software, but on your home computer these files will enter your system and do their dirty work.

RULE 3: NEVER BUY ANYTHING ADVERTISED IN SPAM EMAILS

Entities send unsolicited commercial e-mail because people buy the products or services being promoted. If no one buys the products advertised with SPAM, the incentive is reduced. And, if you purchase something from a spammer, you are "marked" as someone who is likely to respond to spam. Use a secondary email address when dealing with commercial entities.

RULE 4 (and most important):
NEVER RESPOND TO AN EMAIL THAT REQUESTS YOUR LOGIN ID, PASSWORD OR OTHER PERSONAL INFORMATION! – NEVER!