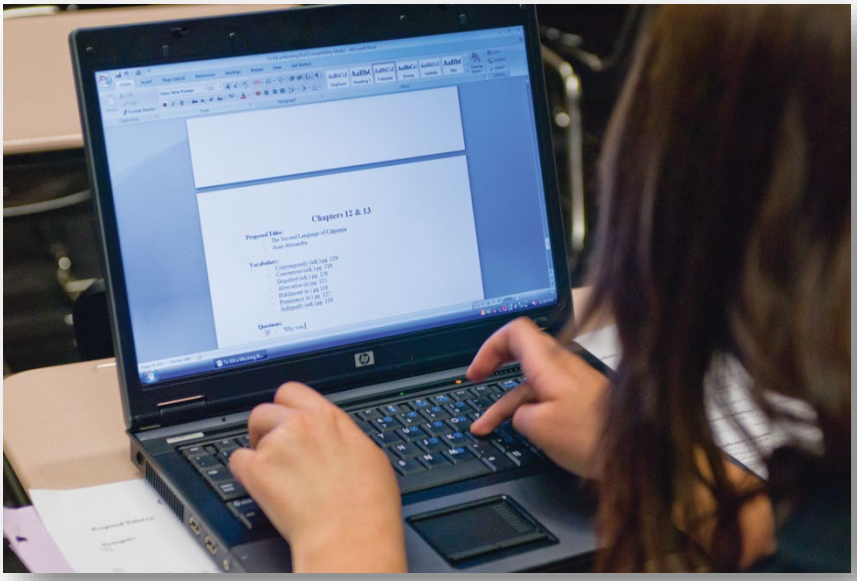

Laptop Handbook

Contents

Overview 2

Parent/Guardian Responsibilities 2

Laptop Rules & Guidelines 3-4

Laptop Use & Care 4

Consequences for improper use, loss or damage 5

Internet Access 5

Student Use of Electronic Resources Policy & Procedures 5-8

Frequently Asked Questions 9-12

Internet Safety Resources 13-14

Overview

The Mobile Access for Students program provides each Lake Washington School District student a laptop computer for their educational use. 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.

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

Laptop Rules & Guidelines

The following information is summarized from the district's Student Acceptable Use Procedure Please review the Student Use of Electronic Resources section under Policies and Regulations on the district website. Students must understand and follow these procedures.

- Do:
  - Use equipment for educational purposes.
  - Use equipment in appropriate manner.
  - Use good judgment.
  - Protect passwords:
    - Change as required every 90 days after start of school.
    - Do not share your password or use someone else's account.
    - Do not put your password in an email or another 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.
- 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.
  - Do not try to get around filtering, use proxies, special ports or change browser settings.
  - 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. Stickers of a removable "cling" type are allowed.
- 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.

- 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:
  - 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.
- 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.
  - Be sure to RESTART your computer on a regular basis.
- Use only proper cleaning methods:
  - Do not use water or cleaning solutions.
  - Wipe surfaces lightly with clean, soft cloth or monitor wipes.

Consequences for improper use, loss or damage

- Inappropriate use or behavior in conflict with school rules will be in accordance with school discipline policies and may include:
  - Corrective action including more restrictive access to computing resources
  - Suspension/expulsion for serious or repeated offenses.
- 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.

Internet Access

Need affordable home Internet service? Access to the Internet has become critical to students for learning at home and to families for communicating with school.

Information can be found on the District web page for Computers/Internet Access: Community Resources - Lake Washington School District (lwsd.org) and the new Federal Get Internet page: Get Internet | The White House

The district offers free cellular hotspots to families in need. Contact your school directly for more information about how to check these out.

Student Use of Electronic Resources Policy & Procedures

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.

Should personal equipment be used on the district's networks, the district reserves the right to gain access to the device for analysis to resolve any identified issues or threats. As a condition of using the district's networks, a student will provide requested device immediately.

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").
- 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, missed 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 email 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 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, including immediately leaving and reporting inappropriate sites to school officials.
- 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.
- The use of USB (aka thumb drive) emulators to run games, bypass proxy, or otherwise run non-district installed .exe files or other emulation software is strictly prohibited. USB drives should only be used for non-executable, school related content.
- District provided storage (e.g., OneDrive, Outlook, laptop hard drive, or Class Notebook) is for storing only content generated as part of the student's education or required for educational process. Attempt to store or storage of games or any executable files or inappropriate content is strictly prohibited.
- 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 person's account.
- Do not use personal wireless hotspot devices while at school.
- Do not connect personal smartphones, personal computers, personal storage devices, or any non-district device to the district's LAN or WLAN network. Connection to GUEST network is allowed.

- 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.

Attempts to install or installation of malware, proxy bypass software, network, administration tools, local administration tools, or any software, malware, or tool that allows for the manipulation of user accounts or administrative privileges are strictly prohibited. Such install attempts or installation of such malware, software, or tools will be considered exceptional misconduct.

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 email 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.
- Email.
- Internet access.
- All information transmitted or received in connection with network and email 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.

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:
06/25/2012

Revised:
07/10/2013
10/16/2017
7/2/2018
7/23/2019
8/5/2020
7/2/2021
5/18/2022

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 request a loaner laptop from the library for the day. 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 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 checkout?
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. Once the student's original laptop is repaired, the student will be notified to swap the loaner for the original laptop.

What if the laptop is stolen?
The loss needs to be reported ASAP to your student's school along with a police report. 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 always! 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. A secure location will be made available for students in PE and on athletic teams to keep laptops safe during those programs.

How are students kept safe online?

When students' use district issued laptops, while at school or home, they access the internet through district filtering and security systems. These systems are provided to help ensure students' online safety as they explore the World Wide Web. They are also designed to meet the federal requirements outlined in the Children's' Internet Protection Act (CIPA) with which the district must comply. LWSD computer filtering relies on security systems and Microsoft. These state-of-the-art filtering systems are used to block inappropriate or objectionable material and provide online computing environments for students which support their education. However, no filtering system is 100% reliable. It is reported that over 33,000 web sites are created each day and new sites with objectionable material for students can be missed or may have not yet been indexed for filtering. Students are responsible to help ensure their online safety and should report any inappropriate sites as well as immediately leave the site. The district's Acceptable Use Policy prohibits the use of proxy bypass or other tools that can circumvent the district's filtering systems.

General categories of sites which are blocked by district firewalls include: Alcohol, tobacco and abused drugs; nudity and adult content; dating; social networking; games, shareware and freeware; streaming media and music purchase and download; web hosting and web based email, online storage and backup; hacking, malware, and phishing; internet portals, personal sites and blogs, private IP addresses; proxy bypass/avoidance and dynamic DNS; and translation sites which can circumvent filtering systems; as well as other identified objectionable content.

District technology staff can block additional sites identified as containing inappropriate content. If sites within blocked categories are needed for specific instructional purposes, teachers can request those sites be opened for access.

Students computing offsite on district-issued computers are tunneled back through district firewalls so that they cannot bypass safe student filtering while connected to private networks.

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 username 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 a reduced monthly price. For more information, visit InternetEssentials.com or call 1-855-846-8376. Information can be found on the District web page for Computers/Internet Access: Community Resources - Lake Washington School District (lwsd.org) and the new Federal Get Internet page: Get Internet | The White House

The district offers free cellular hotspots to families in need. Contact your school directly for more information about how to check these out.

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 can 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: LWSD provides robust technical support through our on-site and after hours technical support team to our district owned and supported devices and systems. We can't offer the same level of support to BYOD / personal devices and systems, 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 standard district issued 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.
- 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 or electronically acknowledges 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 Students will be subject to disciplinary actions. If there is no other computer at home, the student may be at a disadvantage to complete and/or submit homework.

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 basic print 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 print 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.

As an added measure, at home, parents can add filtering to their 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.

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 might be tempted to use the devices for illegal file sharing. All those actions violate the district's Acceptable Use Policy.

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?