1:1

Parent & Student Handbook

Evan Bishop
Hopkinton High School Principal

Ashoke Ghosh
Director of Technology

Adopted from:
Natick Public Schools 1:1 Handbook

Special Thanks to:
Natick's Administrative and technology Teams

Section 1:
Student Responsibilities

Each student will be responsible for :

- Arriving at school with their fully-charged computer, carrying case, computer charger, thumb drive and personal headphones.
- Attending each class with their computer, carrying case and computer charger.
- Agreeing to and signing Hopkinton Public School's Acceptable Use Policy (AUP) and Acknowledgement of Receipt
- Protecting and backing up all electronic files or data created.

Charging of Computer Battery

Students must arrive at school each day with a fully charged computer battery. To fully charge the battery, the computer charger must be plugged into an electrical outlet and attached to the computer for at least two hours (if the computer is shut-down).

A charging station will be available in the technology center and power-strips will be made available in classrooms to charge computer batteries that are running low. However, the teacher may have the student move to an area of the classroom that has an outlet or look on with another student while the battery recharges. NOTE: Being prepared for class includes fully charging the laptop battery each night and failure to do so may lead to detentions as a consequence.

Backing Up Files & Data:

It is the responsibility of each student to backup his or her own data. In the event your laptop needs to be serviced and swapped out with a loaner it will be critical to have an up to date backup of all your important files.

Hopkinton Public Schools will provide basic instructions for configuring automatic backups using Time Machine which is a built-in application that backs up important files in the background. Time Machine along with an external drive, thumb drive, or cloud service are some of the easiest ways to backup and protect your important work.

Equipment Responsibilities

Students need to be responsible for the upkeep of equipment issued to them.

- Loaner laptops will be provided to the school based on student enrollment.
- Student laptops will be periodically checked for AC adapters and physical condition.
- If a student is leaving the district, then the laptop and associated accessories must be returned on the last day of attendance.

Laptop Accidental Damage/Loss Policy

Repairs and Damages:

Level 1 –*Software issues, login issues, general help desk questions*.
Stop by the Technology Center to get help with your problem or submit a request with the ticket system online at https://helpdesk.school.hopkinton.k12.ma.us/portal and a technician will email you to set up a time to meet.

Level 2 – *Defective hardware*
Most repairs will be covered under the AppleCare agreement if the problem results from defective or faulty hardware. Technicians will identify what parts need to replaced if any and will fix the equipment in- house. You will be provided a loaner laptop for the duration of your repair.

Level 3 – *More expensive claim - i.e. spill damage, cracked screen, dropped laptop*
Students will be responsible for paying for the parts and labor associated with the repair of a laptop due to accidental spills, drops, or other related damage.

Level 4 – *Lost or stolen device*
Students and parents will have to file a police report and a full investigation will be conducted to help retrieve the missing laptop. Once it is determined that the device is stolen and not missing, the school will replace the laptop. Students that violate the rules as stated in the 1:1 handbook or fail to store their laptops correctly will be responsible for buying a new device.

Discipline:

CLASS BEHAVIOR: Students are expected to refrain from inappropriate behavior in class. Yelling, using crude language, being disrespectful to others, and generally disrupting a class, will not be tolerated. The classroom teacher will assign students who engage in inappropriate classroom behavior a detention. If a student fails to report to an assigned teacher detention, for which twenty-four hours notice was given, the teacher will notify the parent, and the student must serve the detention with the teacher the next day. Students who fail to report to this teacher detention will be referred to the office for the assignment of two (2) office detentions. **Excessive disruption of class will result in an office detention, Saturday School, and/or suspension.**

Consequences for Inappropriate Classroom Behavior

First Offense:
Students will be given a warning and teachers may notify parents of the incident. If it is a serious offense that violates the Acceptable Use Policy or the Student Handbook students will be referred to their Assistant Principal.

Second Offense:
Students will be assigned a teacher detention, teachers will notify parents of the incident. Assistant principals will be notified and incident will be recorded in iPass. Depending on the magnitude of the incident the student may lose laptop and network privileges.

Third Offense:
Students will be referred to their assistant principal and a Saturday school will be assigned and parents will be notified. Depending on the magnitude of the incident student may lose laptop and network privileges,

USE OF COMPUTER TECHNOLOGY: Acceptable Internet Use: Students are responsible for proper behavior on school computer networks just as they are in a classroom or a school hallway. Communications on computer networks are often public in nature. General school rules for behavior and communications apply. Network access is provided for students and staff to conduct research and to communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner. It is the policy of the Hopkinton Public School System to maintain an environment that promotes ethical and responsible conduct in all network activities by staff and students. It shall therefore be a violation of this policy for any employee or student to engage in any computer activity that does not conform to the established purpose and general rules and policies of the Hopkinton Public School System. These rules include but are not limited to:

- No student will be allowed independent access/use of the Internet, or e-mail system if a parent/guardian has refused permission. Independent access/use means use not under the supervision of a professional staff member who is actively engaged in the supervision of the student's Internet activity.
- All use of a school's local area network (LAN), Internet connection, or e-mail system must be in support of education and research and consistent with the purposes of Hopkinton Public Schools.
- Students shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.
- Users shall not download or remove any files without the expressed permission of a professional staff member.
- Hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited on the LAN or on the Internet.
- Malicious use of the LAN/Internet to develop or use programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
- Use of the LAN/Internet to access or process pornographic material or files dangerous to the integrity of the local area network is prohibited.
- LAN/Internet accounts are to be used only by the authorized owner of the account for the authorized purpose. Accounts are password protected for security reasons. Under no circumstances should usernames and passwords be shared with others.
- All information accessed via the Internet should be assumed to be the private property of the information

provider unless otherwise stated and is not to be used without permission.

- There may be no unauthorized removal or movement of any computer equipment.
- Users should make no changes to a computer system that would inhibit the use of that system.
- Giving out personal information about self or another person, including home address or phone number is strictly prohibited.
- Students must notify parent(s)/guardian(s), a teacher, or a school administrator immediately if any individual is trying to contact them for illicit or suspicious activities.
- From time to time, the Hopkinton Public Schools' Director of Technology will make determinations on whether specific uses of the network are consistent with the acceptable use practice.

Violation of any of these rules could result in loss of computer privileges, detention, suspension, or any punishment deemed appropriate by the school administration.

Internet use is governed by Hopkinton School Committee policy, school rules and codes of conduct and applicable law and regulation. See School Committee policy IJNDB (www.hopkinton.k12.ma.us/schoolcommittee/policies.html) for further information or obtain a copy of this policy and additional information regarding use of computers in school from the principal.

Parents and students are strongly urged to review the complete School Committee policy on Acceptable Internet Use.

CHEATING/PLAGIARISM: Cheating is intolerable in an academic institution and it will be dealt with seriously. Cheating involves the intentional attempt to pass off the work of others as one's own. If a student is unprepared or under-prepared for an assessment s/he should bring that to the attention of the classroom teacher. Cheating is not an acceptable alternative. Aiding or abetting an individual in cheating is also considered cheating. Cheating includes (but is not limited to):

- Getting or giving your assignments to another person
- Using assignments submitted by others in previous semesters or other courses
- Soliciting to have someone do your assignments in part or in whole for you
- Having someone do your assignments in part or in whole for you
- Doing someone else's assignments for them
- Submitting work that is not completely created by you
- Looking at someone else's test during an exam or asking someone for help during the exam
- Using technology to get answers during an exam

Any person giving information and any person using information are both cheating.

Consequences for Cheating and Plagiarism:

Consequences are cumulative from year to year

First Offense:

- The teacher who observes the cheating will notify the parents and the assistant principal who will keep a record of the event.
- The student will likely receive no credit for the work in question.

Second Offense (In addition to the above):

- The student will be assigned to Saturday School.

- The student will be ineligible for any awards during that year.
- A conference with the student, teachers, parents/guardians, and assistant principal will be held.

Third Offense (In addition to the above):

- The student will receive a suspension. The amount of suspension days will be at the discretion of the administration.
- The principal will meet with the student and parents/guardians to explain the consequences of additional offenses.

Consequences for Not Charging Laptop Batteries

First Incident:

- Teacher may have the student move to an area of the classroom that has an outlet or look on with another student while the battery recharges. The student will receive a verbal warning and the parent/guardian may be notified.

Second Incident & Subsequent Incidents:

- Teacher may have the student move to an area of the classroom that has an outlet or look on with another student while the battery recharges. The student will receive a teacher consequence and the parent/guardian will be notified. Consequences for repeated incidents will follow the behavior rubric guidelines.

Behavior Rubric	1st offense	2nd offense	3rd offense	4th offense
Unprepared for learning including but not limited to: laptop not in class; battery uncharged missing accessories	Warning May Call/notify home	Teacher consequence Will Call/notify home	Office or classroom detention(s) Call/notify home	**Either/and/or:** Multiple before/after school detention(s) Suspension Restriction of technology privileges Loss of school privileges Parent Conference
Refusal to follow directions including but not limited to: On computer without permission; off-task computer work; online/on sites without permission	Warning May Call/notify home	Teacher consequence Will Call/notify home Possible restriction of technology privileges	**Either/and/or:** Office detention(s) Restriction of technology privileges Call/notify home	**Either/and/or:** Multiple before/after school detention(s) Suspension Restriction of technology privileges Loss of school privileges Parent Conference
Reckless/damaging care of laptop/accessories including but not limited to: Carrying laptop outside of case; laptop in unauthorized places(locker, backpack, cafeteria, etc); eating/drinking near laptop; decorating/defacing laptop; vandalizing laptop	**Either/and/or:** Warning Teacher consequence Item replaced or damage restitution made Call/notify home Possible police notification	**Either/and/or:** Teacher consequence Office consequence Item replaced or damage restitution made Call/notify home Possible police notification	**Either/and/or:** Office Consequence Item replaced or damage restitution made Restriction/removal of technology privileges Call/notify home Possible police notification	**Either/and/or:** Multiple before/after school detention(s) Item replaced or damage restitution made Suspension Restriction of technology privileges Loss of school privileges Parent Conference
Violation of acceptable use policy including but not limited to: recording sound, picture. video on school grounds without permission/facilitation by faculty; violation of copyright laws; use of and/or viewing obscene, profane, lewd, inflammatory, threatening, disrespectful language or images; causing damage or disruption; engaging in personal attacks, use of false or defamatory information; use of unauthorized software; sharing/accessing passwords, access codes, etc; use of someone else's name, account, etc.	**Either/and/or:** School detention(s) Office calls home Restriction/removal of technology privileges Possible police notification	**Either/and/or:** Multiple before/after school detention(s) Suspension Office calls home/possible conference Restriction/removal of technology privileges Possible police notification	**Either/and/or:** Suspension(s) Parent conference Restriction/removal of technology privileges Loss of school privileges Possible police notification	**Either/and/or:** Out of school suspension(s) Parent conference Restriction/removal of technology privileges Loss of school privileges Possible police notification

Section 2:

Care and Maintenance

- Use only approved wipes for the screen - cleaners that are designed for LCD screens (regular glass cleaners that contain alcohol or ammonia and will cause damage).
- While the computer is turned off, you may clean the keyboard, trackpad and surfaces with a lightly damp cloth. Never spray cleansers directly on your computer.
- The trackpad can be damaged if not used properly. Never use a pencil, eraser or other object on the trackpad.
- Don't place heavy objects on top of the laptop. This may cause damage to the screen. The laptop should never be in a pile!
- Do not place stickers on the inside/outside of the laptop.
- Be careful with the screen. Don't touch the screen with your fingers or any other object.
- Don't place anything between the screen and the keyboard when you close the computer.
- Do not use CDs/DVDs that have labels on them.
- Use your laptop on a sturdy surface that allows for adequate air circulation. Placing the laptop on a pillow during use or blocking the side air vents can cause it to overheat.
- To maximize the overall life of the battery, once or twice a month, run the battery down completely before charging your laptop.
- Do not bend the AC adapter wire. Leave plenty of room for the wire to reach the computer.

When moving about with your laptop (From room to room and/or leaving school):

- Save all open documents
- Put laptop to sleep (close the lid)
- Place laptop in its laptop case

Wellness:

Before you head to wellness please lock your laptop in your locker. If you need to charge your device at this time, stop by the tech center and they can place it in the charging cart.

Cafeteria:

Student laptops are not allowed in the cafeteria during lunch periods. This is a high traffic zone and food and liquid spills can cause severe damage to your laptops. If you had to replace your logic board the estimated cost is $700.00 and a cracked screen is roughly $300.00. If you would like to use your laptop during lunch please sit in the atrium or the space in from of the Athletic Center. However, you can and should bring your laptops to study hall.

End of Day:

Students should take their laptops home at the end of the day. If you need to attend an extracurricular activity

(practice, games, clubs, etc.) please lock your laptop in your locker. Do not leave your backpacks in the locker rooms or hall ways unattended and not locked. Locker rooms are high risk areas and are not regularly monitored after school.

Save and Backup Your Data:

Data will be backed up if and only if you save your documents to your portable USB Drive, CD/DVD, or external drive. Be sure to save every time that you do a significant amount of work that you would regret losing. Data should be backed up to the external drive at a minimum of once per week.

All students are responsible for backing up their own data!

At least once a week:

- Empty the trash
- Restart (recommended but not a requirement)
- Shut Down your computer if you are not going to use your laptop for 1 or more days.
- Back up your laptop to the external hard drive.

Keep organized:

- Do not keep documents on your desktop- reserve the desktop for documents that you want to temporarily take off the network shares, work on at home and then put back on the network when finished.
- Keep your folders organized; documents in the Documents folder, movies in the Movies folder, pictures in the Pictures folder, and music in the Music folder.

Quit applications that you are not using:

Applications like iTunes and Firefox query the network every few minutes and put a strain on the network that slows down traffic for all of us. If you are not using an application you should quit the application.

To maximize battery life:

- Turn down volume
- Turn down brightness
- Quit any applications that you are not using
- Your laptop needs power to keep up with you. Make sure to charge your computer fully before the beginning of the day.
- Use your laptop case to transport your laptop between home and school.
- Dim your screen to conserve power and make your battery charge last longer.
- Only keep open applications and websites you are using. This saves processor power, memory and extends your battery life.
- Save early, save often. Don't wait until the end of class to save documents for the first time. Make sure to save regularly while you are working.
- At the end of class make sure to save all your work, put your Macbook to sleep, and place it in your carry case only after it is asleep (cover closed). Plan to leave at least 2-3 minutes of time at the end of class to get this done before the next class.
- Work on a flat and level surface and not on top of other items on your desk. Don't risk having your laptop end up on the floor!

- When you're not using your laptop in class, place it in your carry case. Don't leave it out on the desk where it may get knocked off.
- Use time at lunch to charge your laptop.
- Don't try and walk the halls with an open laptop because sooner or later you will regret it!
- Use your case when transporting your Macbook between classes.
- Don't put pens, scissors or paper clips in the same compartment as your laptop; they may damage the screen or one of the ports.

After School and at Home

- You can use the classroom charging stations after school.
- Use a surge protector instead of plugging directly into the wall to protect from lightning strikes and power surges.
- If you plug into a cable modem at home, disconnect the network cable during thunderstorms or when you are not using your Internet connection.
- When connecting to power, plug in to the wall first, then your Macbook.
- When disconnecting from power, unplug from your MacBook first, then from the wall.
- Make sure to shut down your laptop if you don't plan on using it for more than a day.
- Don't work on a soft surface like a bed or a pillow or use in a way that will block the vents.
- Be wary of "borrowing" wireless access from others in your neighborhood. You can never be sure if others are stealing your information.
- Use your laptop away from food and liquids. Spills can be deadly to your Macbook.
- Leave your laptop in a secure place during after school sports and activities.
- Don't leave your laptop in a car overnight or for long periods. Extreme heat or cold can damage your MacBook.
- Keep your laptop locked in a safe location when you are away for the holidays.
- Keep your laptop safe from pets and younger siblings.
- Don't keep magnetic items like paper clips or staples near the power port on your laptop. The magnetic charge on the port will attract them and may cause damage.

Computer Troubles ?

- Force quit an application by going to the Apple menu and selecting Force Quit or by using the key-combination Command-Option-Esc
- If your computer is slow or certain applications aren't working right, try saving your work and restarting.
- If your computer won't turn on or won't come out of sleep, check your battery to make sure there's enough power left.

Section 3:
Technology Tips

The MacBook laptops are equipped with a wireless card. Wireless connectivity is available at school. For home use, students should only to connect to a password protected wireless network. The cards can also access unprotected networks; however it is not suggested to do so because it will leave the computer and data vulnerable.

If a wireless network is not available at home, an Ethernet cable can be plugged into the computer and the cable modem. The computer will pick up the DHCP address and internet access should be available.

Printing at Home

- To be able to print at home, printers must be MAC OSX compatible.
- Printer must have a USB connection.
- MacBooks have many print drivers pre-installed and can often self detect the appropriate drivers. Additional drivers may need to be located and installed from the printer manufacturer's website.

The following steps will help students connect their MacBook to a home printer:

1. Turn your printer on and connect your MacBook to the printer. Open the Printer Setup Utility (located in the Dock as a printer icon)
2. Click ADD/Printer Icon on the Printer List window.
3. Select the type of printer from the 1st drop-down menu list.
4. Your printer should be listed in the Printer Setup Utility window.
5. Click on the printer name to select it and click ADD.

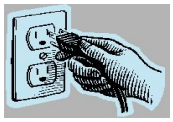
Technical Support and Repairs

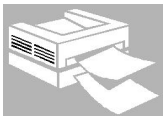
Technical support is available during school hours from the HPS Technology Department. In the event that a laptop needs repair, report it to the school computer technician. Every effort will be made to repair or replace the laptop in a timely fashion. Depending on the severity and nature of the issue, a loaner laptop may be provided until your laptop is repaired and returned to you.

If a technical issue occurs at home or outside of the school day all laptops are covered under the AppleCare Program. This coverage provides phone support for many hardware and software related questions. AppleCare Support can be reached at **800-APL-CARE (800-275-2273)**. AppleCare service is also provided by visiting the nearest Apple store which can be found at http://www.apple.com/buy/locator/service/

Basic Troubleshooting Steps





Be sure that the printer is powered on and paper is loaded
Be sure that the power is on
Ask the school technician for help
Force Quit the application using Option + Apple + Esc keys
Wait 3 minutes
Attach the AC adapter to your computer and plug it into an electrical outlet
Make sure that the sound is not muted - Press F5 several times
Check volume on external speakers
Check to make sure that the brightness on the screen is turned up – Press F2 several times
Make sure that the correct printer is selected for the print job
Check that the speakers are plugged into the proper jack
Restart the computer using the Apple + Shift + Esc Keys
Ask the school technician for help
Press and hold power button to turn off the computer, wait 15 seconds and turn the computer on again
Ask the school technician for help

Additional Resources

The following websites offer additional information regarding your MacBook:

Mac 101

MacBook Users Guide

Learning about iLife

The following are video tutorials to help you with the iLife Suite:

iPhoto Video Tutorial

GarageBand Video Tutorial

iDVD Video Tutorial

Section 4: Files

- Laptops come with a standardized, pre-loaded image. This image may not be changed in any way.
- Software may not be copied, altered or removed from the laptops.
- It is your responsibility to backup your data just in case a laptop may need to be re-imaged.

Installing and Deleting Files

Do not delete any application files that you did not create. The deletion of these files could cause issues with the computer functioning properly.

STUDENTS ARE NOT PERMITTED TO DOWNLOAD OR INSTALL PROGRAMS TO THEIR LAPTOPS.

Illegal File Sharing

File sharing programs used to illegally download music, videos, games, etc. will not be allowed to be installed or used on the laptop. It is a violation of Hopkinton Public School's Acceptable Use Policy and may be a violation of federal copyright laws.

Password

Students will login under their assigned username and password and will not share their passwords with other students.

Student Files

When creating documents for your classes stay organized, create folders on your desktop or within your documents folder for each of your subjects. Create a folder for L&L, Math, Social Studies, Science and Foreign Language. As you create documents, save them to the appropriate subject folder to make it easier to find your documents and stay organized.

To create a new folder:
Click the Finder icon in the Dock.
From the **File** menu, choose **New Folder**; a new "untitled folder" icon appears on the desktop.
Name your folder by simply typing a name in the highlighted text box below the folder icon.
You can now drag any files, other folders, into your new folder to establish a hierarchy.

Mac 101 Applications, Files and Folders

Section 5:

Email and Internet Use

Email

Students will be using Gmail as their email accounts for school. When email is sent, the name and user identification is included in the email message. Students are responsible for all email they send. In association with any investigation, email, stored data, transmitted data or any use of online services are not confidential and will be made available to district, local, state, and federal officials.

Internet Use

Hopkinton Public Schools maintains filtering and firewalls as required by the Children's Internet Protection Act (CIPA). The firewall and filtering restrict access to unacceptable sites, chat rooms, and online games. However, no filter is a reliable as adult supervision. It is the responsibility of the student to appropriately use the laptop, network and the Internet.

Students should notify a teacher if they access information or messages that are inappropriate, dangerous, threatening or make them feel uncomfortable.

Internet Use At Home

While the same filtering is used at home and at school, it is the responsibility of the parent/guardian to monitor student laptop use, especially Internet access while at home. Laptops should be used in locations that can be easily monitored and supervised by the parent/guardian.

Hopkinton Public Schools will provide Internet filtering software for the laptops while connecting to the Internet from home which will meet the CIPA guidelines. It is the responsibility of the parent/guardian to contract with an Internet Provider in accessing Internet from home and is their financial responsibility.

Remember Some Basic Internet Safety Rules:

- Never give out personal information such as addresses, phone numbers, passwords, and social security numbers to anyone.
- Never arrange to meet an Internet contact in person
- Obey all copyright laws.
- Never use or transmit anything with abusive, threatening, demeaning, slanderous, racist or sexually explicit.
- Always notify a teacher, parent/guardian if you accidentally access an inappropriate site and close the window immediately.

Internet Safety Links

Safe Teens

Wired Safety

ISafe

NetSmartz Workshop

Section 6:
Ergonomic Tips

"Ergonomics" can be a black hole of suggestions, with ideal positions and posture to do just about anything. There is a daunting list of rights and wrongs, but there are basic rules to follow to feel comfortable, and to allow your body to tolerate using a computer comfortably, longer.

The Rules to Comfort!

- Ideally **work on a tabletop surface**, such as a desk, counter, or kitchen table. (If you must work from your lap, tilt the screen and support your elbows or forearms as cued below).
- Your seat needs to **keep your lower back arched**, and to allow your forearms to be parallel with the table top height. This key position should enable you to properly relax all other body parts, allowing the chair to do the work, and you're your back or neck.
- Your **elbows should rest by your sides**, bent 90 degrees to enable you to you're your forearms on the tabletop.
- If possible, it's even more ideal to be able to rest your elbows and forearms on the table, as long as your **shoulders are not elevated**.
- **Tuck your chair in** close to the table surface or you'll likely slouch away from the chair's back, changing your entire spinal posture, neck and shoulder positions.
- **Support your feet**, to keep your hips/knees bent to relatively 90/90 as well.
- Keep your head aligned over your spine and shoulders, **rolling your chin down** so your eyes gaze straight ahead to the top edge of the display screen.
- For even better ergonomics, **use an external keyboard and mouse when possible**, especially if you're going to be there a while! Prop your screen to eye level, and use a supportive chair to get the right fit.
- Keep your other studying items close by, **reaching within your arm's length** to keep from having to slouch to get them.
- **Take regular breaks** of at least 20 seconds every 20-30 minutes. Stretch, bend, reach about.

Best Places to Avoid Laptop Use




- Lying on the couch, floor or bed
- Any chair without back support
- Perching on the edge of your seat
- Sitting in any soft or cushioned chair in which you can't readily reproduce your low back arch!

Some Fun Review Videos for Optimal Laptop Use:

- For kids
  http://www.youtube.com/watch?v=ZLwIP8cBaWA

- For Adults
  http://www.youtube.com/watch?v=S3z7uYMmaZ0&feature=related

Optimal Recommendations When Working at Your…

Desktop:

- Just putting the laptop on the counter, table or desk lowers the viewing screen below the recommended 'eye-level' height.
- Tilt your head on your neck like nodding, but keep your head's weight centered over your shoulders, rather than rolling your whole head down towards the screen if it's to be used in your lap
- Adjust the screen so that it is parallel with your face
- Your eyes should align straight ahead to the top edge of the viewing screen
- Try to sit with any window or other strong light source 90 degrees to your side in order to minimize glare
- Look to have lights overhead, and slightly behind your computer instead of behind you
- Try to have your seat height elevated so that your elbows can rest comfortably on the table surface.
- Shouldn't need to use a wrist support; laptops don't typically need wrist supports as one is built into the computer's chassis.

What about my chair?

- The most important part of any ergonomic setup!
- Most chairs are made for "one size fits all", but we're obviously not all the same!
- Any chair can be adjusted to suit the needs of the particular user, but it takes pillows and props
- You want to start with sitting tall, maintaining your lower back arch. That's the same amount of arch you have when your have when you're standing up, relaxed.
- "Ergonomic chairs" have an arch built into their backs, but you have to use it!

- If the depth of the seat is too deep you may need to fill the gap between the chair and your back with a pillow. Contour pillows are best
- Feet should be supported underneath to keep your hips/knees b/w 90-110 deg
- Elbows should be bent 90 degrees/at a right angle, shoulders relaxed, down and back.
- Forearms should slide directly onto the keyboard then in front of you; not be elevated, nor dropped

In your lap:

- Elevate the computer so that your elbows and shoulders remain relaxed, and bent 90/90 as above. Elbow supported in this position is more supportive
- Tilt the laptop screen back and roll your head downward to have your eyes gazing straight ahead to the top edge of the viewing screen
- Remember the chair needs to be properly supporting your spine, and hence everything else

At the kitchen table:

- Ideally, have the screen directly in front of you. Constantly being turned L or R to view and type can lead to other issues

Common Questions about Ergonomics

- **What about using a detachable keyboard/mouse?**
  Great idea for most people. Usually lets you find the most optimal alignment to sit with, or can even relax back in a recliner

- **Should I use a pull-out tray support for a keyboard/mouse?**
  Often a great solution for optimizing desktop space, but need to be aware that you seat height likely needs to be changed

- **How long should I be able to stay in any one place without tiring or hurting?**
  20 minutes is typical before one becomes fidgety due to ergonomic discomfort. Most recommendations suggest brief stretching and shifting in your seat every half hour, and taking a 5 minute break for every hour of work.

- **Do I need to get a new chair?**
  Often times no, but adapting what you have can do the trick
  Depends more on where do you most often use your laptop

- **What about sitting on a ball or kneeling chair?**
  No ball nor kneeling chair is ideal, but they do offer good alternatives to help you sit up with a more properly aligned lower back. Change of position is often better than always using the same one chair or setup.

Section 7:

Internet Safety Tips

The Internet is now an integral part of everyday life for most people. And within a short period of time, it has evolved from simply being a tool for accessing information and conducting communication and commerce to becoming a significant venue for social activity and interaction. For many young people who have never known a world without the Internet, it is also a vehicle for self-expression, a source of entertainment, and a creativity and distribution tool unimaginable by previous generations.

Know the Risks

The Internet should be a place where kids have fun communicating with friends and learning about the world around them. While using the Internet is an integral part of a young person's life and a necessary life skill, there are risks associated with it. Young people and parents should be aware of them to avoid or minimize their impact and help keep children's online time constructive.

In general, the positive impact and benefits of the Internet outweigh its risks. However, it is still essential to be aware of the risks and practice critical thinking and common sense to avoid them altogether. In considering the risks, it is important to take into account what may reach young people through the Internet as well as what they may share over the Internet with the outside world. Not all young people will encounter all of the potential hazards listed below, but by being aware of them, families can consider how to respond to them before ever going online.

What may reach them	What they share with the world
Inappropriate content • Pornographic • Violent, Self-destructive (eating disorders, substance abuse, etc.) • Inaccurate or Extreme	Personal/private information • That could be used by persons with bad intentions • That may damage a young person's (or a parent's or peer's) reputation, candidacy for school or job, etc
Unwanted contact • Grooming (sexual predator behavior) • Cyberbullying (peer harassment)	Disparaging comments and inappropriate content • Libelous, lewd, racist comments • Bullying peers, classmates, relatives • Sexting (explicit images taken and sent via cell phones)
Aggressive or undesired commercialism • Blur between content and advertising • Sweepstakes & requests for personal	Unintended and/or illegal file-sharing • Music, videos, games, other files using a peer-to-peer service that is not legal or is not

information (leading to spam, or annoying/malicious pop-up ads)	set correctly so that the computer can be accessed or hacked by outsiders
Computer Security Threats • Spyware, spam, viruses, identity theft	

What may Reach Them

- ***Inappropriate Content***

  A lot of discussion and concern has centered on young people's access to websites that promote pornography, violence or self-destructive behaviors. While parents and caregivers should be concerned about the content they see on the web, they also need to consider sites that are or look legitimate, but are fake, have been infected by malicious software, or are used by malicious hackers to steal passwords and other information. It is important to be aware of a website's security and privacy practices, especially if it requires a young person to provide personal information in order to use the site or features and software on it (such as widgets or 3rd-party code for use on social networking sites). Digital security and appropriateness of content are both important factors to think about when considering which sites are appropriate for young people.

  ### Safety Tip

  • Keep the computer in a common area where you can supervise as needed.
  • Use parental control features in most security software to block categories of sites, set time limits, and prevent personal information from being posted online.

- ***Unwanted Contact***

  As a social medium, the Internet enables young people to stay in touch with friends when they are separated from them or to meet new people who share their interests. If a young person is socially active on the Internet, they are very likely managing at least one personal profile on a social networking site which requires or allows them to publicly share something about themselves. While this ability is not inherently bad, there may be people familiar or unfamiliar to them who could take advantage of this. Behaviors such as online grooming (technique used by a sexual predator to convince an underage person to have relations with them offline) and cyberbullying (online harassment of peers) are some examples of unwanted online contact that parents and caregivers should understand and help young people recognize and act on if they ever experience it. In both cases, the first and best response to encourage is to alert their parents so they can figure out next steps together.

  ### Safety Tip

  • Ignore contact from strangers or from people that are attempting to bully.
  • Report repeated, hurtful, or troubling contact to the website and to a responsible adult who can help track the communications for remedial action.

- ***Aggressive or Undesired Commercialism***

  The Internet is a powerful marketing tool, and advertising messages targeting young people are plentiful. Parents and caregivers should be mindful of messages that entice them to acquire products or services in exchange for information or money. It is important to be aware of how this type of commercialism is delivered, what is being offered, and what young people may do as a result of it. Vendors are using more creative ways to promote their goods and embed their marketing messages which may make it difficult for a young person to differentiate between an advertisement and the content they are accessing (a technique called immersive advertising). Free offers and promotions for age-inappropriate products and services (dating services, gambling services, etc.) may also be compelling enough to a young person to enter

personal information that could later be used by the advertiser to deliver continuous, intrusive advertising (as spam or pop-up advertising) or worse, may end up in the wrong hands (to perpetrate hack attacks, identity theft, etc.).

Safety Tip

• Think critically about offers that are too good to be true. Turn on pop-up blockers in your web browser.
• Use up-to-date security software and if available, the ad-blocking feature which can prevent ads being displayed.

- ***Computer Security Threats***

The massive adoption of the Internet as a social medium has not made it immune to the risks of information security threats. Risks of spyware, spam, viruses, or hack attacks still exist as they always have. In the case of the social web, attackers mask their attempts by preying on behavior that is normal or intuitive to a young person using the Internet. This is called "social engineering" and attacks can be cloaked with as simple a message as, "Hey, check out this video" in a video sharing site. The attacker's' motive is simple: to make money. And the Internet is an attractive place to make it, since it offers anonymity and a large user base comprised of many unsuspecting users who are more susceptible of falling for the techniques they use.

Safety Tip

• Always use up-to-date security software.
• Stick to reputable sites and read the user license agreements carefully for anything you are downloading.

What They Share with the World

- ***Personal/Private Information***

A young person who is socially active online—creating personal profiles, communicating with friends, and sharing things about themselves with others—is simply extending what they do offline onto the Internet. But in order to take advantage of online social venues they have to provide self identifying information from user names to photos to personal opinions, likes and dislikes. In this vein of self-expression, they may also provide too much information, which could be used by people with bad intentions or that may damage their own reputations among people they never intended to see it. It could also be used by hackers for the purposes of identity theft. Information posted online could be accessible at any point in the future, so young people should think before publicly sharing anything personal, through any online medium.

Safety Tip

• Understand anything posted online could be made public and is permanent. Avoid sharing too much information–in words, pictures or videos–that could hurt you in the end.
• Use privacy settings and never share your username or password with anyone.

- ***Disparaging Comments and Inappropriate Content***

The anonymity of the Internet can unfortunately encourage offline bad behavior to continue and be exacerbated online. As noted earlier, young people can become targets of cyberbullying, but they can also be as much a participant as a victim in this behavior. Because the information they post can be accessed by anyone virtually forever and can potentially be traced back to them, it is best always to be respectful of others, online or off. More severe comments, particularly those involving physical threats, may be considered a criminal offense.

A new trend is the use of cell phones by kids for "sexting", the act of sending sexually explicit messages or photos electronically, primarily between cell phones. The photos are often of themselves or kids they know. This may seem funny to them, but they don't realize they could be charged with the distribution of child pornography, a very serious criminal offense.

Safety Tip

• Do not post or forward anything online that could hurt another person. Some types of harassment or content can be considered a criminal offense, and can be traced back to you.
• Report any bullying or inappropriate content that can be hurtful to another.

- ***Peer-to-Peer (P2P) File-Sharing Services***
  File-sharing services are a popular tool that enables young people to share media files such as music, movies, or video games. The public discussion and concerns surrounding these types of services have focused a lot on the legal issues (copyright infringements) as well as the age appropriateness of the media being shared (such as pornography or violent games). But in addition to these risks, file-sharing services have increasingly become a destination for cybercriminals to fool people into downloading fake or malicious software. As noted before, their primary motivation is money. A combination of awareness of what is legal and what isn't, proper use of the file-sharing service, and security technology can help young people safely and securely enjoy sharing their favorite forms of media with their friends.

Safety Tip

• Determine if your kids need to use these services at all. They can open up your system to security risks and may be encouraging them to share illegally copied material.
• Always use up-to-date security software to help prevent hackers from installing malicious software on your computer and stealing your personal information.

Be Prepared for What may Reach Them

Below are some additional basic safety measures you and your child can do together today particularly if your children are just beginning to explore the Internet:

- **Keep Computer in a Common Area.**
  Where you can be present while your child is using the computer or spot-check its use, as appropriate to the child's age.

- **Agree to Time Limits for Using the Internet and all Social Devices.**
  Per day, per week, etc. Some security software will allow you to set specific times when your kids can access the Internet.

- **Keep Security Software Up-to-Date. (Provided by HPS with Issued Equipment)**
  Make sure you have purchased and installed up-to-date security software to protect your computer from things such as viruses, spyware, spam.

- **Agree on Websites your Kids can Visit (For Younger Children).**
  Create a list of websites they would like to visit. Make sure they only use sites that are age-appropriate – for example, many social networking sites have minimum age requirements.

- **Use Web Filtering. (Provided by HPS to Filter the same at Home as in School)**
  Use the URL filtering capability, a parental control feature in most computer security software, to ensure your kids access only the kinds of sites you feel are most appropriate for them.

- **Review Content and Privacy and Security Policies of the Sites your Child Frequents.**
  Ensure the content of the site is age appropriate; make sure you understand how and what type of personal information might be collected by the site and how it may be used.

- **Talk with your Kids about Entering Personal Information Online.**
  Advise kids to stay on the agreed upon websites only and not give out personal information such as name, address, phone number, age. If they are tempted to do this because of a contest, poll, or membership form, ask them to discuss with you first and only proceed with your permission and involvement; it could be opening the door to spam or something more harmful such as spyware.

- **Ignore Unwanted Contact from People They Have Never Met.**
  Unwanted online contact will usually stop if they do not respond or react to it. If it persists, advise them to let you or any adult know about it. You should also report this to the site or service being used to contact your child, and the authorities if you or your child feels he/she's in danger in any way.

- **Run a Manual Scan with your Software Security and Check Browser History.**
  After they are finished using the computer, do a manual scan to ensure no infections have occurred; you can teach them how to do this and let them to do it themselves if they are old enough. If you wish to, you can also let your kids know that you will check the browser history when they are finished using the computer to ensure they did not wander off onto websites they shouldn't have visited.

Be Prepared for What They Might Share

In general, common sense and critical thinking are the foundation for young people to become safe, responsible users of the Internet. Any interactions they have online should be done with the same approach as they would offline, so talk to your kids about using the guidelines below:

- **Be Cautious and Wise About What You Post.**
  Think before sharing thoughts, photos, videos that are very personal or less than positive about you, knowing they could also be used against you.

- **Use the Privacy Tools Available in Social Networking Sites.**
  Only those you invite to join your network should be able to see details about you and the people in your network. Even so, it is still wise to think twice before posting anything that is not intended for others to see or know because it can be passed along by friends.

- **Where Possible, Use Nicknames, Not Your Real Name, to Identify Yourself.**
  On social-networking sites, in chat rooms, on blogs.

- **Be Respectful of Others.**
  Avoid posting anything about another person that is libelous, lewd, racist or in violation of a site's or service's terms of service. Not only will it be taken down, but it could be traced back to you and—if it is considered illegal—may land you in trouble.

- **Use Legal File-Sharing Services Only and Ensure They are Set Up Properly.**
  If files are being shared illegally, whether it was intentional or not, you could be held legally responsible for copyright infringement. Also, having the proper settings for the service will ensure that your computer and its contents aren't vulnerable to hackers, viruses, spam, spyware, etc.

Section 8:
Social Networking Tips

As a social medium, the Internet enables young people to stay in touch with friends when they are physically separated from them and sometimes to meet new people who share their interests. Social networking sites, chat rooms, message boards, and blogs are some of the many ways this is possible on the Internet.

Know the Risks

If a young person is socially active on the Internet, he or she is very likely managing at least one personal profile on one or more social networking sites which require or allow them to publicly divulge something about themselves. While this ability is not inherently bad, there may be people familiar or unfamiliar to them who could take advantage of this.

- ***Unwanted Contact***
  Behaviors such as online grooming (technique used by a sexual predator to convince an underage person to have relations with them offline) and cyberbullying (online harassment of classmates or peers) are some examples of unwanted online contact that parents and caregivers should understand and help young people recognize and act on if they ever experience it. In both cases, the first and best response is to encourage kids not to respond to such messages and to alert their parents so they can figure out the next steps together. It's also a good idea not to delete the messages in case they later need to be used as evidence.

- ***Aggressive Commercialism***
  In addition to unwanted contact, parents and caregivers should be mindful of online messages - sometimes legitimate, sometimes malicious – that entice young people to acquire products or services in exchange for information or money. It is important to be aware of how this type of commercialism is delivered, what is being offered, and what young people may do as a result of it. Vendors are using more creative ways to promote their goods and embed their marketing messages, which may make it difficult for a young person to differentiate between an advertisement and the content they are accessing or even interacting with (a technique called immersive advertising). Free offers and promotions for age inappropriate products and services (dating services, gambling services, etc.) may also be compelling enough to a young person to enter personal information that could later be used by the advertiser to deliver continuous, intrusive advertising (as spam or pop-up advertising) or worse, perpetrate cybercrime (hack attacks, identity theft, etc.).

- ***Cybercrime***
  Social networking sites are also an increasingly popular place for cybercriminals to trick people into divulging information or downloading software onto their computers for any number of uses. Their methods range from simple to elaborate.

Sometimes a young person will just see an advertisement or link to download seemingly harmless software that they can use on their own social networking profiles, such as a widget, but which in fact has been infected with malicious software that gets downloaded along with the legitimate software. Some applications that run on social networking sites may encourage young people to complete a survey or provide information that might not be appropriate to share with others. Other times, a young person can be lured to see an "attractive" video but is told it is necessary to download a viewer in order to see it. While downloading a viewer is a normal action necessary to see videos online the viewer could be infected with other software that, once installed, can be used by the cybercriminal to steal information from the computer, spy on the activities of its owner, or other uses depending on the type of malicious software installed.

- ***Behaviors Toward Others***
  Kids and adults believe everything we do online is anonymous and cannot be tracked back to us. Unfortunately, this believe can encourage bad behavior done offline to continue and be exacerbated online. Young people can be victims as well as participants in behaviors such as cyberbullying and harassment. It is important for them to know that information they post can be accessed by anyone virtually forever and can potentially be traced back to them, so it is best to be respectful of others, online or off. More severe comments, particularly those involving physical threats, may also be considered a criminal offense.

Be Prepared

Parents, teachers, and others who care for young people who are socially active online should first set reasonable expectations. Forbidding young people to use social networking sites may force them to go "underground" and find other avenues (e.g. library computers, mobile phones, friends' computers) to continue their social life online. A positive alternative is to teach them how to think critically about what they are seeing, reading, hearing and sharing online.

Below are some guidelines **for students** to follow when they are using social networking sites, chat rooms, blogs, or message boards:

- **Use a Nick Name or Code Name.**
  It is best not to use your real name or to use names that might be sexually suggestive or offensive to others in any way. This can help reduce the likelihood of your being harassed online.

- **Set Your Profiles to Private.**
  Social networking sites can be a great tool for connecting with others. A good way to stay safe using these services is to use the highest level of privacy settings possible, that still allows flexibility to use the site in a way that is useful.

- **Keep Personal Information to Yourself.**
  It is best not to share your address, phone number or other personal information online, with strangers. Don't reveal your actual location or when and where you plan to be somewhere.

- **Think About What You Post.**
  Be cautious about sharing provocative photos or intimate details online, even with people you know or even in a private email or text conversation. The information or conversation could be copied and made public by anyone you share it with - and tough to get removed. Remember: what you say in a chat room or instant messaging session is live - you cannot take it back or delete it later.

- **Keep Your Security Software Up-to-Date.**
  Social networking sites are very popular. Because there are so many people using them, cybercriminals have been known to use stealthy tactics in order to infect the computers of people who use them.

- **Read Between the "Lines."**
  It may be fun to meet new people online for friendship or romance, but be aware that, while some people are nice, others act nice because they are trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.

- **Avoid In-Person Meetings.**
  The only way someone can physically harm you is if you're both in the same location, so – to be 100% safe – don't meet them in person. If you really have to get together with someone you "met" online, don't go alone. Have the meeting in a public place, tell a parent or some other solid backup, and bring some friends along.

- **Be Nice Online.**
  Treat people the way you'd want to be treated. Harassing or bullying anyone online, if considered threatening, can also be considered a criminal offense.

- **Think About How You Respond.**
  If someone says or does something that makes you uncomfortable, block them and don't respond. If they continue, let your parents or another adult know. If the messages are threatening in any way, save the messages and tell your parents as this may be considered a criminal offense.

- **Be Smart When Using a Cell Phone.**
  All the same tips apply with phones as with computers. Except phones are with you wherever you are, often away from home and your usual support systems. Be careful who you give your number to and how you use GPS and other technologies that can pinpoint your physical location. And if your phone has a camera, be sure that the photos you take or share won't get you into trouble. Sending or sharing inappropriate photos of yourself or others to friends on social networks (or text) can end up getting you and others into serious trouble.

Be Prepared

It's important to note that most major social networking sites require all users to be age 13 or older, as noted in their Terms of Use. Assuming they are old enough, below are some guidelines for parents and teachers to consider when it comes to letting kids use social networking sites, chat rooms, blogs, or message boards.

- **Ease Into the Process Together.**
  If you're going to help your kids use social networks safely and responsibly, it's a good idea to use them yourself. There's no need to be a power-user or a technology expert. Just spend a few minutes setting up a profile, using the privacy settings, and connecting with a few close friends or family. It is the best way to help your own kids use it safely.

- **Consider Keeping an Eye on their Social Network use From Time to Time.**
  One way is to connect with your kids is to connect with them on the social network. But if that feels like encroaching too much on their space or if you want your own privacy online, there are social network monitoring services that let you do this. You can also use search engines and the search tools on social-networking sites to search for your kids' full names, phone numbers and other identifying information. If you do it you're not invading their privacy if they're putting personal info in public "places"

online. If their pages are private, that's a good thing, but it's even better if they share it with you. You might also consider having them do this themselves so they can see and learn if they are putting too much out in the public domain that they never meant to.

- **Be Reasonable and Try to Set Reasonable Expectations.**
  Pulling the plug on your child's favorite social site is like pulling the plug on his or her social life. Instead of being protective, it can shut down communication and send kids "underground" where they're more at risk. It's too easy for them to set up free blogs and profiles from anywhere, including friends' houses or even a cell phone.

- **Talk with Your Kids About How They Use the Services.**
  They, not news reports or even experts, are the ones to consult about their online social experience. Help them understand basic safety guidelines, such as protecting their privacy (including passwords), not harassing peers, never talking about sex with people they don't know, avoiding in-person meetings with people they "meet" online, and taking care in what they post - because anything people put online can be grabbed, reworked, and used against them.

- **Support Critical Thinking and Civil Behavior.**
  No laws or parental-control software can protect better than a child's developing good sense about safety and relationships. Research shows that kids who are aggressive and mean online toward peers or strangers are at greater risk of becoming victims themselves. So teach them to be good citizens and friends online as much as offline.

- **Consider Requiring Internet Use in a High-Traffic Place in Your Home.**
  Try to stay aware of your kids' time online by keeping the computer in a shared area of the house. This way, you can encourage a balance between online time and their offline academic, sports, and social times. Know that there are also many ways kids can access the Internet away from home, including on many mobile phones and game players.

Safety Tips for Sharing Videos and Photos Online

Below are some guidelines for young people to follow when posting and sharing videos and photos online.

- **Tough to Take Back.**
  Whatever you post is basically permanent. Even if you later delete it, there is a chance that it has been copied, forwarded or reposted. And there are Web archives that hang on to content even after it has been taken down.

- **What the Background Reveals.**
  Think about what's in the scene you're recording: posters on your wall, photos on a shelf, school or team t-shirts people are wearing, address signs in front of a house or car license-plate numbers all can reveal your identity or location. What you say during recording can, too.

- **'You Are What You Wear.'**
  It's an old maxim with new meaning in online video. Think about what your appearance "says" about you. Would you feel comfortable showing this video to your relatives, boss, potential employer, or college recruiter?

- **Respecting Others' Privacy.**
  Be respectful of the privacy rights of people in your video. If taping in a public place, be sure to ask

permission before including bystanders, and never take video of children without their parents' permission.

- **Everybody's a Videographer.**
  Don't think someone needs a video camera to record video. Most cell phones and still cameras are also now video recorders. Be aware that when people take out a cell phone, they could be using it as a camera or camcorder.

- **Be a Good Citizen.**
  It's your right to express your point of view and even make fun of public officials or policies, but don't be mean or nasty, especially when it comes to people who aren't in the public eye. You can be held legally responsible if you slander, libel or defame someone.

- **Respect Terms of Use.**
  Most video sites have terms of service that you must adhere to. Most of them prohibit sexually explicit content, gratuitous violence, and videos that are harassing, defamatory, obscene, libelous, hateful, or violating other people's privacy. Most responsible sites report videos depicting child exploitation and threatening or illegal acts.

- **Respect Copyrights.**
  All reputable video-sharing sites prohibit the unauthorized use of copyrighted material. Of course that means that you can't rip-off segments from TV shows or movies. But it also means: Think about the music tracks you use in videos.

- **Talk with Kids About Video Bullying.**
  Creating a video that makes fun of or ridicules another person can be extremely hurtful. This and other forms of cyberbullying are a growing problem on the Internet which affects many children and teens.

- **Kids' Web Video Viewing.**
  As with all media, parental discretion is not only advised - it's a necessary part of parenting. Even though most of the major sites prohibit pornography and gratuitous violence, there are videos that are not suitable for younger children and there are some sites that do permit video that may be inappropriate for children or teens. Depending on the age of your kids and their maturity, consider using the filtering features of sites like YouTube or be nearby whenever they are using video sites.

Glossary Of Terms

Acceptable Use Policy (AUP): A set of guidelines and expectations about how staff/students should conduct themselves online.

Blog: An online diary or chronological log of comments published on a web page.

Bandwidth: A measure of capacity for communication channels. It is usually expressed in thousands of bits per second (kbps).

Broadband: Communications or web access which includes cable and digital subscriber lines (DSL).

Browser History: The web browser maintains a list of websites accessed which allows users to review and quickly access again.

Cache: A place to store files which can be temporary or permanent and is used to speed up data transfer.

Chat: Real-time Internet conference between two or more users usually by typing on a keyboard.

Chat Room: A virtual room where the chat session is held.

Cookie(s): Visited websites often use these to track users and their preferences so that the next time the user visits that site, it recognizes the user. The websites stores these files within the user's web browser.

Cyberspace: A reference made to the Internet or the online, digital world.

Database: A collection of information organized in a way in which certain pieces of the data stored can be accessed and selected.

Download: The process of copying a file(s) from an online source to your computer.

Encryption: A way to convert plain text into secret code (cipher text) to prevent anyone but the intended people to read it.

File attachment: A method used in email to attach files to the email message. A paperclip icon often represents the process of attaching a file to the email.

File Name Extensions: Usually three to four letters that appear after a file name and a period which are used to identify an application program that the file was created with.**(.doc, .exe, .TIFF, .JPG)**

Filter: A type of technology which blocks Internet material or activities which are considered not appropriate.

Firewall: Hardware and software that secures computer files by blocking unauthorized access.

Freeware: Software that is available for anyone to use without charge and cannot be sold or distributed without permission.

Graphics File: A file which holds an image. Popular formats are JPG, GIF, TIFF, PNG and BMP.

HTTP: An acronym for (Hypertext Transfer Protocol) which is the standard communication of the World Wide Web.

Hyperlink: A word, image or phrase that when clicked on will go to another location within the document or another website. It usually appears in a different font color.

Internet Service Provider (ISP): A company that provides access to the Internet.

Internet Surfing: A metaphor for browsing the World Wide Web (www).

IP Address: A numeric Internet address separated by periods that is assigned to each computer connected to the Internet.

Phishing: A form of identity theft scamming where email messages link to fake sites that look so similar to the real ones and personal information is requested to be submitted to the fake but very real looking sites.

Podcasts: A web based audio broadcast converted to an audio format for playback such as MP3.

Portal: Websites such as Yahoo and Google who offer services such as email, search engines and other resources as well.

RSS: An acronym (Really Simple Syndication) which will automatically update the subscribed user with updated news, blogs, audio and video.

Spam: Unwanted, junk email.

Upload: The transfer of a file from a computer to a remote site.

URL: An acronym (Uniform Resource Locator) which provides the specific location of accessing a specific item or source on the Internet.

Web Browser: A program used to access the Internet such as Firefox, Internet Explorer, and Safari.

Wiki: A website that allows visitors to add, edit and change contents posted to the site.