

SECURITY CHECKLIST

If you take anything from this brochure, pay attention to this checklist.

Make sure the accounts on your computer all have passwords.

- **Post** – CPS Lab/Classroom Computers/Equipment/Internet Use Policy by computer (s) in room.
- **When** making a purchase or entering personal information into a Web page, make sure it is a secure site. The URL should begin with “https.”
- **Do not** click on pop-up windows, particularly ones promising to rid your computer of spyware.
- **Download** files and software only from sites which are familiar.
- **Never** open an attachment you aren't expecting.
- **If** you receive unwanted e-mail, delete it and/or set up a filter to delete ones like it in the future. Never click on any links or respond to them. See Teacher Place for setting up GroupWise rules.
- **Never** respond to an e-mail requesting personal information, unless you have initiated a request for help with a trusted company.
- **Do not** allow students on a teacher station
- **Make** sure student screens are visible by teacher
- **Never** leave students alone while working on a computer
- **If** having computer issues; please contact lab manager
- **Review** Access and Use Policy
- **When** leaving station – use the window key at the bottom of the keyboard + L and it will lock the workstation down. To re-engage, retype password.
- **Skyward** will automatically log out of 20 minutes of inactivity – Never allow students to use/enter grades into Skyward or give them password information
- **Back up** important data to your server space.

PASSWORD SECURITY

Passwords provide access to your accounts. Protect your accounts by creating strong, unique passwords. Avoid using easy-to-guess words or phrases. You are encouraged to change them at least every 1-3 years. Never share your passwords with anyone.

Tip: A strong password combines uppercase and lowercase, numbers, and punctuation marks.

Password Security:

- Never log a student on with teacher login or password
 - Students have generic logins that can be used on student stations in classrooms for Word Processing, Spreadsheets, etc.
 - If a student needs Internet Access in teacher's classroom, use Interlock (looks like Mozilla on the desktop). A password is required and should not be given to the student; teacher should access password from lab manager or media specialist and type into the computer
- Do not give out any passwords to anyone including tech staff (lab managers)
- Do not write down passwords and leave by computer or anywhere that is easily accessible by another.
- Fill out Charlottenet.org application from Teacher Place to request password change

Passwords Must Have:

- At least 8 characters
- A combination of upper and lower case letters
- At least 1 number (0-9)

Passwords Cannot:

- Contain all of characters of your username in any order
- Be a password previously used for this account

Strong Password Examples:

P@55w0rd	(password)
07fr3Sh_m@n	(07fresh_man)
G0*gr3En	(go*green)
B@!tUn!v	(baltuniv)

TECHNOLOGY SECURITY AWARENESS

CHARLOTTE PUBLIC SCHOOLS
TECHNOLOGY DEPARTMENT

Resource Information provided
[Lock it down](#), Technology Security Awareness, Baltimore,
Maryland: Office of Technology Services & Charlotte Public
Schools Technology Department

We've all heard the horror stories of pop-up ads that won't go away, stolen credit card numbers, virus attacks affecting millions of internet users. The Technology Department has written this brochure to provide you with simple – and inexpensive – ways to protect your information resources in today's high-risk computing environment.

Remember the Internet is an unregulated space. You are responsible for protecting your privacy and computer's security. Never give out password information or allow someone to use your computer when you are logged in. Exercise caution when visiting unfamiliar sites. While the adage is old, it is appropriate to our time: Better safe than sorry! Lock it down!

DESKTOP SECURITY

Antivirus Software – Protect against viruses and worms, which can cause harm to your computer or its data. Up-to-date AV software will repair damage isolate, or delete the threat.

Tip: Charlotte Public Schools uses F-Prot for Virus Protection

Firewall - Protect your computer from the risk of intrusion by hackers and other computer threats. Firewalls monitor and filter Internet traffic and protect against unwanted activity.

Tip: Charlotte Public Schools uses Sonicwall

- Remember that Internet filtering is never 100% fail safe
- If you select an option in a web browser and you enter an area that is inappropriate – close out and immediately notify the Tech Department.

Software Patches and Updates - Improvements and critical fixes to software and operating systems are regularly released. Never click on a pop-up Web window to obtain updates.

Tip: Many software providers – such as Adobe, Apple, Microsoft, Symantec, etc. - provide free security update to protect against new threats. These updates are automatically done through our system.

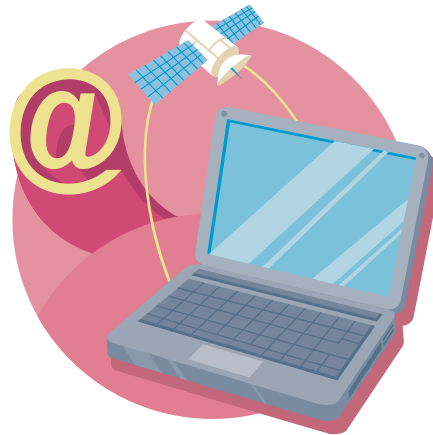
Computer should be powered down every night when leaving.

INTERNET SECURITY

Spyware and Adware – Spyware collects and transmits browsing behavior without your knowledge. Adware displays advertisements on your computer, in the form of a pop-up window. Both can dramatically impair your computer's performance. Protect against these nuisances with anti-spyware and adware software.

Wireless Networks – Although public wireless internet access is convenient, you cannot be sure of the network's security. Think twice about the type of surfing or business you transact while using a public, wireless internet connection. Always use encryption when sending personal information across them.

If a site is not blocked and should be because of questionable material please contact lab manager with the information



E-MAIL SECURITY

Spam – Unsolicited e-mail – or “junk mail” – sent to you without your consent can be overwhelming. You can avoid most spam by not posting your e-mail address on public Web sites. Also, don't respond to spam at all as this will cause more unwanted messages.

Tip: Many e-mail applications contain a junk mail filter that helps you identify and block spam. Charlotte Public Schools uses GWAVA as spam filter

Attachments – Hackers use e-mail attachments to transmit viruses and worms to your computer. Never open any attachments from unknown senders – or even unexpected attachments from friends.

Phishing – Ever receive an e-mail appearing to come from a legitimate bank asking you to confirm your personal information? This is a type of fraud designed to steal your identity. These messages deceive you into divulging sensitive information – such as your social security, bank or credit card numbers, passwords, etc. Never respond to an e-mail asking for any type of personal information or account passwords.

Tip: Report any messages you suspect are phishing scams to the Internet Fraud Complaint Center (www.ic3.gov)

