98 Internet Safety Tips For Your Youth Ministry

http://www.ChristianTeenWorld.com

Thanks for reading!!! ...

Also, Make sure you check out our main page for more materials to use with your Youth Ministry : http://www.christianteenworld.com

1. Set Rules.

Determine what your child needs to use the computer for. This could be school-related or just for entertainment. Make sure your child knows what he or she is and is not allowed to do on the computer. Boundaries can be set based on a child's age and maturity level, and can include site restrictions, program use, and activities. Establish consequences for breaking the rules.

2. Make a Pact.

Create a family contract regarding Internet use. This document can contain house rules about on-line conduct. Basic templates can be found on-line, and you can modify the document to include your children's input when preparing a final draft. You may also want to include facts and statistics about on-line safety to remind children of the dangers. Have children read and sign the contract, and post it near the computer area for easy reference.

3. Take the Quiz.

Many Internet safety websites offer on-line multiple choice quizzes that children can take to test their knowledge about being safe on-line. After discussing Internet safety with your child, suggest they take one of the quizzes to show you what they know.

4.Create a Schedule.

While the Internet can be fun and useful, children should be involved in activities outside of using a computer. One child using the Internet more than others can also result in jealousy and arguments. Make a schedule with fair time limits to allow all family members to have access to the Internet when necessary. Determine time limits based on how much Internet use is necessary for homework and other activities. Outside of homework research, no more than an hour on-line daily could be a good rule of thumb.

5.Computer Area.

Keep the computer in an open, family area instead of in a child's bedroom. This will make it easier to keep an eye on their activities. If there are multiple computers in your home, consider designating one as a family computer and password restricting access to the others.

6.Home Alone.

Until you are confident that rules can be followed, do not let children use the Internet unless a parent is home to monitor activity. Passwords to block access to the computer can be used to enforce this practice.

7.Block Viruses.

Be sure that personal computers and laptops are equipped with virus detection software that scans and updates on a regular basis. A good program will also monitor spyware and alert you of any threats.

8.Block Pop-ups.

Set the Internet browser to block pop-up websites and advertisements. This will allow for cleaner web surfing, as well as minimize the chances of children viewing offensive material.

9.Limit Browser Functionalities.

Modify Internet browser settings so they do not automatically save website information, like user names and passwords. Clear cookies and temporary Internet files on a weekly basis.

10. Protect Wireless Networks.

If wireless Internet access is used, protect the wireless network connection with a password and firewall to keep unwanted users out.

11. Consider Kid-Geared Browsers.

Several companies have created browsers made specifically for younger users. These Internet browsers feature built-in filtering capabilities to protect young eyes from unwanted and explicit material. Browsers like Glubble and Buddy Browser include features to disable external chat and encourage media sharing and social interactions with family and other people the child already knows.

12. Suggest Family-Friendly Websites.

Find educational and wholesome websites for your child to visit, and add them to a bookmark list. Show your child how to access the bookmark menu to view the sites. Good suggestions include the websites for your child's favorite educational television programs, government-sponsored educational websites, and school or community websites.

13. Create Separate User Accounts.

If a home computer is used by all family members, it may be a good idea to give a unique log-on identifier to each user. This can help minimize the risk of important files or folders being accidentally deleted by kids. Parents' user accounts should have full rights to view and change all files saved on the computer, as well the ability to add or delete users.

14. Create Solid Passwords.

Teach children to create passwords that are easy for them to remember but difficult for others to guess. Strong passwords will include numbers and letters, and should not be obvious (like a name and birth date.) Teach children how to enter their password when logging in, and show them how to make sure that the Caps Lock is not engaged if the password is case-sensitive.

15. Change Passwords Regularly.

Get in the habit of changing password for computer access and websites on a regular basis, every 60 days or so. Be sure that all family members update passwords by scheduling a day when everyone makes their changes.

16. Know Your Kids' Passwords.

Keep a list of websites your child uses and the user names and passwords for each. This is useful for monitoring their activity and reminding them of a password when it is forgotten. Make sure they give you're their new password if they change it.

17. Protect Passwords.

Teach children not to share their user names or passwords with friends and strangers. Their passwords should be known only by them and their parents. Have them change their password if it is discovered by someone else.

18. Program Installation.

Don't allow kids to install new programs unless supervised. Knowing what is being installed on the computer and where it came from can prevent risk of virus infection. Adult installation of new programs will also ensure that new programs are installed correctly.

19. Learn from Kids.

Since Internet use is so prevalent in schools, children might know more about the technology than parents do. If you need help understanding how certain sites or programs work, kids are always proud to share their knowledge.

20. Secure Sites.

Teach children to recognize secure sites by looking for the "https" prefix. Many browsers also display a padlock or green address bar when a site is secured. Most browsers will display a warning when a website's security certificate is inconsistent or expired. Teach children to avoid sites when a security warning is displayed.

21. Update.

Keep software and hardware up to date. When latest technologies are used, the computer will run more smoothly and be less susceptible to hackers and viruses.

22. Close Browser Windows Correctly.

Teach children to log off of sites that require a user name and password instead of simply closing the browser window. Officially logging off is secure, and it ensures that private information does not remain viewable to hackers or third-parties.

23. Explain Risks.

Teach children about on-line dangers, like sexual predators and cyberstalkers. Children will have a better appreciation for the family Internet usage rules if they understand that the rules are not created to keep them from having fun, but intended to protect them from harm.

24. Don't Talk to Strangers.

Children are naturally trusting and will talk online with anyone who seems friendly or nice. As in real life, remind children not to talk in a chat room or via e-mail with anyone they do not know. If children are approached by strangers in a chat room, instruct them not to respond and to tell you about the encounter immediately.

25. Don't Take Anyone at Face Value.

Internet predators are known for posing as children in chat rooms to lure real kids into conversations. This tactic often results in children exposing more personal information than they would to an adult stranger. Instruct children to always be cautious about anyone they meet on-line.

26. Know Who to Call.

If a child is being stalked or threatened on-line, contact police with the user's screen name and any other given information.

If a child is bullied on-line by a classmate, contact the bully's parents. If parental control software is not working correctly, contact the manufacturer's technical support department for assistance.

27. In-Person Meetings.
Do not allow children to meet on-line friends in person. This can be difficult for young children to understand, especially if they feel they "know" the person from multiple on-line conversations. If they insist on meeting an on-line friend, accompany your child and meet in a public place.

28. Role Play.
Use role playing to reinforce how children should act when approached on-line by someone they do not know. Practice what to say and not sharing personal information. Teach them to feel comfortable ignoring strangers or exiting chat rooms when approached. Also review how they should handle cyber bullies. This practice will make your kids feel more comfortable if the time comes when they need to deal with the real thing.

29. Too Good to Be True.
Educate children on how to avoid Internet scams, like moneymaking schemes, chain emails, and false charities. Children can be naive to these ploys and often get taken advantage of. If it's too good to be true, it probably isn't.

30. Express Discomfort.
Let children know that they can tell you if anything they saw on-line made them feel uncomfortable. This can include photos or conversations in chat rooms. Do not get angry at

them for seeing something they shouldn't have seen. Instead, thank them for bringing it to your attention.

31.No Secrets.
Tell children to let you know if anyone on-line asked them to engage in a conversation or activity that was to be kept secret. Explain that there is no reason to keep a promise with a stranger, especially when the stranger specifically says not to tell parents.

32.Be Fair.
Don't punish children for their friends' bad on-line behavior. Only enforce consequences for actions that your child actually does. This will help to maintain your child's trust that they can tell you about things that happen to them on-line.

33. Photo Sharing.
Tell children never to send a photo of themselves to anyone they do not know. Explain that when strangers learn more information about a kid's appearance, hometown, age, etc. it can make it easy to find children and hurt them.

34. Photo Safety.
If children post photos to their website or social network page, ensure that the photos do not contain identifiers, like house numbers or car license plate numbers. Although a single photo may not seem harmful, predators can use information form a collection of photos to determine a child's home or school location.

35. Maintain Privacy.
Tell children not to share personal information on-line. This includes their last name, phone number, address, or school

name. If this information is required for registration with a website, kids should check with parents first before supplying the information.

36. Cost Containment.
Don't give children credit card numbers to use for on-line purchases or website registrations. An adult should always supervise any financial transaction on-line to ensure that the website is legitimate and secure.

37. On-line Auctions.
On-line auction sites, like eBay, do not require credit card information to establish an account. Children can sign up and bid on items without realizing that they are entering a contractual obligation to purchase.

38. Smart phones.
If your child has a phone or music player with on-line capabilities, be sure that they understand that the same Internet rules apply, whether on the pc or on a handheld device. If internet access on a smart phone is too much freedom, disable the service or install a parental control application.

39. Apps Add Up.
Require parental approval before children download applications to their Smartphone. Not only could the app's content be inappropriate, but the cost of multiple applications can result in a shocking expense on the monthly phone bill.

40. Consider Parental Controls.
Software is available to block unwanted content from the Internet. These programs generally block pornography and

violence, but can also be customized to block specific websites or website categories. Adults can use a password to access all sites. Keep in mind that kids may be so familiar with the Internet that they can find ways around parental controls. Be sure to pick a strong password that your children won't figure out.

41. Less Obvious Sites.

While parents may immediately think of blocking access to pornography, there are other websites that children should not be exposed to. Don't forget to restrict access to sites depicting dangerous activities, drug use, and hate. Depending on age and maturity level, you may also want to block shopping websites.

42. Be Involved.

Know what websites your child visits and be involved in his or her on-line activities. Ask your child to show you his or her favorite sites and explain why he or she likes them. Spend time together looking at websites on the Internet and finding new appropriate sites to visit.

43. Learn Chat Room Abbreviations.

The abbreviations kids use when chatting can seem like a foreign language to parents. Get to know the acronyms used in chat rooms and instant messaging so you can tell just what they are talking about. Research on-line can help you decipher the meanings of many abbreviations, or you can ask your child to teach you what those letters mean.

44. Type Carefully.

Make sure that children use care when typing a url into the browser's address bar. Some predatory websites purposely choose close spelling variations of legitimate websites just to expose children to explicit material. Children should also mind the various extensions; completing a url with .net instead of .com will lead to a completely different website than the one intended.

45. Have a Purpose.

Do not allow random web surfing. This often leads to children visiting inappropriate sites that were linked from another site or found from a web search. If your child can not describe exactly what he or she needs to use the Internet for, don't let him or her use it until the purpose is explained.

46. Know Your Child's Friends.

Get to know your child's chat room and social networking friends just like you would learn about his or her real life friends. Find out which ones are on-line only friends, how old they are, and how your child met them. Being involved in your child's social circle will help you to recognize any unusual signs as early as possible.

47. Know the Source.

Remind children not to open up emails, attachments or links that come from anyone they do not know. If they do not know the person who sent the email, they should delete the message without reading it.

48. Be Skeptical. Teach children not to believe everything they see on-line. Content is not regulated, so nearly anyone can post information regardless of whether or not it is true. Encourage use of reputable sources for home work assignments, including sites with the .org, .edu, and .gov suffix.

49. Know the Difference.
Young children may have difficulty separating on-line life from life in the real world. This can be especially confusing when the child is involved in role-playing games with avatars. Maintain a healthy balance of real life and Internet use to reinforce the separation.

50. Family E-mail.
Create an e-mail address that all family members can share instead of giving young children their own e-mail address. This will allow parental monitoring of e-mails as the child learns more about how to use the Internet.

51. Chat Room Safety.
If children use chat rooms, encourage them to stay in the public chat area instead of engaging in private chat. There is safety in numbers, and in a public chat area (as in the real world) a Good Samaritan is likely to jump in if someone is being targeted or threatened.

52. Pornography.
Curious teens may want to view pornographic photos or videos. Talk to them about their interest and explain to them about why they should not visit those websites. Use parental control software to block these sites if necessary.

53. Follow Age Limits.

Most websites require that registered users be older than 13 years old. Follow these limits; they are there for a reason. Sites that are geared towards teens and adults may include photos or language inappropriate for young children. Pornographic websites and websites for tobacco companies often require that visitors be over age 18, and alcohol manufacturer websites require visitors be older than 21 years of age.

54. Kids Social Sites.

If your child wants to join a social networking site, suggest those specifically designed for kids, like Webkinz or Club Penguin. These sites offer gaming and a social atmosphere in a kids-only environment. They also have built in privacy features, like use of an avatar instead of a profile photo.

55. "Friend" Your Kids.

Create an account on the same social networking site that you child uses and become one of their friends. This will allow you to keep an eye on what they do, as well as monitor the activity of their friends.

56. Social Networking Privacy.

If your child uses an adult social networking site, teach your child how to use the privacy features so they can keep personal information private. Set up their pages so friends can only be added with their consent. Unless someone is a confirmed friend, he or she will not be able to view any of the details of your child's page.

57. Instant Messaging Privacy.

Help your child set up an instant messaging profile that only allows people from a buddy list to see when he or she is online. His or her status will remain invisible to strangers, which will eliminate messages from unknown users.

58. Protect Your Child's Friends.

Review websites and blogs that belong to your child's school friends to ensure that they too are protecting their own privacy. Let the friends' parents know if you notice any postings or activity that could pose risks.

59. Time Limits.

If Internet use becomes excessive or replaces normal socialization and activities, install a program that sets limits on time spent on-line and blocks access during specified hours. Programs that enforce time limitations can be found on-line, and many parental control software programs include time limit features.

60. Follow Website Policies.

Most websites include a terms and conditions page that may include rules of conduct in discussion boards or use of copyrighted materials. When a child registers with a website, read these policies together to ensure your child understands the expectations.

61. Beware Classified Ads.

Although children may like to browse for sale/wanted ads on Backpage or Craigslist, do not allow them to respond to the ad directly. Instead, a parent should initiate the communication.

62. Check Their E-mail.

Log in to your child's email account from time to time to ensure they are following the house rules of Internet conduct. Check both incoming and outgoing messages for anything unusual.

63. Avoid E-mail Spam.

Reduce e-mail spam by limiting the websites your child registers for using an e-mail address. Also teach children not to reply to junk e-mails. Most e-mail programs have spam filters that will automatically delete pornographic or bulk advertising messages.

64. Email Preview.

Set email preferences so messages do not display unless clicked on. When the content of e-mail messages displays automatically, your child may see explicit photos or messages that they had no control over receiving.

65. Photo Downloads.

Tell children not to download pictures or videos from unknown sources. Although they may be labeled innocently, these files could contain viruses or display pornographic materials.

66. Research Safeguards.

Learn about the filtering programs and protections used anywhere your child accesses the Internet, including at school, at the library, or at friend's houses.

67. User Names.

Require parental approval of children's nicknames for websites, chat rooms, and on-line games. Be sure that the name does not contain too much personal information and that it does not include slang or references that are inappropriate for a child. If an avatar is used for certain websites, also ensure that it is tasteful and age-appropriate.

68. Be Wary of Strange Messages.

Hackers and e-mail viruses can operate under recognized identities, so teach children to be aware of any strange e-mails, even if the sender's name is familiar. Examples of strange messages include attachments with odd file extensions or incoherent words in the message body. Treat these messages as they would ones from unknown senders.

69. Protect Others' Email Addresses.

To avoid sharing away e-mail addresses of friends and family, do not allow children to let social networking sites scan their e-mail address book.

70. Go Direct.

Instead of using a search engine to access sites, have children type the url directly into the address bar or use a bookmark. This will eliminate the possibility of offensive or unrelated sites being accessed from a web search.

71. Search Engine Filter.

Using a filtering program can help eliminate inappropriate results from a web search. Without a filter, a web search can bring up material that children should not see.

72. Assume Permanence.

Teach children to operate under the assumption that everything they post on-line is permanent and can be found by predators or hackers even after deletion. While social networking pages and websites can be deleted, people who know how to find it can still access the information.

73. Blog Privacy.

If your child wants to write in a blog or web diary, find a site that allows private and password-secured blogs. Blogs with privacy protection will ensure that your child's personal profile is not revealed. Modify the blog settings so comments can not be added to posts; this will reduce spam and negative or offensive feedback.

74. Positive Examples.

Find content-appropriate blogs made by other children as an example for your child to model his or hers after. Good examples may be blogs centered on a favorite sports team, television show, or hobby.

75. Review Their Posts.

Screen your child's writing or photos before they are posted on-line to ensure that they do not include too much personal information. Watch out for less obvious identifiers, like school mascot names and names of friends.

76. Protect Emotions.

Blog and diary content can include very personal topics. Ask your child if he or she is comfortable sharing the content with strangers before they post it. If he or she is not sure, do not post.

77. Be a Detective.

Perform occasional web searches for your child's name, address and other identifying factors to see if they have posted any personal information on a website. This research can also help you determine if your child started a website or blog without your knowledge.

78. Watch for Obsessive Behavior.

E-mail and social networking can become an addiction for adults and children. Watch for signs of obsession, including constantly wanting to check for new messages or frustration when not able to access the sites.

79. Vulnerability.

Be aware of blog posts or discussion board comments that show emotional vulnerability. Not only are these what Internet predators look for, but they could be signs of emotional stresses and troubles that your child is not comfortable sharing with you.

80. Cyberbullying.

Bullies no longer exist only in the classroom. Oftentimes, the same child who bullies a child in person will begin to bully on-cyberbullying, like a child becoming upset when online or a not wanting to go to school.

81. Golden Rule.

Don't allow your child to bully or gossip about others on-line. Even though the interactions are not in-person, the same rules of conduct and respect should apply. Have disciplinary consequences for not treating others kindly.

82. Honesty.

Do not allow your children to pretend that they are someone else online.This includes not listing their actual age on social networking sites. Instead of lying, teach them to use privacy controls to hide information and not answer questions that make them feel uncomfortable or would require them to reveal personal information.

83. Piracy.

Do not allow children to download, share, or duplicate copyrighted software or music without paying. Even if your child is not distributing the material further, use of pirated software and music is still illegal. Explain that it is stealing and there are serious legal consequences.

84. Block File-Sharing.

File-sharing network sites often distribute copyrighted material. The unknown source of the download creates privacy and virus risks. Many file sharing software programs also place a file on your computer that allows others to receive files from you, with or without your knowledge.

85. Use Voice Chat With Care.

Some on-line video games allow for voice chatting. Be sure that if children participate, they follow the same rules as in a text chat room and do not divulge personal information to strangers. Keep in mind that predators may disguise their voices to sound like children even though they are adults.

86. Encourage Playing with Friends.

Recommend that your child play on-line games and chat with friends from school and other activities instead of exclusively communicating with on-line only friends. Knowing everyone personally creates the safest environment for on-line play.

87. Know the Games.

Become aware of the games your child plays on-line. Understand the rules, content, and average player age. Playing games with your kids is a good way to get involved in their on-line activities without appearing too intrusive.

88. Minimize Fees.

Many on-line video games have monthly service fees that children may not know about until parents receive the bill. Steer your kids towards free games that do not require submission of personal credit card information.

89. Prohibit Gambling.

Remind your children that it is illegal for minors to gamble on-line. Even though it's not real money, discourage use of non-monetary casino gambling games (like free poker and blackjack), as they still operate around a wagering system that can lead to actual gambling in the future.

90. Supervise.

Young children should not use the Internet without supervision. Always stay with young kids while they are on-line to answer questions and eliminate the possibility of wandering onto an inappropriate site.

91. Role Model.

All members of the family members should act as positive role models for children who are just beginning to use the Internet. Everyone should follow the same rules of conduct with respect to safety concerning the sharing of personal information. Parents especially should practice what they preach with regard to software piracy, pornography, and chat rooms.

92. Cyberdating.

Discourage teens from using websites to meet potential boyfriends or girlfriends. These sites are intended for adults, and many have niches that may not be appropriate for anyone younger than 18 years old. In addition, people are not always what they seem, and these romance sites are a haven for Internet predators.

93. Review Browser History.

Take a look at the history of sites visited to see where your child went on-line and what they did. Confront them with indiscretions or questions you have about their web browsing activities.

94. Webcams.

While webcams can be useful for video chat with friends or long-distance relatives, ensure that children use the device appropriately. Children should avoid video chat with strangers because of the physical recognition factor. Review your child's videos before they are posted or distributed to others.

95. Sexting.

Explain the dangers and legal consequences of children and teens sending each other nude or partially nude photos via the Internet. Once the photo is sent by the originator, he or she has no control over what other people decide to do with it. Remind them that once something is posted on-line it can travel quickly and be seen by many people, including family, friends, and teachers.

96. Look for Signs of Misconduct.

If a child or teen quickly closes a browsing window when you enter the room or you find that browsing history has been deleted, it is often a sign that he or she is not following the rules. Children rarely hide good behavior. Find out what is going on and discipline accordingly.

97. Plagiarism.

When a child uses on-line resources for homework assignments, be sure that they do not copy other people's ideas as if they were their own. Explain plagiarism and the consequences it will have at school. If you suspect that your child has used someone else's content, several free plagiarism-detections services exist on-line.

98. Sibling Enforcement.

Teach older children to protect younger brothers and sisters on-line and to tell parents if they are engaging in any potentially harmful activities. Younger children often look up to older siblings and are comfortable learning the ropes from them.

