

Computers in Hand,
What Parents Need to Know

Greg Wasserman
Director of Guidance
The Wheatley School

Popular Teenage Technology

- Facebook 
 - Most popular social networking website; over one billion users worldwide
 - Recommended age of user: 13
- Twitter 
 - Users post personal thoughts, pictures or videos, repost other's comments, follow celebrities, political figures, etc.
 - Most popular user: Katy Perry (49,363,470 followers)
 - Recommended age of user: None
- Live Journal 
 - A virtual community where Internet users can keep a blog, journal or diary
 - Recommended age of user: 13
- Vine 
 - Vine is a mobile app by Twitter that enables its users to create and post short video clips.
 - Video clips created with Vine have a maximum length of six seconds and can be shared on a variety of social network sites
 - Recommended age of user: 17

- Instagram 
 - An online photo-sharing and social networking service that enables its users to take pictures, apply digital filters to them, and share them
 - Recommended age of user: 13
- Tumblr 
 - A blogging platform that allows users to post text, images, videos, links, quotes and audio to their tumblelog, a short-form blog
 - Recommended age of user: 18
- Ask.fm 
 - An interest-based social Q&A website
 - The user can choose to accept questions from anonymous sources
 - Recommended age of user: 13
- Snapchat 
 - users can take photos, record videos, add text and drawings, and send them to a controlled list of recipients. Users set a time limit for how long recipients can view their photos, up to 10 seconds, after which it will be deleted from the recipient's device and the company's servers
 - Recommended age of user: 13*
 - *** 2014 Spapchat Hack***

- Kik Messenger 

- An app that allows users to message, send video/pictures and more without using your service provider
- Recommended age of user: 17

Similar apps: Viber, Whatsapp, Oovoo

- Omegle 

- Omegle is an app for meeting new friends. When you use Omegle, it picks another user at random and let you have a one-on-one chat with each other either via text or video.
- Chats are completely anonymous, although there is nothing to stop you from revealing personal details if you choose to.
- Recommended age of user: 17

- Spoofcard 

- An app that allows users to hide or falsify their caller id, change their voice, record calls or add background sounds to their conversations

Technology Quiz

- What is an Internet Troll?

- An internet troll, or simply troll in Internet slang, is someone who posts controversial, inflammatory, irrelevant or off-topic messages in an online community, such as an online discussion forum or chat room, with the primary intent of provoking other users into an emotional response or to generally disrupt normal on-topic discussion.

- What is a hashtag?

- By adding a hash (#) in front of the word, phrase or acronym that best describes your message. This allows people to search very easily for common interests or topics

- Is online harassment/bullying prosecutable?

- Yes, Nassau County District Attorney's office prosecutes cyberbullying

- True or False, a cell phone is the only way you can text or make phone calls?

- False, you can use an iPod/iPad, Computer, Handheld Gaming device

Threats and Dangers

Common Teenage Mistakes

- Sharing passwords or devices
 - "Young, in Love and Sharing Everything, including a Password," NY Times article states that teenagers share passwords as a sign of trust
 - When individuals share passwords or devices, it can bring about many problems. If a friendship dissolves, teenagers are more likely to use these in malicious ways against each other.
- Multiple accounts
 - Now that teenagers realize that parents, colleges, etc. monitor their social network accounts, they have created alias accounts.
Ex. John Smith becomes J0hn Smith
 - With email addresses so readily available, it has become very easy to accomplish this
- Posting/sending graphic, inappropriate or suggestive pictures/text
 - Teenagers recklessly post content online or send them to each other without thinking of the consequences

Instagram



COLLEGE

80% Of College Admissions Officers Use Facebook To Check Out Students

Source: www.collegeboard.com, 1/14/2014

More than 80% of college admissions officers use Facebook to check out students, according to a new survey. The survey also found that 70% of admissions officers use social media to check out students.

College admissions officers are increasingly turning to social media to check out students. A new survey by College Board found that 80% of admissions officers use Facebook to check out students, up from 60% in 2011. The survey also found that 70% of admissions officers use social media to check out students.

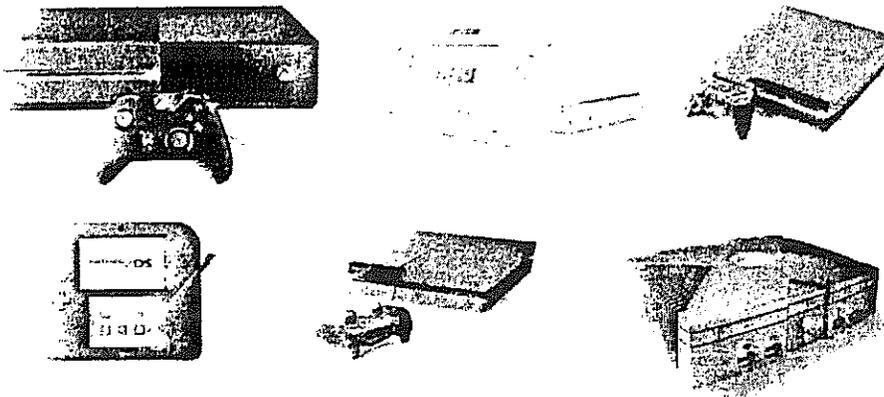
College admissions officers are increasingly turning to social media to check out students. A new survey by College Board found that 80% of admissions officers use Facebook to check out students, up from 60% in 2011. The survey also found that 70% of admissions officers use social media to check out students.

College admissions officers are increasingly turning to social media to check out students. A new survey by College Board found that 80% of admissions officers use Facebook to check out students, up from 60% in 2011. The survey also found that 70% of admissions officers use social media to check out students.

College admissions officers are increasingly turning to social media to check out students. A new survey by College Board found that 80% of admissions officers use Facebook to check out students, up from 60% in 2011. The survey also found that 70% of admissions officers use social media to check out students.

So, I've taken away my child's computer, cell phone, iPod and iPad, there is no way for them to get online and be in danger.

Wrong



Bullying/Cyberbullying

- Using technology has become a very dangerous way for teenagers to bully
 - By not having the person in front of you, it makes it easier to say mean and hurtful statements
- While there are websites/apps that enable cyberbullying (ask.fm, formspring), teenagers have found ways to turn even the most innocent apps into cyberbullying forums
 - Negative comments can be made on Youtube, Facebook, Twitter, Instagram, Vine.....basically any site that allows comments
 - Spoofing is the practice of altering identification of a caller's number so that a different number appears on the receiver's caller ID (SpoofCard, iSpoof, Crazy Call)
 - Beauty Pageant on Instagram allows for kids to rank each other publicly by their looks

Porn

- 30% of all Internet traffic involves pornographic sites; some sites report over 100 million hits per day
- Reddit (also reddit) is a social news website on which users can post links to content on the web as well as private pictures and video
 - In addition to mainstream and traditional topics, there are also forums for Gore, WTF, Porn, etc.
- Chatroulette and other webcam sites have gained popularity in recent months
- Teenagers do not realize that in many instances, receiving or sending naked text messages (sexting), is illegal and can bring serious consequences

How to protect yourself and your family

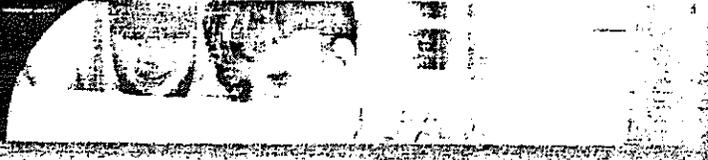
"My teen girl has been posting pics and dirty talking online. She has been posting suggestive pics and talking dirty to guys online. I think she has been doing it on web cam too. Now that I found out and grounded her she is threatening to kill herself . What should I do > I can't get her into see a counselor for a few weeks."

What can Parents do?

- Set rules and talk to your children
 - Responsible use of technology needs to be taught at an early age. It becomes far harder to educate or limit technology use after it has already become part of their lives
- Change dangerous settings
 - Many apps now incorporate location sharing tools (Facebook, Instagram), so it is important to educate your children on why this is dangerous and turn off the settings on these apps
 - Did you know that you can set restrictions on an iPhone/iPad/iPod? Through these settings, you can limit purchase, set up internet restrictions and camera settings
- Monitor their devices
 - You can view the apps that have been downloaded by going into the itunes program associated with their phone and selecting "Apps" from the Library
 - As their parent, you are entitled to check their devices
 - Set up user accounts on shared or personal computers. Through these accounts you can limit and monitor usage
 - Filtering Tools: Allow parents to establish a strong defensive mechanism to prevent children from accidentally encountering or intentionally accessing inappropriate sites and content, such as pornography, vulgar language, and hate sites.
 - Monitoring Tools: Allow parents to collect "intelligence" and check up on their child's online activities by tracking a child's website visits, emails, instant messaging, and other Internet behavior.

What can Parents do?

- Google your child's name and any email addresses
- Stay connected and educated
 - There are numerous websites that frequently detail threats and educate parents on current trends, both online and using smartphones
 - Read the Guidance Newsletters and Guidance Alerts
 - Attend Guidance Office and Wheatley/Roslyn Coalition events
- Additional Resources
 - [MyMobileWatchdog](#) – Is an app that allows parents to monitor all cell phone activity (Available for Blackberry and Android phones)
 - [Findmykids/FamilyTracker](#) – An iPhone app that allows you to see you children's phone's location on a map
 - [StealthGenie](#) – An iPhone/Android app that allows you to monitor all cell phone usage
 - KidTrack – Is an Android app that allows parents to monitor cell phone activity
 - <http://www.internetsafety101.org/> - Fantastic website that provides up-to-date information regarding internet and technology safety



TWO- TO FOUR-YEAR-OLDS

KIDS AT THIS AGE

- Will accept media content at face value
- Don't have the critical thinking skills to be online alone
- May be frightened by media images, both real and fictional
- Risk moving from appropriate to inappropriate sites through hyperlinks

GUIDELINES

- Always sit with your child at the computer (EIE recommends that children at this age not be exposed to the Internet).
- Parents can begin teaching basic computer skills by introducing age-appropriate games and educational programs.

FIVE- TO SEVEN-YEAR-OLDS

KIDS AT THIS AGE

- Are very capable at using computers and cell phones (i.e., following commands, using the mouse, and playing computer games)
- Will accept media content at face value
- Don't have the critical thinking skills to be online or text alone
- May be frightened by media images, both real and fictional
- May be unintentionally exposed to inappropriate websites
- Are vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
- Risk moving from appropriate to inappropriate sites through hyperlinks

GUIDELINES

- Always sit with your children when they are online.
- If children are introduced to the Internet, parents are encouraged to:
 1. Use kid-friendly search engines and/or "walled gardens" with parental controls. (See Appendix B-B for a list of kid-friendly search engines.)
 2. Set age-appropriate filtering at the most restrictive level.
 3. Create a personalized online environment by limiting your kids to their list of favorite or "bookmarked" sites.
 4. Keep Internet-connected computers in an open area where you can easily monitor your kids' activities.
 5. Start teaching kids about privacy. Tell them never to give out information about themselves or their family when online.
 6. Have your kids use an online nickname if a site encourages them to submit their names to "personalize" the web content.
 7. Block or disallow the use of instant messaging (IM), e-mail, chat rooms, mobile Internet, text, picture and video messaging, and access to or message boards at this age.

NOTE: Services such as The Children's Internet offer children safe, age-appropriate Internet experience available for a monthly fee. If you do allow your child to use a mobile device, use a kid-friendly mobile device (See B-16).



EIGHT- TO TEN-YEAR-OLDS

KIDS AT THIS AGE GUIDELINES

- Are interested in the activities of older kids in their lives, are starting to develop a sense of their own identity, and they tend to be trusting and do not often question authority
 - Enjoy surfing online and using mobile devices for fun and playing interactive games
 - May be using e-mail and may also experiment with instant messaging (IM), chat rooms, and message boards (online forums), social networking and other interactive sites, and mobile devices although the use of these programs is strongly discouraged at this age
 - Are curious and interested in discovering new information
 - Lack the critical thinking skills to be online alone
 - Are vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
 - May be frightened by realistic portrayals of violence, threats, or dangers
 - May begin to communicate with online acquaintances they may not know in real life
 - May be influenced by media images and personalities, especially those that appear "cool" or desirable
 - May be exposed to search results with links to inappropriate websites
 - Are vulnerable to online predators if they use chat rooms, message boards, social networking, text messaging or instant messaging (IM)
- Sit with your kids when they are online, or make sure they only visit sites you have approved.
 - Keep any Internet-connected computer in an open area where you can closely monitor your child's online use.
 - Set parental controls at the age-appropriate levels and use filtering and monitoring tools as a complement—not a replacement—for parental supervision.
 - Use kid-friendly search engines or search engines with parental controls.
 - Do not allow instant messaging, chat rooms, or social networking sites intended for older audiences at this age. (See Appendix B-12 for a list of social networking sites for younger children.)
 - You and your child should have the same e-mail address. Establish a shared family e-mail account with your Internet service provider rather than letting your kids have their own accounts.
 - Get to know your child's online activities and friends. Talk to your kids about their online friends and activities just as you would about their other activities.
 - Teach your kids to always come to you before giving out information through e-mail, message boards, registration forms, personal profiles, and online contests.



FOURTEEN- TO EIGHTEEN-YEAR-OLDS

KIDS AT THIS AGE

GUIDELINES

- ⊖ Crave both group identity and independence
- ⊖ Tend to download music, use instant messaging (IM), e-mail, social networking sites, and play online games; most of them have visited chat rooms, and many have participated in adult or private chat
- ⊖ May push the boundaries of safe online behavior by looking for gross humor, gore, gambling, or explicit adult sites
- ⊖ Are more critical and selective in their media interests and activities
- ⊖ Are more likely to receive unwanted sexual comments online
- ⊖ Receive the highest percentage of pornographic spam
- ⊖ Are interested in building relationships with online acquaintances (especially true of girls)
- ⊖ Are more likely to be asked for a real-life meeting by an online acquaintance, and more apt to accept
- ⊖ Are still vulnerable to online marketers who encourage them to give out personal information through surveys, contests, and registration forms
- ⊖ May be bullied or be bullying others online
- ⊖ Are more likely to use credit cards online
- ⊖ May be experimenting with online gambling

REMEMBER: A teen's prefrontal cortex is not fully developed at this age; teens still need your guidance!

- ⊕ Create a list of Internet house rules with your teens (see *Rules 'N Tools** Youth Pledge). You should include the kinds of sites that are off limit.
- ⊕ Set parental controls at the age-appropriate levels and use filtering and monitoring tools as a complement—not a replacement—for parental supervision. Use parental controls on all Internet-enabled devices such as cell phones, gaming devices, iPods, and PDAs.
- ⊕ Keep Internet-connected computers in an open area and out of your teens' bedrooms.
- ⊕ Talk to them about their online friends and activities just as you would about their offline activities.
- ⊕ Talk to your teens about their IM list and make sure they're not talking to strangers. Your teens should only use parent-approved buddy lists and you should check their lists regularly to make sure your teens do not alter them.
- ⊕ Insist that your teens tell you first if they want to meet an "online friend." Then check out the online friend, and if you feel the online friend is safe, accompany your child to the meeting.
- ⊕ Teach your teens to protect personal information (see *Rules 'N Tools**).
- ⊕ Help protect them from spam. Tell your teens not to give out their e-mail address online or respond to junk mail, and to use e-mail filters.
- ⊕ Teach your teens responsible online behavior. File-sharing and taking text, images, or artwork from the web may infringe on copyright laws.
- ⊕ Talk to them about ethical behavior. They should not be using the Internet to spread gossip, bully, or threaten others.
- ⊕ Oversee financial transactions online, including ordering, buying, or selling items.
- ⊕ Discuss gambling and its potential risks, and remind your teens that it is illegal for them to gamble online.
- ⊕ Do periodic spot checks (like checking browser history files) to monitor your kids' online behaviors.

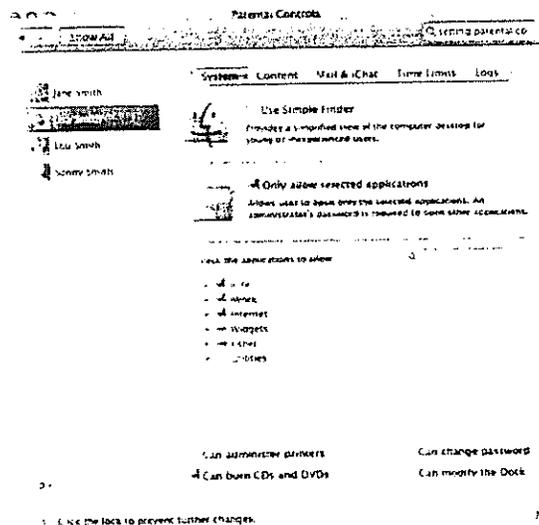
REMEMBER: Kids are safest if not on social networking sites. Follow the *Rules 'N Tools** if you allow your teens to use them.

About.com Macs

Set Up Parental Controls on Your Mac

By Tom Nelson

Parental Controls - System and Applications Setup



Each managed account can have its own Parental Control settings.

The Parental Controls window is divided into two main areas. The left side houses an account pane that lists all of the managed accounts on your Mac.

Managing Access to System Functions and Applications

1. Select the managed account you wish to set up with Parental Controls from the list pane on the left.
2. Click the 'System' tab.
3. Parental Controls lists the available options for controlling access to system functions and applications.
 - **Use Simple Finder.** Simple Finder is a Finder replacement that has a simplified user interface. The user is allowed to access a selected list of applications, and create and edit documents in their home folder, and prevented from accessing or modifying most system settings.
 - **Only allow selected applications.** This option allows you to select the applications the managed user can access. Parental Controls organizes the applications into the following groups: iLife, iWork, Internet, Widgets, Other, and Utility. You can expand each group by clicking the triangle next to its name. Once you expand a group, you can place a check mark next to the individual applications you want the user to be able to access.
 - **Can administer printers.** Allows the managed user to select a printer other than the default printer.
 - **Can burn CDs and DVDs.** Lets the user burn files to optical disks.
 - **Can change password.** Allows the user to change his/her password.
 - **Can modify the Dock.** Lets the user add applications to the Dock for easier access.
4. Make your selections by placing check marks next to the appropriate items.

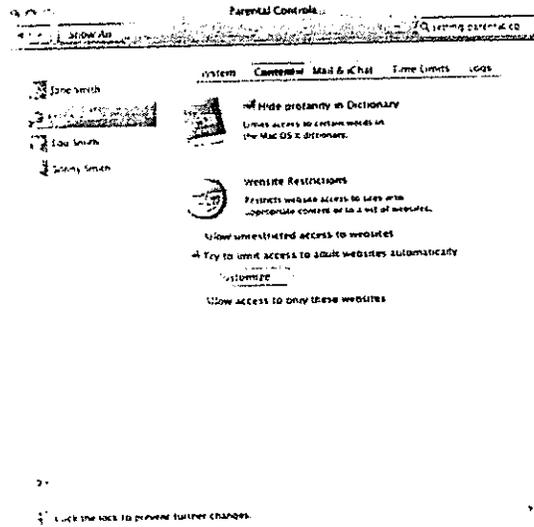
This About.com page has been optimized for print. To view this page in its original form, please visit: http://macs.about.com/od/switchersnewusers/ss/parentalcontrol_2.htm
 ©2014 About.com, Inc. All rights reserved.

About.com Macs

Set Up Parental Controls on Your Mac

By Tom Nelson

Parental Controls - Content



You can restrict access to websites, and filter access to the dictionary

The 'Content' section of Parental Controls lets you control which web sites the managed user may visit. It also lets you place a filter on the included Dictionary application, to prevent access to profanity.

Set Up Content Filters

1. Click the 'Content' tab.
2. Place a check mark next to 'Hide profanity in Dictionary' if you wish to filter the included Dictionary application.
3. The following web site restrictions are available from Parental Controls:
 - **Allow unrestricted access to web sites.** This is the same type of access a standard user would have to the web.
 - **Try to limit access to adult web sites automatically.** Web sites containing adult content will be restricted according to a proprietary method that Apple uses. You can click the 'Customize' button to add specific web sites to 'allow' or 'never allow' lists.
 - **Allow access to only these web sites.** Selecting this option produces a pre-populated list of well-known kid-friendly sites. You can add sites to the list, as well as remove sites from the list.
4. Make your selections.

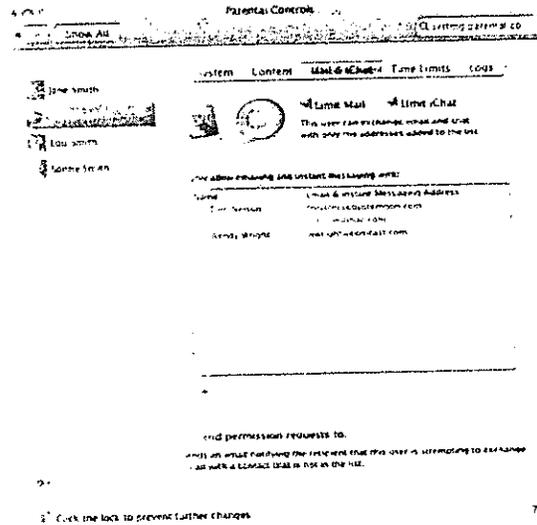
This About.com page has been optimized for print. To view this page in its original form, please visit: http://macs.about.com/od/switchersnewusers/ss/parentalcontrol_3.htm
 ©2014 About.com, Inc. All rights reserved.

About.com Macs

Set Up Parental Controls on Your Mac

By Tom Hulse

Parental Controls - Mail and iChat



You can limit who the managed account can interact with in Mail and iChat

Parental Controls gives you the ability to limit the use of Apple's Mail and iChat applications to a list of known, approved contacts.

Set Up Mail and iChat Contact Lists

1. **Limit Mail.** Place a check mark to prevent the managed user from sending mail to or receiving mail from anyone who isn't on the approved list.
2. **Limit iChat.** Place a check mark to prevent the managed user from exchanging messages with any iChat user who isn't on the approved list.
3. If you placed a check mark next to either of the above items, the approved contact list will be highlighted. Use the plus (+) button to add an individual to the approved list, or the minus (-) button to remove an individual from the list.

4. To add an entry to the approved list:

1. Click the plus (+) button.
2. Enter the first and last name of the individual.
3. Enter the email address and/or iChat name of the individual.
4. Use the dropdown menu to select the type of address you're entering (Email, AIM, or Jabber).
5. If an individual has multiple accounts that you want to add to the list, click the plus (+) button at the end of the Allowed Accounts field to enter additional accounts.
6. If you would like to include the individual in your personal Address Book, place a check mark next to 'Add person to my Address Book.'
7. Click the 'Add' button.
8. Repeat for each additional individual you wish to add.
5. If you would like to receive a permission request each time the managed user wants to exchange messages with someone who isn't on the list, place a check mark next to 'Send permission requests to' and enter your email address.

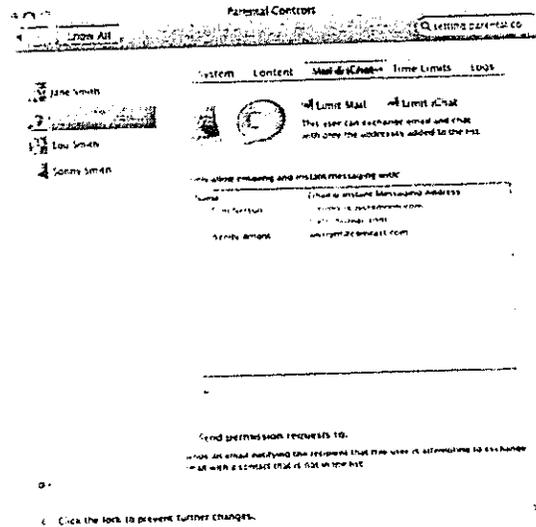
This About.com page has been optimized for print. To view this page in its original form, please visit: http://macs.about.com/od/switchersnewusers/ss/parentalcontrol_4.htm & print
 ©2014 About.com, Inc. All rights reserved.

About.com Macs

Set Up Parental Controls on Your Mac

By Tom Nelson

Parental Controls - Mail and iChat



You can limit who the managed account can interact with in Mail and iChat

Parental Controls gives you the ability to limit the use of Apple's Mail and iChat applications to a list of known, approved contacts.

Set Up Mail and iChat Contact Lists

1. **Limit Mail.** Place a check mark to prevent the managed user from sending mail to or receiving mail from anyone who isn't on the approved list.
2. **Limit iChat.** Place a check mark to prevent the managed user from exchanging messages with any iChat user who isn't on the approved list.
3. If you placed a check mark next to either of the above items, the approved contact list will be highlighted. Use the plus (+) button to add an individual to the approved list, or the minus (-) button to remove an individual from the list.
4. **To add an entry to the approved list:**
 1. Click the plus (+) button.
 2. Enter the first and last name of the individual.
 3. Enter the email address and/or iChat name of the individual.
 4. Use the dropdown menu to select the type of address you're entering (Email, AIM, or Jabber).
 5. If an individual has multiple accounts that you want to add to the list, click the plus (+) button at the end of the Allowed Accounts field to enter additional accounts.
 6. If you would like to include the individual in your personal Address Book, place a check mark next to 'Add person to my Address Book.'
 7. Click the 'Add' button.
 8. Repeat for each additional individual you wish to add.
5. If you would like to receive a permission request each time the managed user wants to exchange messages with someone who isn't on the list, place a check mark next to 'Send permission requests to' and enter your email address.

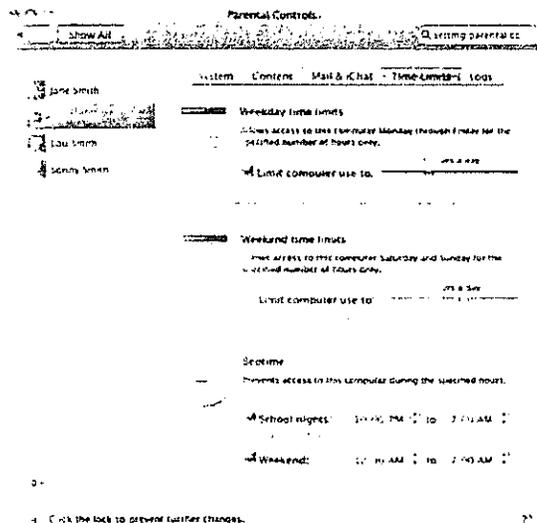
This About.com page has been optimized for print. To view this page in its original form, please visit: http://macs.about.com/od/switchersnewusers/ss/parentalcontrol_4.htm
 ©2014 About.com, Inc. All rights reserved.

About.com Macs

Set Up Parental Controls on Your Mac

By Toni Nelson

Parental Controls - Time Limits



Limiting the time spent on the Mac is just a checkmark away.

You can use the Mac's Parental Controls feature to control when your Mac will be available for use by anyone who has a managed user account, as well as how long they may use it.

Set Up Weekday Time Limits

In the Weekday Time Limits section:

1. Place a check mark in the 'Limit computer use to' box.
2. Use the slider to set a time limit from 30 minutes to 8 hours of use in a single day.

Set Up Weekend Time Limits

In the Weekend Time Limits section:

1. Place a check mark in the 'Limit computer use to' box.
2. Use the slider to set a time limit from 30 minutes to 8 hours of use in a single day.

Prevent Computer Use on School Nights

You can prevent the computer from being used by a managed user during specified time periods on school nights.

1. To control weekday use, place a check mark next to the 'School nights' box.
2. Click the hours or minutes in the first time field, and either type in a time or use the up/down arrow to set the beginning of the time when the computer may not be used.
3. Repeat the above step for the second time field to set the end of the time when the computer may not be used.

Prevent Computer Use During Weekends

You can prevent the computer from being used by a managed user during specified time periods on the weekend.

1. To control weekend use, place a check mark next to the 'Weekend' box.

2. Click the hours or minutes in the first time field, and either type in a time or use the up/down arrow to set the beginning of the time when the computer may not be used.
3. Repeat the above step for the second time field to set the end of the time when the computer may not be used.

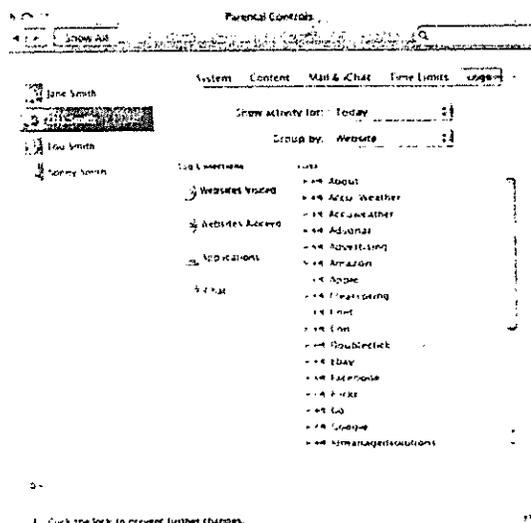
*This About.com page has been optimized for print. To view this page in its original form, please visit: http://macs.about.com/od/switchersnewusers/ss/parentalcontrol_5.htm
©2014 About.com, Inc. All rights reserved.*

About.com Macs

Set Up Parental Controls on Your Mac

By Tom Nelson

Parental Controls - Logs



With Parental Control logs, you can keep track of websites visited, applications used, and iChat contacts

The Mac's Parental Controls feature maintains an activity log that can help you keep track of how a managed user is using the computer. You can see which web sites were visited, which web sites were blocked, and which applications were used, as well as view any instant messages that were exchanged.

View Parental Controls Logs

1. Click the 'Logs' tab.
2. Use the 'Show activity for' dropdown menu to select a time frame to view. The choices are today, one week, one month, three months, six months, one year, or all.
3. Use the 'Group by' dropdown menu to determine how the log entries will be displayed. You can view entries by application or by date.
4. In the Log Collections pane, select the type of log you wish to view: Websites Visited, Websites Blocked, Applications, or iChat. The selected log will display in the Logs pane on the right.

*This About.com page has been optimized for print. To view this page in its original form, please visit: http://macs.about.com/od/switchersnewusers/ss/parentalcontrol_6.htm
 ©2014 About.com, Inc. All rights reserved.*

About.com Macs

Set Up Parental Controls on Your Mac

By Tom Irelson

Parental Controls - Wrap Up

The Parental Controls feature is fairly easy to set up, but it's up to you to manage its parameters. If you're using Parental Controls to filter web sites, don't assume that Apple knows what's best for your family. You need to diligently monitor the sites your family is visiting by reviewing the Parental Controls logs. You can then customize the web site filter to add sites that should have been blocked, or to remove sites that are acceptable for a family member to visit.

The same holds true for the Mail and iChat access lists. Kids have an ever-changing circle of friends, so the contact lists must be updated in order for the filtering to be effective. The 'send permission request' option can help strike a balance between giving kids a little freedom and keeping on top of their activities.

This About.com page has been optimized for print. To view this page in its original form, please visit: http://www.about.com/od/switchersnewusers/ss/parentalcontrol_7.htm
©2014 About.com, Inc. All rights reserved.

MEET WINDOWS DOWNLOAD & SHOP HOW-TO SUPPORT

Sign in

Installation Search & touch Personalization Security & accounts Apps & Windows Store Web & networks Email & communication Music & photos

Set up Parental Controls

Windows 7 ▾

If your computer is connected to a domain, Parental Controls aren't available.

You can use Parental Controls to help manage how your children use the computer. For example, you can set limits on the hours that your children can use the computer, the games they can play, and the programs they can run.

To watch a video, see [Video: Using Parental Controls](#).

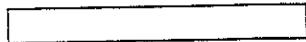
When Parental Controls blocks access to a game or program, a notification is displayed that the program has been blocked. Your child can click a link in the notification to request permission for access to that game or program. You can allow access by entering your account information.

To set up Parental Controls for your child, you'll need your own administrator user account. Before you get started, make sure each child that you want to set up Parental Controls for has a standard user account. Parental Controls can be applied only to standard user accounts. For more information about user accounts and setting them up, see [What is a user account?](#)

In addition to the controls that Windows provides, you can install additional controls, such as web filtering and activity reporting, from a separate service provider. For more information, see [How can I add additional parental controls?](#)

To turn on Parental Controls for a standard user account

1. Open Parental Controls by clicking the **Start** button , clicking **Control Panel**, and then, under **User Accounts and Family Safety**, clicking **Set up parental controls for any user**.  If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
2. Click the standard user account that you want to set Parental Controls for. If the standard user account isn't set up yet, click **Create a new user account** to set up a new account.
3. Under **Parental Controls**, click **On, enforce current settings**.
4. Once you've turned on Parental Controls for your child's standard user account, you can adjust the following individual settings that you want to control:
 - **Time limits.** You can set time limits to control when children are allowed to log on to the computer. Time limits prevent children from logging on during the specified hours. You can set different logon hours for every day of the week. If they're logged on when their allotted time ends, they'll be automatically logged off. For more information, see [Control when children can use the computer](#).
 - **Games.** You can control access to games, choose an age-rating level, choose the types of content you want to block, and decide whether you want to allow or block unrated or specific games. For more information, see [Choose which games children can play](#).
 - **Allow or block specific programs.** You can prevent children from running programs that you don't want them to run. For more information, see [Prevent children from using specific programs](#).



MEET WINDOWS DOWNLOAD & SHOP HOW-TO SUPPORT

Sign in

Installation Search & touch Personalization Security & accounts Apps & Windows store Web & networks Email & communication Music & photos

Looking for web filtering and activity reports in Windows Parental Controls?

Applies to these editions of Windows 7

In this page

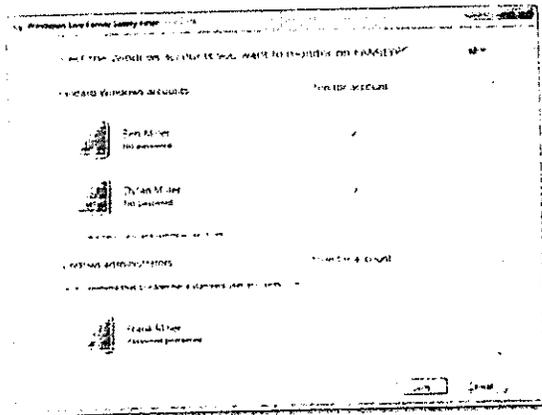
Family Safety Filter

Windows Live Family Safety website

You might have noticed that in Windows 7, web restrictions and activity reports aren't included in Parental Controls. You can still restrict the sites your kids can visit and see reports of their online activity by adding a service provider in Windows Parental Controls, such as Windows Live Family Safety. With Family Safety, you can set up web filtering and activity monitoring for your kids.

Family Safety Filter

The Family Safety Filter monitors your child's computer activity and filters the content they can see on the web. It needs to be installed and set up on each computer your children use. To see if you already have the Family Safety Filter installed on your computer, click the **Start** button, type **Windows Live Family Safety** in the search box, and see if it appears in the results. If not, you can download and install Windows Live Family Safety—a part of Windows Essentials—for free.



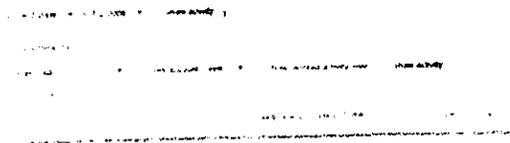
In the Family Safety Filter, you choose which Windows accounts you want to monitor

[Top of page](#)

Windows Live Family Safety website

Once you've installed the Family Safety Filter, you can use the Family Safety website to do the following, and more:

- **Get detailed activity reports.** See what websites each of your kids visited (or tried to visit), what programs they used, and how much time they spent on the computer.



See what websites your kids visited, or tried to visit.

- **Choose your children's web filtering level.** When you first set up the Family Safety Filter, your child's web filtering level is automatically set to basic. You can change it to strict or custom, and block or allow specific webpages or websites.

This page is blocked

http://www.usa.com/

Ask your parent for permission to view this page



✉ mail your request



👤 ask in person

✉ add a note to your e-mail request

Instead of a website with inappropriate content, your child will see this webpage where they can ask permission to see the website.

[Top of page](#)

For more information about Family Safety and all of the programs in Windows Essentials, go to the Windows Essentials website. Or visit the Parental Controls feature page to learn more about Windows 7 Parental Controls.

Hello from Seattle. United States of America

[Disclaimers](#)

[Terms of Use](#)

[Trademarks](#)

[Privacy & Cookies](#)

[Site Map](#)

© 2014 Microsoft

About.com Internet / Network Security

How to Setup Parental Controls on an iPad, iPod Touch, or iPhone.

By Andy O'Donnell

Just about every kid on the planet seems to have an iPod Touch, iPad, or iPhone. If they don't have one, chances are that they are borrowing yours and getting their greasy little paw prints all over its screen.

As parents, we usually consider these devices nothing more than game systems or music players. We grew up in an era when a CD player was just a CD player. We don't often contemplate the fact that these little glossy iGadgets are basically the digital equivalent of a Swiss Army knife. They have a full fledged internet browser, video player, Wi-Fi connection, camera, and an app for almost anything you could imagine. Oh yeah, and they play music too (like MTV used to).

What's a parent to do? How do we prevent little Johnny from purchasing every app in the app store on our credit card, visiting raunchy websites, and renting bad/scary/tasteless movies?

Luckily, Apple had the foresight to add a fairly robust set of parental controls to the iPod Touch, iPad, and iPhone.

Here's the quick and dirty on how to setup parental controls on your child's iPhone, iPod Touch, or iPad. Kids are pretty smart and may figure out a way around many of these settings, but at least you did your best to try and thwart the little schemers.

1. Enable Restrictions

All of the parental controls rely on you to enable restrictions and enter a PIN number that you keep secret.

To enable restrictions, touch the settings icon on your iOS device, choose "General", and then touch "Restrictions".

On the "Restrictions" page, choose "Enable Restrictions". You will now be prompted to set a PIN number that you will need to remember and keep from your kids. This PIN number will be used for any future changes you want to make to the restrictions that you have set.

2. Consider Disabling Safari and Other Apps.

Under the "Allow" section of the restrictions page, you can choose whether you want your child to be able to access certain apps such as Safari (web browser), Youtube, FaceTime (video chat), and several other of Apple's built-in apps. If you don't want your child to have access to these apps, set the switches to the "OFF" positions. You can also disable the location reporting feature to prevent your child from publishing their current location in apps like Facebook.

3. Set Content Limits

Much like the V-Chip feature in most modern TVs, Apple allows you to set limits on what type of content you want your child to have access to. You can set the permitted viewable movie ratings by placing a check next to the highest rating level you want them to see (i.e. G, PG, PG-13, R, or NC-17). You can also set levels for TV content (TV-Y, TV-PG, TV-14, etc) and the same goes for apps and music.

To change the permitted content levels, select "Music & Podcasts", "Movies", "TV Shows", or "Apps" in the "Allowed Content" section and choose the levels you wish to allow.

4. Disable "Installing Apps"

While some of us love fart machine apps, they are not for everyone. No one wants to be sitting in an important meeting and have the "scheduled fart" go off that Little Johnny setup when he installed the Super Ultra Fart Machine app on their iPhone the night before. You can prevent this by setting the "Installing Apps" feature to the "OFF" position. You can still install apps, you'll just need to enter your PIN number before doing so.

5. Disable In-app Purchases

Many apps allow in-app purchases where virtual goods can be bought with real-world money. Little Johnny may or may not realize that he's actually causing your bank account to be charged for the "Mighty Eagle" he just bought while in the Angry Birds App. If you disable in-app purchasing you can at least breathe a sigh of relief that your child won't go on a bird buying shopping spree on your dime.

As I've said before, Kids are very tech savvy and will probably find a way to get around these restrictions. The fact that the restriction PIN is only 4 digits long doesn't help either. It's only a matter of time before they guess the right one, but at least you've done your best to try and keep them safe. Maybe they'll thank you one day when they have kids of their own.

This About.com page has been optimized for print. To view this page in its original form, please visit: <http://networksecurity.about.com/od/frequentlyaskedquestions/a/How-To-Setup-Parental-Controls-on-an-iPad-iPod-Touch-or-iPhone/>
©2014 About.com, Inc. All rights reserved.

