MAC PARENTAL CONTROLS

JEFF GRABER

The Mac Support Store

Mac Parental Controls

By Jeff Graber

Copyright © 2015 The Mac Support Store

All rights reserved.

FORWARD

Let's face it: if you have a Mac, your kid is going to want to use it. And in some households the children are more tech-savvy than the adults.

But that doesn't mean you give them free reign on your Mac. There are all kinds of dangers lurking online for youngsters. How do you make sure your child is using the Internet appropriately? How do you set up parental controls?

Jeff Graber answers these questions — and many more — in "Mac Parental Controls." It's a must-read for anyone who has both a computer and kids in the house.

I've known Jeff for years. He's a true expert on all things Apple and knows the Mac inside and out.

No wonder. Jeff has penned how-to articles and opinion pieces for my online publications and others for over fifteen years. His expertise is evident in "Mac Parental Controls" not for just it's area of expertise, but it's also written in a style that any non-techie parent can understand and use immediately.

Even if your kid is the computer whiz in your house.

Dennis Sellers

Editor/Publisher

appledailyreport.com

Contents

Introduction 7
The Reasons Your Child Should Be on Your Mac 8
Online Dangers 10
1. Pornography 10
2. Sexting 10
3. Cyber Bullying 11
4. Predators 11
5. Gaming 12
6. Social Networks 12
7. YouTube 12
8. Identity Theft 12
9. Piracy and Intellectual Property Theft 13
10. Gambling 13
11. Hacking 13
Think Your Child is Using the Internet Appropriately? 15
Benefits to Monitoring Your Child's Online Activities 16
To Spy or Not to Spy 17
Mac Parental Controls - Defined 18
How to Set Up Parental Controls 20
How to set up Parental Controls on Your Mac 20
How to Add Your Child's Managed Account: 21
Launching Parental Controls 22
Options under the Apps Tab 24
Use Simple Finder 24
Limit Applications 25
Allow App Store Apps 25
Allow Joining Game Center Multiplayer Games 26
Allow Adding Game Center Friends 26
Disable Use of Dictation 29
Hide Profanity in Dictionary 29

The Limitations of Internet Monitoring Tools 31

Conclusion 32

Introduction

If you're like most parents, you want to allow your children the freedom to learn how to use your Mac at home, but you also worry about the dangers of the internet. You hear the stories on the news about predators, cyber bullying, and other issues that kids can be exposed to while they are using a Mac, browsing the Internet and chatting with friends.

Unsupervised and with a few clicks of a mouse, your child can cause malware and spyware to install itself onto your computer. He or she can inadvertently allow hackers to get your credit card information by browsing to the wrong website and installing malicious software. A child who doesn't know his or her way around a computer could accidentally delete crucial files or your family photos and home videos.

Just like you would supervise your child in their other activities, you should also monitor your child's Mac usage. The smartest thing that a parent can do is to educate themselves on the dangers of the internet and take steps to mitigate the risks to your child in using your Mac at home. There are hundreds of dangers online, some of which you may have never thought you had to protect your child against. As with anything, it is better to be safe than sorry and a Mac user should always err on the side of caution.

The Reasons Your Child Should Be on Your Mac

When you start to look at monitoring software, the question may cross your mind "Does my child really need to use my Mac?" The answer is a resounding "Yes". Studies have shown that children who have used computers on a regular basis tend to test at higher scores than those who do not. They tend to learn more when they are allowed to research topics on the internet at home than their counterparts who are not allowed to use a computer or do not have a computer. Children who are introduced to the computer tend to learn at an earlier age, retain information they learned longer, and have better academics, which leads to higher self-esteem and self-confidence.

Children can use Skype to interact with family members that are in different states or countries. They can have pen pals in another country, which helps them to learn real world things about other cultures and other places. A child can experience animals that are not native to their town and see mountains, oceans, and lakes that they wouldn't have normally been able to see. They can learn a new language or learn dance or photography. The internet is a place of awe and wonder for a child. It can help them develop skills in nearly anything they can imagine.

The internet was initially created for research, government and educational use. At its core, children can still access those sites that are educational and still reap benefits that they normally would not have without access to computers and internet.

Another reason not to deny your children the use of a computer is that technology will continue to advance with or without them. When they graduate from college, a majority of professions will have some computer use involved and they could be passed up for jobs if they don't lack the computer skills required to do the tasks in the job. Computer and technical jobs continue to grow at an alarming rate and many of them have excellent pay and growth opportunity. Many jobs are now going to online application processes and a child needs typing and word processing skills to complete a resume at the very least.

You might be thinking that you will simply let the schools and the teachers educate your children on computers. The truth is that in many cities and rural towns the teachers lack the help to watch a class of 20-30 children playing on the computer, so they may avoid training their class in a readily accessible computer lab. Some teachers lack the computer skills necessary to answer questions of their students, so they may shy away from giving this education to the students. In many places, technology is not yet a requirement in the school curriculum, and if your child's teacher is behind in technology, your child will also be behind in

it without you allowing him or her to use your Mac at home. Additionally, some schools do not have adequate equipment for the students. Their computers and software are often outdated due to budget constraints.

Online Dangers

Along with the benefits, there are also many dangers that your child can fall prey to while they are surfing online. We will discuss some of the dangerous things your child can be exposed to on the computer below. Remember that this list is not all-inclusive.

1. Pornography

As you probably already know, viewing sexually explicit graphics can be very harmful to children. You don't want your child to become overly curious of sexual activities at a very young age. With teen pregnancy and sexually transmitted diseases, it is our responsibility to keep our child innocent for as long as we can. Exposure to sexually explicit materials gives a child a permissive attitude toward sex and sexual activities. This could lead to relationship problems and casual sexual behavior in their teen years. Kids will hear enough about sex and relationships from school and from their peers. It is best not to allow them free reign of the Mac at home to look at things they shouldn't be viewing.

2. Sexting

With the rise in cell phone usage by tweens and teens, there is also a rise in sexting. As a parent, you may not be aware of what sexting is. Sexting, at its basic definition, is the sending and receiving of nude or partly nude photos and videos. Children think that it is fun to trade photos with friends and romantic partners, however, with Facebook and the explosion of social media, your child's photo could be all over the internet in a matter of minutes. Children and teens aren't able to see the overall consequences of this type of behavior. It may seem to be fun and games at the time, but it is exposing a part of your child that others should not see.

Some people think that photographs are not harmful. However, your child putting images of their body online could haunt them for the rest of their lives. If they want a job in politics, or become a famous actor or singer later, people could bring up the images to harm his or her professional reputation. This could stop them from getting the job they want, getting into the college they want, or marrying the partner they want to marry. They shouldn't have to explain nude photos to their marriage partner later in life. You don't want your child's reputation tarnished for the rest of their life.

Additionally, teens and adults can be charged with sex crimes for sending and receiving photographs of nude minor children or children in sexual acts. Sometimes parents are charged

with crimes for allowing this type of behavior with their children. There is a crime called "failure to protect" that a parent can be charged with for not controlling their child's sexual behaviors. This is serious stuff that your child and you should be no part of.

3. Cyber Bullying

Bullying isn't what it was before the internet became so popular. Years ago, bullying might have entailed someone calling you names in the school yard. Bullying today happens on playgrounds and also via social media websites. Ill words or harmful rumors can be exchanged through email and on platforms like Facebook, and quickly spread to tens of thousands of people. Even if your child isn't called names online, someone can hack into his or her social media profile or email and pretend that they are your child, sending harmful things out about other children.

Cyber bullying is extremely harmful to a child's self-esteem. There have been news articles and reports of suicidal deaths associated with cyber bullying. Once a child is targeted, they may suffer in silence, fearful about telling their parents or others about what is happening. Even worse, parents have less recourse than in previous years to control things like cyber bullying. Parents and teachers cannot necessarily easily remove harmful things another student posted online. Even if they can get it removed, chances are good that a large portion of their peers have already seen the information.

Even if your child isn't exposed to cyber bullying themselves, they may be anxious or fearful of cyber bullying because they have seen it happen to their friends.

4. Predators

Just like there are malicious people walking the streets, there are probably even more lurking on the internet. Children are very impressionable and easily swayed, so an adult can log online pretending to be their friend. The adult can ask for the child's address or school and abduct them while they are walking home from school by themselves. Children sometimes feel neglected by their parents because of hurried schedules and job demands, and it is easy for them to think that someone that pays attention to them is a good person. This can set the child up for sexual misconduct towards them or for an abduction to occur after a predator spends some time on the internet talking to them in order to 'groom' them.

5. Gaming

Gaming can be a lot of fun for children, but it also opens up their world to different things that can be harmful. Many games have online chat where your child could meet a predator in a virtual environment who might ask them to meet them somewhere in person to play games. Your child may not realize their game buddy is an adult and has bad intentions. Video games can also contain sexual content, violence and profanity. Even if the game itself is clean of these things, the other children chatting online might start chatting about inappropriate topics that your child shouldn't be reading.

6. Social Networks

Social networks and social media can be extremely harmful to your child in many ways. First, cyber bullying can occur on these sites. Secondly, your child could be projecting a bad image to their peers and to potential employers later. There is a lot of information that happens in your household and at school that shouldn't necessarily be broadcast out all across the internet, but your child might not realize that it is bad to tell things to other people. They see everyone else doing things that may be inappropriate online, so they will think these things are appropriate just because their peers are doing them.

7. YouTube

If your child has a video camera or a phone, he or she can upload inappropriate videos and photos to the internet easily via YouTube. A child can also view inappropriate content on YouTube or other video sites. A lot of videos that they may think are harmless contain violence, nudity, sexual content, inappropriate behavior, and profanity.

8. Identity Theft

Identity theft may not be one of the dangers that you think about when you consider your child's activities online. But if your child comes across a malicious website that seems harmless and doesn't realize that software installed itself onto your computer, a hacker could get your personal banking information from your Mac without you even being none the wiser. An online thief could clean out your bank account or rack up unauthorized charges on your credit card.

Additionally, your child might enter their own name, birthday and address into a form online thinking that they are signing up for something neat, when in reality, they are giving out their personal information to a stranger. Identity theft can harm your credit and your child's credit and you could fight charges on your card or bad entries to the credit reporting bureaus for years without resolution.

9. Piracy and Intellectual Property Theft

Many children tend to think that things which are available online are free for the taking. Their friends tell them about a website where they are able to download videos, movies, music, pictures, art, and games without paying for them. If you haven't told your child about copyright laws and licensing, chances are that they don't know these things can be viewed as stealing. Piracy is a cybercrime and is punishable. While many people practice piracy and intellectual property theft on a daily basis, it doesn't mean that it is appropriate and a person can get arrested and face charges. Educate your child to the consequences of taking and sharing things online that they may not have appropriate rights to. They need to know that just because their friends are doing it doesn't mean it is legal or moral.

Sometimes, websites are put up or being monitored by authority figures in order to crack down on sites and individuals who are distributing copyrighted materials. There are certain times when stings are done and the authorities make an example out of a few individuals who were caught online doing something illegal. You don't want this to be you or your child. Often times, the parent is the one charged with the crime, because the internet and the computer were in their name and they are ultimately responsible for any activities that their children take part in.

10. Gambling

Another thing that may not cross the mind of a parent is gambling. Your child might play games online and not realize that they are gambling. Online gambling is illegal in many places.

11. Hacking

Another thing that your child might be doing on the computer without your knowledge is hacking. A child that is particularly talented in computers may hack as entertainment to himself and his friends, however, hacking into computers of others or of companies, or writing

malicious code intended to breach other computers is also illegal and can get you or your child into a lot of legal hot water if discovered.

Think Your Child is Using the Internet Appropriately?

Think again!

Recent studies have shown that upwards of 70% of tweens and teens hide at least some of their online activities from their parents. You may think that you are in the know about everything that your child is doing on your Mac when you aren't in their vicinity, but chances are good that they are engaging in behavior that you may not even know existed.

Surveys also found that teens admitted to doing things to hide their activities from parents, including deleting the history in their browsers. They also admit to hiding or closing sites when their parents stopped to talk to them at the computer.

Benefits to Monitoring Your Child's Online Activities

As you can see, your child's reputation and their self-esteem can be harmed by using sites that they think are appropriate. They can be bullied online or 'groomed' by sexual predators while you are completely unaware. They can become victims of identity theft. They can learn inappropriate behavior and act very inappropriate online if you aren't paying attention to what they are doing and monitoring their activities.

As parents, it is our responsibility to pay attention to their activities and protect them from dangers that they don't think about. In addition to protecting your children from inappropriate content, you can protect them against malicious predators. You can also make efforts to protect them against cyber bullies or against becoming a bully themselves.

You can protect them against doing things online that will get them in trouble with the law and might ruin their future. Neglecting the necessity for protecting your children's online activities can cause irreversible damage to their futures.

To Spy or Not to Spy

You may think that spying on your children's activities is invasion of their privacy. But with your children baring everything they know and love online to their friends without a filter, you are endangering them more than you even know by not spying on your children. You can be charged with crimes as an adult for not protecting your children against underage pregnancy, sexting, abduction, and cyber bullying other children. You don't think that your children will become victims or perpetrators of malicious activity online, but most parents think that same way of their own children.

But do you have to 'spy' on them long term? It depends upon your relationship with your child and how mature they are. Some children are more trustworthy than others. They are responsible. They do their schoolwork on time. They talk to you about everything. But you should still monitor them for a period of time so that you can educate each other on what types of things your child thinks can be harmful to them and what types of things actually are.

For example, your child may think someone messaging them online isn't harmful, but that someone could be an adult pretending they are 12 years old. A child's mind wouldn't go there, as we have taught them to be respectful to others. The best thing that you can do while you are monitoring your children's activities is to sit down and share the information with them and discuss what types of problems can be caused by any activity that you want them to discontinue. This will help your child to build problem solving and safety skills of their own so that eventually they will know how to make good choices while they are online.

One important thing that you want to do is to share with your child that you are monitoring them initially. Actively spying on your children can cause a breach in the trust between your children and you. You don't want to do it in a disrespectful way to your child, but you want to be mature and discuss it with them. Tell them that you are monitoring and you will both learn together what is harmful and what is not so that they can make better choices with more experience online. Talk about the dangers that are online with your children in an age appropriate manner, so that they are aware of them without being too fearful.

Mac Parental Controls - Defined

The Mac's Parental Controls feature gives you the ability to control what your children see on the Mac. It lets you choose how the applications on the Mac behave, which websites your child is allowed to see, which programs your child is allowed to run and what files your child can access.

Parental controls also allow you to block or allow incoming or outgoing email, so that you can ensure that your child is not getting email that is inappropriate from other online users. You can stop your child from using iChat or block certain pals that they are not allowed to talk to on iChat.

If your household has a timeframe in which the child is allowed to use the computer and you want the computer to stop allowing the use at specified times, then you can use Parental controls to set the times per day when access is allowed and deny access during the other times. Maybe your child's Mac is in their room and you don't want them to stay up all night playing on the Mac, playing computer games or chatting with their friends. You can set the access to shut off at bedtime. If your child wants to jump on the Mac in the morning instead of getting ready for school, blocking use during those morning hours is critical to getting him or her out of bed and off to school on time.

Some parents like to be in control of how many hours their child is allowed to use the Mac throughout the day, especially on summer vacation. You would like them to get outside and play instead of being cooped up inside all day on the Mac doing things that might not be productive or enable them to learn. Maybe they are limited to 2 hours per day on their electronic gadgets. You can not only set the timeframes they are allowed to be on the Mac, but you can also set the number of hours per day that they are allowed to be on it.

If you are worried that your child will be using the Mac for things other than what you have knowingly allowed or blocked, you can review the logs of their usage to best determine where they are spending their time when they are logged on. This will give you a better idea of where to start with blocking and allowing certain things and can help you monitor their usage for anything inappropriate. This gives you the ability to talk with your child also about what is appropriate and what is not appropriate as the two of you discover and adjust the settings on the Mac. When a child gets older, you may want to open up the settings on the Mac and show them a little bit of trust, while still keeping an eye on their behaviors so that they don't tread into dangerous waters while they are online.

Mac Parental Controls aren't just for the children in your household. You can use them to lock down Mac use for anyone who visits your household or stays at your house whom you don't want to get into your personal files. If a babysitter is watching your children and you want her to have access to minimal things on the Mac to play movies for your children, for example, you can give her an account that is locked down so that she cannot view your personal files. You can set up an account for grandma. Or maybe you don't want your guests having the ability to browse illegal websites or download torrent movies. Whatever the reason, Parental Controls is a great tool to help you limit access to anyone. Employers lock access down to their employees so that they won't use inappropriate websites during work hours, so don't feel bad for using computer security for what it was intended or for worrying that someone might use your computer for malicious activity. It's better to be safe than sorry.

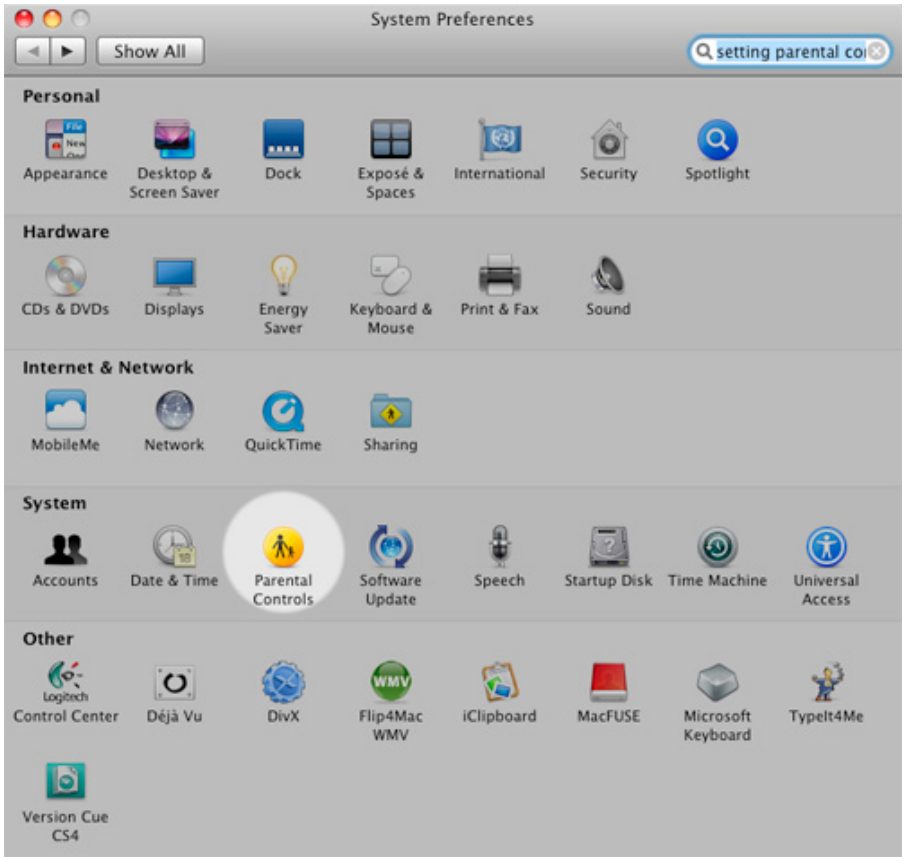
How to Set Up Parental Controls

How to set up Parental Controls on Your Mac

- 10.10.x Yosemite is the newest version of Mac. These instructions will cover how to set up Parental Controls on 10.10.x. There are documents available on www.macs.about.com that will show you how to set up Parental Controls on older versions of Mac.

- In order to set up Parental Controls, you will need an administrator account and the appropriate administrator password to gain access to make the appropriate changes. In order to use Parental controls on your Mac, you will need to set up one or more managed user accounts using the instructions below before you can set up the Parental Controls for your child's account. A folder will also be created for the account.

Note: If your child already has a managed account with parental controls enabled, you can skip this portion of the instructions.



How to Add Your Child's Managed Account:

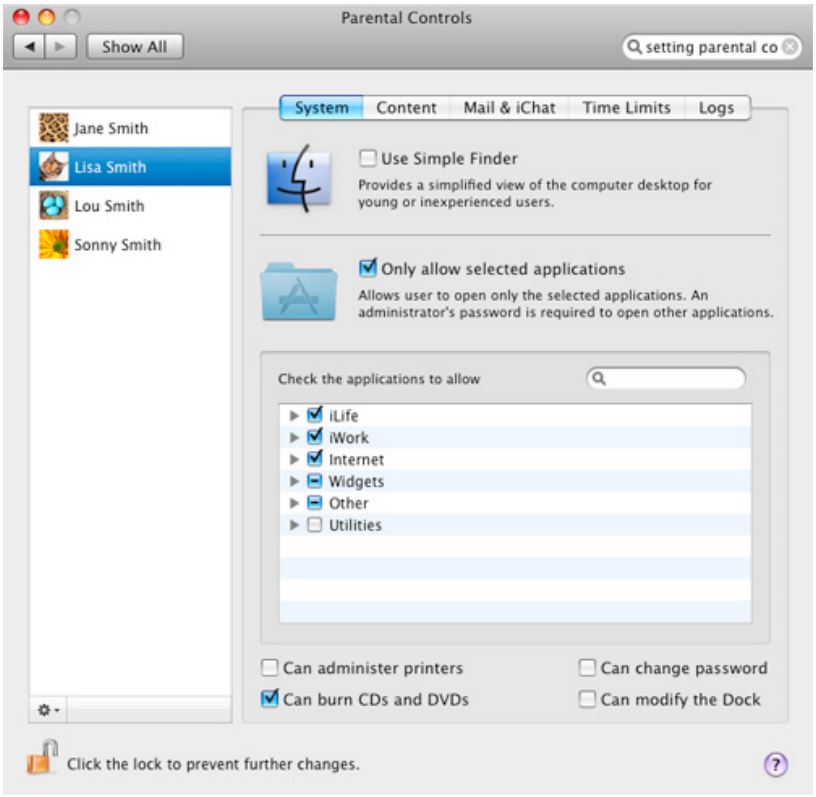
1. Click the Apple icon in the top left of your screen.
2. Click Users & Groups.
3. Click the Lock icon in the lower left corner of the Users & Groups screen.
4. Enter in your administrator username and password.
5. Click Unlock.
6. Click the + button in the lower left corner of the Users & Groups screen.
7. In the New Account box, click the dropdown to select Managed with Parental Controls.
8. Enter your child's Full Name in the Full Name: box.
9. Enter a nickname for your child's account into the Account Name box. This should be lowercase with no special characters.
10. Click the Use Separate Password radio button.
11. If you need assistance to choose a password, click the key icon. Inside the Password Assistant box, you can select a type of password that you want the Mac to auto-generate, and you can use the slider to modify the suggested password length. Password type can be: Manual, Memorable, Letters and Numbers, Numbers Only, Random, or FIPS-181 compliant.

12. If you have chosen a Manual password, you may key in the password of your own choosing. Make it something easy for your child to remember, but strong enough to prevent unauthorized use to the Mac.
13. Rekey the password again in the password Verify box.
14. Enter a Hint if you choose. This can help to jog your child's memory if he or she forgets his password.
15. Click Create User to complete the new account.
16. A prompt may come up asking you to continue or discontinue automated login. You can choose whichever way fits your family's usage.
17. Click the Red X to close the Users & Groups window.

Launching Parental Controls

1. Click the Apple icon in the top left of your screen.
2. Click System Preferences to open it.
3. Click the 'Parental Controls' icon that displays in the System area.
4. Click the lock icon. It is located in the bottom left-hand corner of the parental controls screen.

5. Enter in your administrator user name and password to authenticate yourself to make changes.
6. Click ‘OK’.



1. **How to Configure Parental Controls:** Once you are in the Parental Controls screen and have unlocked the ability to make changes in this screen, click on the managed account that you created for your child.
2. Click on the tab you want to modify. We will click the Apps tab first.

Options under the Apps Tab

Use Simple Finder

Simple Finder is an interface that is easier for children to use. It allows them to use the Mac without the ability to inadvertently delete important files or harm the settings to the applications that you have installed on the Mac. Simple Finder gives the child 3 folders: Documents (to save their files), Shared (where you can both share files between your accounts), and Applications (these are the applications that you designate they can use). This option is especially good to set up for younger children who don't know their way around a Mac well.

Limit Applications

Limit applications allows you to choose what applications your child will be able to use. You can search the applications to allow in the search box, then click the checkbox to mark them if you would like your child to use these. Uncheck any applications that you do not wish your child to have access to.

Allow App Store Apps

Once the Limit Applications is checked, you can use the Allow App Store Apps dropdown box to choose which age range can be allowed. For example, if you are okay with your child viewing ages 13+ apps in the App store, you could choose the option 'up to 17+'.

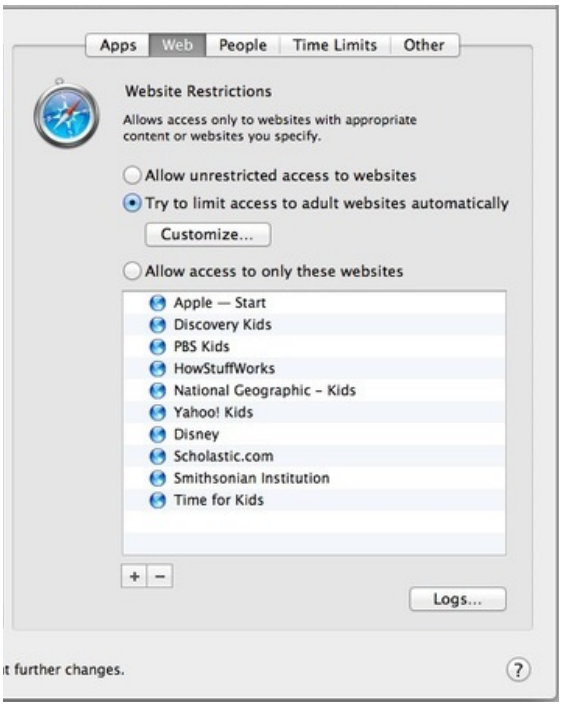
If you want to ensure that your children are only able to visit appropriate websites while they are browsing online, you will want to make some changes to the tab called Web.

Choose one of the following:

Allow Unrestricted Access to Websites – This lets your child have access to anything on the web, including pornographic websites or other inappropriate sites. If you trust your child not to browse these sites and get themselves into trouble, you can opt for this choice.

Try to Limit Access to Adult Websites Automatically – This is a good choice, as it allows Apple to filter out content that is too mature for young viewing eyes. If you still have a few more websites that you want exclusively banned, you can add them also under this option by clicking Customize to include or exclude specific websites.

Allow Access to Only These Websites. This option shows a list which includes kid-friendly websites. The sites included here are: Discovery Kids, Scholastic.com, PBS Kids, and Smithsonian Institution. If you have more sites in mind that you would be okay with your kids visiting, you can click the Plus (+) button to add them.



If you want to keep track of the other people that your child communicates with while they are on the Mac, you can turn to Parental Controls' People tab. You can limit Mail, Messages and Game Center interactions under this tab. The choices are:

Allow Joining Game Center Multiplayer Games

You will want to restrict this if you are worried about your child meeting predators online. Sometimes it is wise to allow them to only play with certain friends, and you can control this with these settings.

Allow Adding Game Center Friends

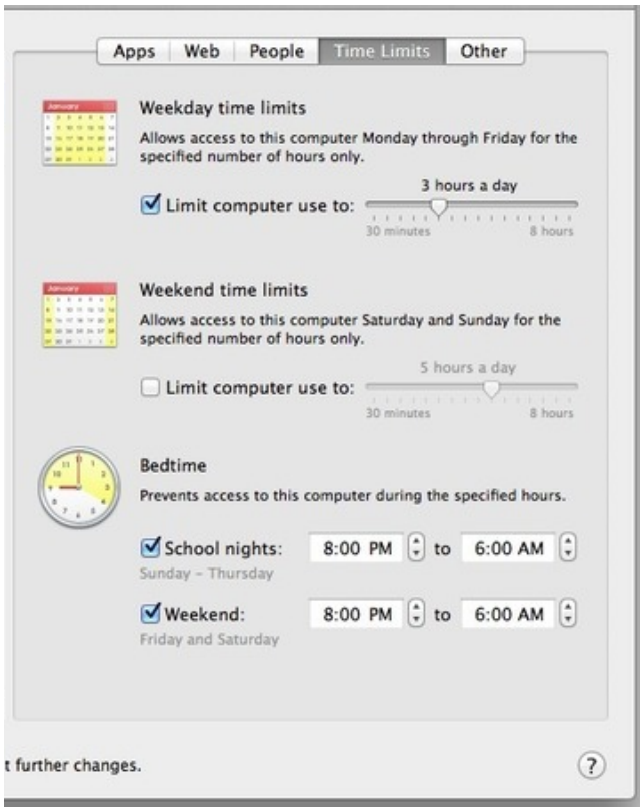
If you want your child to be able to control his or her own Game Center friends, you may be comfortable checking this setting and not restricting their gaming friends.

Click the Plus (+) to add different chat names and addresses that you allow for Mail and Messages. You can auto fill addresses from your contacts or create new ones.

Limit Mail lets you set the Mail so that children can request permission to contact your child and the request is emailed to you for approval. Enter your email address as the administrator. There will be a link emailed to you that you can click in order to allow the new request and the new user to contact your child.

The time limits tab allows you to set time limits from 30 minutes to 8 hours, so that your child is restricted to the amount of time they are allowed to stay on the computer. 15 minutes before time is up, it will warn the child that their time is almost done on the computer so that they have the opportunity for you to enter in your password again and extend the time if you wish. This 15 minute warning also gives them time to close their files and log out of whatever they are doing.

Many parents think that their children are only online a couple hours out of the day. The rest of the family may be busy doing house or yard work, or maybe are not at home for a portion of the day, so they do not realize their teen or tween is on the internet too long. It is best to set time limits so that you can be sure your child gets enough time for their school work, and has the ability to get outside and get fresh air. Often, when we are on the computer, we lose track of time and we do not realize how long we have actually wasted online. This holds true also for your children, so it is best to get a handle on it from the get go.



If you need to set Bedtime limits so that your child has to log off before a set time at night and cannot log back on throughout the night to play or chat, you will want to set the times in the Bedtime limits area. Some parents extend the hours on the weekends to later in the evening because their children are allowed to stay up later on the nights that they have no school.

Staying up too late on the computer can cause your child to be irritable and to suffer when they have school work and tests due. You might see that their grades are suffering because they are staying up and on the computer after you go to sleep, so setting times where they are not allowed to be on the computer is good for their mental health and their academics.

Under the Other tab, you will find the following:

Disable Use of Dictation

Hide Profanity in Dictionary

This setting is a great idea if you don't want your child to use profanity online or in their emails and chats.

Limit Printer Administration

It is always a smart idea to block printer administration from your children. You may want to limit usage so that your children don't print things that are inappropriate, don't use all of your printer's toner or ink, or don't use all of your paper.

Limit CD and DVD Burning

Children can use CD and DVD burning to burn photos, videos and other documents for sharing with their friends. Always ensure that your children are not sharing nude photos or anything else that can be illegal or viewed as inappropriate.

Another thing that you must worry about with allowing CD and DVD burning is piracy. If your child is downloading copyrighted or licensed movies, music, games, photography or artwork and distributing it to his or her friends using CDs or DVDs, he may get into some legal hot water. Teach children that the artists that create these things need to make money, too. Maybe it is a good time to teach them about earning money and chores, and they can work towards a movie, game or music that they want instead of obtaining it illegally online through torrent sites.

Disable Changing the Password

You don't want your child to have the ability to change passwords or change the settings by themselves in Parental controls, or they will be able to allow themselves the ability to get into all of the things that we discussed earlier in this ebook.

These options are self-explanatory and can be allowed and limited at your discretion.

Logs is where you would go if you wanted to check to see which sites your child is viewing, which sites were blocked by your Mac, applications that they launched and messages that were sent and received.

The following options are available under logs:

- Websites Visited
- Websites Blocked
- Applications
- Messages

The Limitations of Internet Monitoring Tools

Unfortunately for parents, monitoring your child's internet usage isn't as easy as using something like Net Nanny or Mac Parental Controls. There are loopholes that kids can use in order to get around such monitoring software and still open up your Mac or PC to identify theft and malicious software, such as spyware, malware and viruses.

Proxy websites are an easy way for kids to go around the internet monitoring software. Kids can also use Peer-to-Peer to share movies, music and files. Some predators use these peer to peer connections to your child in order to put pornographic or malicious material on your computers, or they can be used to get credit card information from your Mac without your knowledge. Most web filters also allow children access to blogs and cannot filter the bad material that is on them in real-time.

You may be monitoring your child's Facebook page, when in reality your child can create 2 Facebook accounts; 1 secret one where they post whatever they want, and 1 Facebook account where they keep contact with family members and they keep things clean.

If your child is especially talented on the Mac, they can look up YouTube videos in order to circumvent the monitoring tools that you have installed on it. Be aware of your child's computer skills. It may be beneficial to consult a computer expert if your child is able to get around the tools you are using to keep them safe. If they know about IP addresses, they can also access a website by the IP address instead of the URL, as some filtering and blocking software only blocks by web URLs.

Conclusion

Parental Controls are essential to help you control, limit and ensure your children's safe browsing activities while using your Mac. Not only will your files be secure, your children will also be protected from strangers and unwanted sites. While you don't need to go 'CIA' on your kids and their computer time, you do need to help them to learn what is appropriate and what is inappropriate behavior online so that they don't get themselves in hot water unintentionally. A little effort and teaching now will save a lot of headaches and problems for you and your child later.