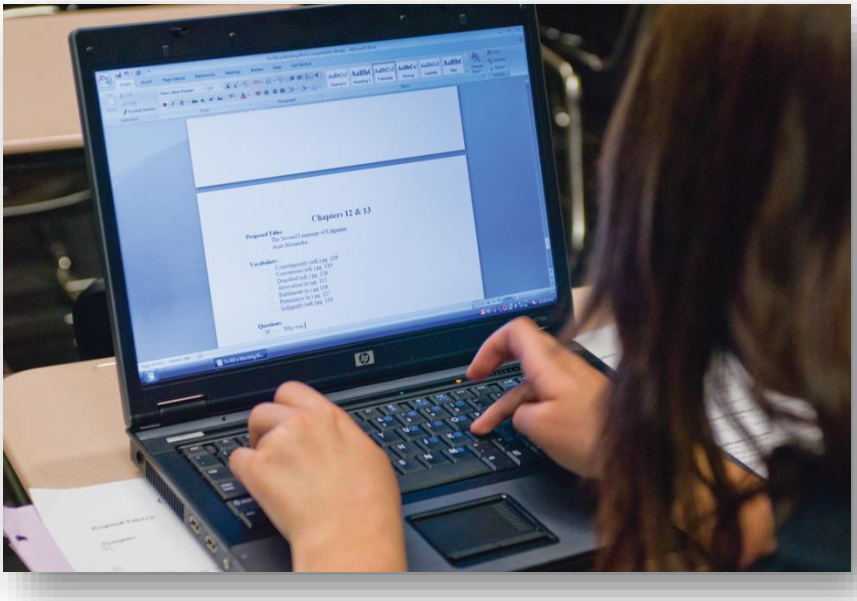

Laptop Handbook

Contents

Lake Washington School District

Secondary Mobile Access for Students – Laptop Handbook

Overview

The Mobile Access for Students program provides each student in grades six through 12 a laptop or netbook computer for their educational use both at home and at school. The use of this tool is designed to enrich the learning environment and to assist teachers as they support students in acquiring the skills, knowledge and attributes outlined in the district's Student Profile.

The privilege of accessing the school network and computer resources is also an opportunity to learn the responsibility of informed, ethical and responsible computer use. This handbook outlines many of these responsibilities. It provides information and resources for families about these expectations.

Parent/Guardian Responsibilities

- Review Laptop Rules & Guidelines
- Review *Student Acceptable Use Procedures*
- Monitor student use when not at school
- Ensure laptop is properly cared for while the student is away from school
- Determine your family's insurance coverage option
- Accept Liability
    - Families are responsible for loss or damage
- Sign Laptop Agreement and return to school

Laptop Rules & Guidelines

The following information is summarized from the district's Student Acceptable Use Procedures. Please review the complete document beginning on page eight of this handbook. Students must understand and follow these procedures.

- Do:
  - Use equipment for educational purposes
  - Use equipment in appropriate manner
  - Use good judgment
- Do Not:
  - Do not use equipment for commercial purposes or personal gain
  - Do not use for political purposes, like trying to influence elections
  - Do not use for anything illegal or indecent
    - No illegal activity, bullying, harassing, or inappropriate images
  - Do not use in a manner that is disruptive to other users, services or equipment
    - No spam or viruses, large amounts of data or trying to hack or crack systems
- Internet Safety
  - Never reveal personal information about yourself or someone else
  - Don't publish student pictures or names on any website without school permission
  - If you see anything dangerous or inappropriate tell a teacher right away
  - Follow school instruction on internet safety, cyber bullying and good online behavior
- Filtering, Monitoring & Network Security
  - The district uses filtering software intended to block inappropriate or objectionable material
    - Filtering software does not always catch inappropriate material. Each user is responsible for avoiding inappropriate sites
    - Don't try to get around filtering, use proxies, special ports or change browser settings
  - Student use of internet is monitored at school
  - Protect passwords:
    - Change as required
    - Do not share your password or use someone else's account
    - Do not put your password in an email or other message.
      If you write it down, keep it safe
    - Do not use "remember password" feature in browser
    - Lock the screen or log off if leaving computer

- Student Data & Privacy
  - Staff maintains the confidentiality of student data in accordance with federal law (FERPA). Permission from parent or guardian is needed to publish student work.
  - Use of the district network, computers, internet and email are not inherently secure or private. The district reserves the right to monitor, review and store and/or disclose any electronic message to law enforcement officials or third parties.
  - Documents, including email, are subject to public records disclosure laws. Backup is made of all district email correspondence for public disclosure and disaster recovery.
- Copyright
  - Don't save or copy any copyrighted material without permission from the owner, unless you comply with the Fair Use Doctrine of the United States Copyright Law.
- Violations of ***Student Acceptable Use Procedures***
  - Violating these rules and guidelines may result in network and computer privileges being taken away. Loss or damage to computers will result in fines. School conduct rules apply and discipline may result from inappropriate use. You could be reported to the police if you engage in illegal activity. See the District Student Discipline Policies and Procedures for more information.

Laptop Use & Care

- Bring the device to school, fully charged, each day unless otherwise instructed
- Always allow a computer scan or update to complete its process
- Do not install, uninstall or modify any application, game or operating system component
- Do not download game emulators, chat clients or peer to peer software
- Do not place stickers or otherwise mark the laptop. Stickers leave residue on laptop parts that is difficult to remove. Identifying stickers of a removable "cling" type are allowed
- Ensure equipment is not lost, stolen or damaged by keeping track of and caring for equipment:
  - Do not leave unattended and follow school rules for securing when necessary, i.e., athletic activities
  - Do not force open the computer lid past its stop point
  - Do not scratch or mar the device's exterior
  - Do not remove district identification barcode
  - Do not insert foreign objects (paperclips, pens) into the device
  - Do not eat or drink near the mobile device
  - Use on a flat, stable surface
  - In the classroom, the device lid should be closed between uses
  - When not in use, the device should be shut down
  - Use only proper cleaning methods
    - Do not use water or cleaning solutions.
    - Wipe surfaces lightly with clean soft cloth or monitor wipes
    - Avoid touching the screen.

Consequences for improper use, loss or damage

- Use of the laptop is a privilege that can be revoked if inappropriately used or damaged.
    - Student and Parent/Guardian will be charged for any damage resulting from abuse or mishandling, or loss of device. A police report is required for any stolen device.
- Inappropriate use or use in conflict with school rules will be in accordance with school discipline policies and may include:
    - Loss of privileges to use or take home computer
    - Suspension/expulsion for serious or repeated offenses
    - Other corrective action
- If equipment is lost or stolen
    - Report lost devices to school immediately
    - If device is stolen, a police report must be filed and copy provided to school
    - Loss of or theft of device due to negligence (leaving unattended, failing to secure per school rules) will result in full replacement cost being assessed
- If equipment is damaged
    - Fees for damages above normal wear and tear, those caused by neglect or multiple incidents of damage, will be assessed fines for the cost of repair/replacement.
    - Refer to laptop fine schedule on page 6.

Laptop Repair Costs

Lost Items:	Replacement cost
Laptop and power cord	$450.00
Battery	$55.00
Power Supply (complete with brick & power cord)	$35.00
Damaged items:	
Cracked or broken screen	$80.00
Damaged LCD Bezel	$45.00
Damaged top case	$80.00
Damaged lower case	$80.00
Damaged palm rest	$80.00
Hard Drive replacement	$70.00
Damaged battery	$55.00
Damaged Keyboard (replacement)	$70.00
Missing key(s) replaced	$10.00
Main system board replacement	$280.00
Other _____(Actual repair cost)	

Insurance Options

Families may wish to protect against liability for lost, damaged or stolen property by reviewing their insurance options. Some homeowner's policy may offer coverage and some may offer this coverage if a rider is acquired. In addition, Lake Washington School District has arranged for an insurance option for families wishing to purchase a specific additional insurance to cover their student's laptop. This insurance can be purchased from Worth Insurance Group. The premium is $54.20 per year and covers accidental damage and theft (police report required). The deductible in this policy is $0. This insurance can be acquired directly by going to http://my.worthavegroup.com/lakewashington. The company also offers coverage for other personal technology devices. If you chose not to purchase the optional insurance or do not otherwise have coverage, you will be responsible for fees for damaged or lost/stolen equipment as defined above.

Internet Access

Need affordable home Internet service? Access to the Internet has become more and more important to students for learning at home and to families for communicating with school. Comcast offers Internet Essentials home Internet service to families with students who qualify for free or reduced price lunch and without internet access for 90 days. This program offers home Internet service for $9.95 a month plus tax, with no activation fees, equipment rental fees or price increases. A low-cost computer ($149.99 plus tax) is available at initial enrollment. For more information visit InternetEssentials.com or call 1-855-846-8376.

Student Use of Electronic Resources Policy & Procedures

Some of the key information from this policy and the following procedure is summarized beginning on page 3. Please review this policy and the procedures that follow.

STUDENT USE OF ELECTRONIC RESOURCES

Student Acceptable Use Procedures (AUP)

Scope

The following procedures apply to all District students and cover all aspects of the District network. The district network includes wired and wireless computers/devices and peripheral equipment, files and storage, e-mail, and Internet content and all computer software, applications, or resources licensed to the District.

Appropriate Network Use

The District expects students to exercise good judgment and use the computer equipment in an appropriate manner. Use of the equipment is expected to be related to educational purposes.

Unacceptable/Prohibited network use by students includes:

- Commercial Use: Using District Network for personal or private gain, personal business, or commercial advantage is prohibited.

- Political Use: Using District Network for political purposes in violation of federal, state, or local laws is prohibited. This prohibition includes using District computers to assist or to advocate, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office.

- Illegal or Indecent Use: Using District Network for illegal, bullying, harassing, vandalizing, inappropriate, or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material), or in support of such activities is prohibited. Illegal activities are any violations of federal, state, or local laws (for example, copyright infringement, publishing defamatory information, or committing fraud). Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that (1) have the purpose or effect or creating an intimidating, a hostile. or offensive environment; (2) have the purpose or effect of unreasonably interfering with an individual's work or school performance, or (3) interfere with school operations. Vandalism is any attempt to harm or destroy the operating system, application software, or data. Inappropriate use includes any violation of the purpose and goal of the network. Indecent activities include violations of generally accepted social standards for use of publicly-owned and operated equipment.

- Disruptive Use: District network may not be used to interfere or disrupt other users, services, or equipment. For example, disruptions include distribution of unsolicited advertising (“Spam”), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of District computers or other resources accessible through the District’s computer network ("Cracking" or "Hacking"). This includes transferring a program or running an unauthorized program from a thumb drive on a computer.

- Personal Use: District Network may not be used for purposes of personal use not specifically authorized by a teacher or other district staff member. This includes connecting personal devices to the district network.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of or access to the district’s computer network or the Internet.

Internet Safety

Students should not reveal personal information, including home address and phone number on web sites, e-mail, or as content on any other electronic medium. Students should not reveal personal information about another individual on any electronic medium. No student pictures or names can be published on any class, school, or district web site unless the appropriate permission has been verified according to district policy. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Internet Safety Instruction

All students will be educated about cyber bullying awareness and response and about appropriate online behavior, including interacting with other individuals on e-mail and/or on social networking sites and in chat rooms. Schools will make every effort to provide Internet Safety Instruction; however, in the absence of such instruction, students are still expected to follow all Acceptable Use Procedures (AUP). Age appropriate training materials will be made available to administration, staff, and families.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children’s Internet Protection Act (CIPA). Other objectionable material could be filtered as identified by the superintendent or designee.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district’s Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings, use of personal portable Wi-Fi devices, and any other techniques designed to evade filtering or enable the publication of inappropriate content;

- E-mail inconsistent with the educational mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not use personal wireless hotspot devices;
- Do not connect personal smartphones, personal computers, personal storage devices, or any non-district device to the district's networks;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen or log-off if leaving the computer.
-

Student Data

District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA). Permission to publish any student work requires permission from the parent or guardian.

Privacy

The District network, computers, internet, and use of e-mail are not inherently secure or private. The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and,
- Any and all information transmitted or received in connection with network and e-mail use.

The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington. Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery.

Copyright

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Discipline

Violation of any of the conditions of use explained in the Student Use of Electronic Resources policy or in these Acceptable Use Procedures (AUP) could be cause for disciplinary action, up to and including revocation of network and computer access privileges, restitution, suspension or expulsion, and/or police report in accordance with District Student Discipline Policies and Procedures.

Adopted: 06/25/12

Revised 07/10/13

Frequently Asked Questions

What if a student forgot to charge their laptop and the battery is dead?
One of the best ways to avoid this issue is to consistently (and constantly) remind students to charge the laptop at home every night. They are expected to bring the laptop to school charged every day. If they fail to do so, they may be able to borrow a spare power cable. Barring that, the student would have to charge their laptop in the school's laptop location (often the library) and lose out on participation in the classroom laptop activities until the battery is charged.

What if my student forgot to bring the laptop to school?
If a student forgets to bring their laptop to school, the student may miss out on laptop-related instructional activities that day. Please help us help your student bring their laptop to/from school daily! Each school has a very small number of "loaner" devices. Priority for these loaners goes to students who experience equipment issues outside their control. When available, a student who forgot their laptop may be issued a "loaner" device by the school.

What happens if a student's laptop is broken after check out?
The student will bring the broken laptop to school to turn it in. A loaner/spare may be checked out on the spot to minimize loss of instructional time. The student is liable for loss or damage to the spare while it's in his or her possession. Once the student's original laptop is repaired, the student will be notified to swap the loaner for the original laptop. If the damage is determined to have been caused by student negligence or abuse, there will be a fine assessed for the repair costs, as stated in the contract.

What if the laptop is stolen?
The loss needs to be reported ASAP to your student's school. The student can then check out a loaner/spare until we settle the loss issue. It is critical that the student maintain good security for the laptop at all times! Please work with your student to reinforce the importance of taking care of the laptop.

My student is on a sports team and/or is taking PE. How will the laptop be kept secure?
PE and coaching staff will instruct students on the specific procedures this week. A secure location will be made available for students in PE and on athletic teams to keep laptops safe during those programs.

How will my student be protected from objectionable material?
As a district, we take the safety and security of our students very seriously. We have invested heavily in state-of-the-art security systems from Palo Alto Networks and Microsoft to secure our students' devices as they explore the World Wide Web. We do this to ensure that we follow state and federal law and that we are compliant with child protection acts.

Known proxy sites and apps are one of the categories that our Palo Alto Networks URL filter system does specifically block. This next generation firewall decrypts and inspects every packet of traffic from student machines to best determine whether or not to filter the site. Approximately 571 new web sites are created every minute, which is over 33,000 every day. If a site or bypass system is brand new or disguised, the filter system cannot block it until it is discovered and added as a threat by Palo Alto Networks. This is universal to how most filter systems and anti-virus systems work.

District technology staff can also add specific sites, as they are discovered, to our web filter, which is a process known as black listing. We do this when required, but Palo Alto Networks has a larger engine to detect and add malicious sites to their filtering system. Unfortunately, there is no filtering system available today that can block every malicious site as fast as they are added. While it is true that whitelisting might be the only way to ensure an almost 100% safe browsing experience, it would limit learning and defeat the purpose of allowing students to explore the millions of safe web sites with valid content for their class projects. Also, white listing might not stop the use of brand-new proxy-bypass apps by students seeking to have an unfiltered web experience.

The district also uses Microsoft Direct Access to force student devices to tunnel back through our district filter so filtering cannot be bypassed while connected to private networks. Microsoft Premier Support designed and set up this system with expert engineers. We use the same Microsoft technologies that Microsoft itself uses for cyber defense, and they are the second most attacked entity in the world after the U.S. Military.

In addition to the technology-based solutions in place, we have policies and procedures in place with respect to both student and staff use of electronic resources. Those policies can be found on our district webpage at: http://www.lwsd.org/About/Policies-Regulations/Technology-Policies/Pages/default.aspx

I don't allow my student to have a password on their home computer so I can monitor its use. How can I know what my student is doing on the school computer?
Get the user name and password from your student. While we prohibit sharing passwords with unauthorized users, parents are explicitly authorized users. We encourage you to know what your student is doing on his or her school laptop.

Home Internet access is expensive. Are families required to provide Internet access at home?
No, we don't require families to have Internet access, though it would be very helpful for students. You should know, however, about the Comcast Internet Essentials program, which provides basic Internet access to families with students who qualify for free or reduced price lunch. This program offers home Internet service for $9.95 a month plus tax, with no activation fees, equipment rental fees or price increases. For more information, visit InternetEssentials.com or call 1-855-846-8376.

Can my student use their own personal computer instead of a district-issued computer?
There are several reasons why we are providing the same computing devices to all students in school. They include safety, instruction, technical support and equity.

Safety: we have installed web filters and have other safety precautions that help prevent students from accessing inappropriate or unsafe websites while at school or home. We can't be sure that devices brought from home meet the same standard.
Instruction: we have purchased and installed several different software packages on district laptops that will not be available on outside computers. The same software, and even the same version, will be on each district laptop, so teachers are able to quickly and more efficiently teach entire classes and help individual students. Trying to teach a lesson with several different kinds of software and/or different versions of that software would be very difficult.
Technical Support: we can provide robust technical support through our technical support staff to a limited universe of computing devices. We can't offer the same level of support to an unlimited universe of devices, which could lead to more computer downtime and lost learning opportunities. This practice is similar to the private sector, where employees are issued a company-owned device to ensure a predictable user experience and optimal technical support.
Equity: some families cannot afford the latest computer or even a computer at all. If all students are using the same device, they can focus on what they are learning with the device, not on who has which device and what else is on it.

Students are not precluded from bringing their personal mobile devices/computers to school, however, students who bring personal computers:

- Must also bring their district computer fully charged and available for use
- Must use the district device when required by the teacher
- May access the Internet only through guest wireless network, where filters are set to the level of protection needed by an elementary student.
- Will not receive technical support or assistance with personal computers
- May not access printing or charge their personal computer at school
- Do so at their own risk. The district is not responsible for lost or stolen personal computers.

What if I don't sign the agreement? I don't want my family to have to be responsible for the laptop.
If no parent or guardian signs the agreement, a student will still get access to a computer when he or she is at school. If the student intentionally damages the computer, families still may be liable for the damage, the same as with any piece of school-owned equipment.

Can kids connect with their home printer or do they have to accomplish it in a different way?
To install a printer at home, follow these steps:

1. Click the Windows Start button and type **Devices and Printers** and press **Enter**
2. Click on '**Add a Printer**'
3. The Add a Device box pops up. Choose your printer and select **Next**
4. When the computer is done adding the printer, click **Print a Test Page** and/or click **Finish**

If your printer is not in the printer list, you may need to download the driver. Students can install drivers and print to some home printers.

- Visit the web site of the manufacturer of your printer and download the driver. You must only download the 'driver only' version of the software as the device will not allow you to install print management software

- Please note the location/folder you save the driver in
- Please note that wireless and network printers require additional steps and possibly software that are beyond the scope of this document and may require manufacturer tech support. Also please note that students are not allowed to install software other than drivers on their computer so printers requiring print management software may not be compatible with the device.

Students are blocked from installing software for security reasons, which will also block the installation of print management software. Check with the manufacturer to see if they offer a driver only solution.

How do I get into the MAS device to add my custom home-network security settings?

For security reasons, the District does not give students or parents Administrator rights to the devices. We set the MAS devices to work with the common security provided by most wireless networks encountered at businesses, libraries, or hotels.
If your home wireless security is more complex, we can offer the following recommendations:

1. Add a segment to your network with less security for use by the MAS device
2. Hardwire the MAS device directly to the home network and bypass wireless
3. Open a hotspot for use by the MAS device separate from your secure wireless network
4. Consider using standard security settings
5. Consider adding security or filtering to your network device, not the computer, such as the offering from www.opendns.com.

Why can't students install software on the MAS devices?

We are bound by the Children's Internet Protection Act (CIPA) to filter Internet content to any devices accessed by students on the LWSD network, including the MAS devices. Some students dislike the filters. Given the opportunity, students could install security-defeating software to bypass this requirement. Some students also would also be tempted to use the devices for illegal file sharing. All of those actions violate the district's Acceptable Use Policy.

I am very concerned about what my student might see on the internet. What can I do?

LWSD goes above the legal CIPA requirements and installs on the devices a filter that works on any network. However, no filter is 100% reliable. To further protect your student, we recommend adding filtering to your home network. One option is using a free filtering service like the one from www.OpenDNS.com that will filter nefarious content from your home network on all devices, including the LWSD MAS device. New websites start up every day and as we become aware of inappropriate sites, we block them. If your student has accessed a website that causes you concern and you feel is inappropriate, please forward the URL to webfilter@lwsd.org.

Internet Safety Resources

The district has selected an internet safety curriculum that is developed by Common Sense Media. As part of this handbook, we have provided some of their tip sheets so that parents can support students in using the internet safely. More resources can be found at www.commonsense.org

FAMILY TIP SHEET

MIDDLE SCHOOL

Common Sense on Connected Culture

What's the Issue?

We are all part of communities. Our schools, our towns, our hobbies or interests all form the centers around which we connect with other people. These communities all have codes of behavior (written or unwritten) that help everyone get along. But in today's 24/7 digital world, we are also part of online communities. And these communities connect us to people we may not know. They connect us in ways where we are known only by screen name, or where we are anonymous. They connect us to people who are sometimes very far away. Whether we're reading or writing an online restaurant review, posting something on a Facebook page, texting a friend, or sharing a picture on a photo website, we're participating in a world where we can be instantly connected to thousands of people at a moment's notice.

Why Does It Matter?

When our kids connect to each other either from a distance or through a screen name, it can impact the way they behave. Actions can be free from discovery or consequences. When something happens anonymously, it's easier for people to behave irresponsibly, cruelly, or unethically. Kids benefit from a code of conduct for online and mobile activity just as they need a code of conduct in the real world. They should be empowered to be good digital citizens, in addition to being good citizens in general. Our kids are creating online communities with every click of the mouse or text they send. And they will have to live in those communities. The information they post about themselves or others will last a long time and travel great distances. So parents and teachers need to help kids think about the consequences of their online actions. Kids should learn that how they behave when they are connected really matters to them, their friends, and to the broader communities they participate in. Finally, there's a great deal at stake. When kids misuse online or mobile technology to harass, embarrass, or bully others, they can do real and lasting harm.

common sense says

Connected culture can be positive or negative – it's what people make it. When guiding our kids, it's important for them to understand that they have a choice in all of their online relationships. They can say something positive or say something mean. They can create great community support around activities or interests, or they can misuse the public nature of online communities to tear others down.

Talk about cyberbullying: It's real. It's everywhere. And remember that kids sometimes will tell you about a friend's problems rather than their own experiences. Make sure your kids know how to deal with a cyberbully, and that if the situation gets serious, urge them to tell a trusted adult about it.

Give kids a cyberbullying vocabulary. Talk about bullies, victims, bystanders (those who witness offensive behavior but don't do anything to stop it), and upstanders (people who actively try to stop cyberbullying). It will help them understand what roles they play or could play.

Encourage positive posting. Are your kids fans of YouTube? Have they said something encouraging about something they've seen and loved? Have they added knowledge to a wiki or shared their experience on a hobby or interest site? From the earliest ages, kids need to know they can add positively to the online world.

Remind kids that texts and IMs may not persist, but they still have impact. Anything they say or do with their phones or through quick messages may seem to disappear when the devices shut down, but the impact on others remains – whether for good or bad.

common sense media

FAMILY TIP SHEET

MIDDLE & HIGH SCHOOL

Common Sense on Cyberbullying

What's the Issue?

Cyberbullying is the use of digital media tools, such as the Internet and cell phones, to deliberately humiliate and harass others, oftentimes repeatedly. Though most teens do not do this, those who do are often motivated by a desire for power, status, and attention – and their targets are often people they are competing with for social standing. Cyberbullies often take advantage of the Web's anonymity to antagonize someone without being recognized.

Cyberbullying can take a variety of forms, such as harassing someone, impersonating someone, spreading rumors, or forwarding embarrassing information about a person. A bully's mean-spirited comments can spread widely through instant messaging (IM), phone texting, and by posts on social networking sites. This can happen rapidly, with little time for teens to cool down between responses. And it can happen anytime—at school or at home—and oftentimes it involves large groups of teens.

Why Does It Matter?

Cyberbullying is similar to face-to-face bullying, but online tools magnify the hurt, humiliation, and social drama in a very public way. Whether it's creating a fake Facebook or MySpace page to impersonate a fellow student, repeatedly sending hurtful text messages and images, or spreading rumors or posting cruel comments on the Internet, cyberbullying can result in severe emotional and even physical harm.

And though anyone can spot bullying behavior in the real world, it's much more difficult to detect it in the online world. Sometimes an entire social circle will get involved, and then it becomes harder for an individual teen to disengage from it. In fact, whole groups of teens may be actively or passively participating, and the target can feel that it is impossible to get away from the bullies. In addition, hurtful information posted on the Internet is extremely difficult to remove, and millions of people can see it.

The following tips can help you recognize the warning signs of cyberbullying and serve as a guide for talking to your teens about preventing it.

What Families Can Do

You seem down. What's going on at school? Is anything upsetting happening online?

I'm here for you and so are your friends. Talk to me anytime.

Are there any teachers at school who have dealt with these kinds of situations before? I think you should tell one of them about what's been happening.

Bullies want attention, power, and status, which explains why they need to cause drama.

I saw a news story about a teen who was bullied online. What would you do in that situation?

common sense says

Recognize context. Cyberbullying is often not thought of as "cyberbullying" to the teens involved. Even though an incident has a history, a story, and nuance, rather than referring it as "cyberbullying," try the words "digital cruelty," "abuse," or "being mean" online.

Help teens understand when behavior crosses the line. Help your teen tune into his or her own feelings. If they feel emotionally or physically scared, it's time to get help.

Encourage empathy. Help teens understand the detrimental impact of cyberbullying on people who are targeted, now and later in life. Encourage them to listen to targets and to become their allies.

Be realistic. Teens have their own social dynamics that often don't include parents, so helping them directly may be difficult. Encourage teens to find friends or other trusted adults to help them through the situation, even if it's not you. Websites are often slow to respond, if they respond at all, but reporting an incident to a website administrator can be an empowering step.

Remember that your teen might be the bully. Teens can take different roles in cyberbullying at different times. A teen who is cyberbullied might turn around and cyberbully someone else to feel powerful again. Ask questions to understand what role or roles your teens are playing.

Tell them to disengage. Encourage your teens to ignore and block the bully, and even log off the computer for a while. Point out that cyberbullies are often just looking for attention and status, so don't let them know that their efforts have worked.

FAMILY TIP SHEET

MIDDLE SCHOOL

Common Sense on Safe Online Talk

What's the Issue?

Kids love connecting with others online. Most young people talk online with their friends and family rather than strangers. But as a parent, you might be concerned that a stranger with bad intent could contact your child.

"Online predatory behavior," as it is commonly known, is when adults contact kids or teens over the Internet in an attempt to "groom" them for inappropriate sexual relationships. Many experts, however, have found that the more realistic threat for teens online is actually "online sexual solicitation." This means encouraging someone to talk about sex, give personal sexual information, or send sexual photos or video. (It does not always mean asking for sex.) For instance, teens might receive inappropriate requests or messages from strangers or acquaintances. However, contrary to popular belief:

- Teens (ages 13 to 17) are more at risk for online solicitations than "tweens" or children
- The majority of online solicitations come from teens themselves, or from young adults (ages 18 to 25)
- Adults that solicit teens are usually up-front about their true age and intentions (Subrahmanyam and Smahel, 2011).

Why Does It Matter?

When teens are led astray about what to look out for online, they can find themselves in unhealthy situations without realizing it. The allure of these kinds of relationships is not surprising, particularly for teens who are already vulnerable. Solicitors can provide teens with a boost of self-esteem with compliments and attention. And once teens engage in these relationships, they might agree to do things they would not normally do because of the imbalance in power between them and the solicitor. It is often not until much later that they realize that they were being manipulated.

common sense says

Discuss responsible online behavior. Talk about who it's okay to chat with and what is okay to talk about. Remember that many young teens are beginning to experiment with flirting and relationships. This is normal. But online flirting with strangers or acquaintances is always risky. Flirting can quickly lead to inappropriate conversations or requests. It may also lead young teens to believe they are in a serious, romantic relationship with someone they don't really know. Both situations can make teens feel uncomfortable or manipulated.

Block, ignore, or leave. Most young teens know how to brush off unwanted contact. Encourage this behavior.

Make sure your child feels safe telling a trusted adult. If something creepy or inappropriate happens, young teens need to know they will not get in trouble if they tell you or another trusted adult about it.

Talk to your child about healthy relationships. It can be difficult for some young teens to recognize when others are manipulating them, especially those young teens that want to experiment or prove that they are mature. Discuss which factors make relationships healthy, and why young teens should not compromise on these values.

Look for warning signs. Does your child seem withdrawn, spend endless hours online, or appear to be hiding something? Young teens who wind up in inappropriate online relationships often show these warning signs. If you think this might be happening, ask your child about it.

Sources

The Berkman Center for Internet & Society at Harvard University. *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force*. 2008.

Smith, A. "Teens and Online Stranger Contact." Pew Internet & American Life Project. Oct 14, 2007. (http://www.pewinternet.org/Reports/2007/A.aspx).

Subrahmanyam, K., and Smahel, D. *Digital Youth: The Role of Media in Development*. 2011, Springer, New York.

Ybarra, M., and Mitchell, K. J. "How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassement Occurs." *Pediatrics* (2008). 121(2), pp. e350-e357.

Wolak, K., Mitchell, K., and Finkelhor, D. "Online Victimization of Youth: Five Years Later." 2006. *National Center for Missing & Exploited Children Bulletin*. (http://www.unh.edu/ccrc/pdf/CV138.pdf).