



Applications and Websites Parents Need to Know About

Children and young people spend a lot of time online and may face risks such as cyberbullying, being exposed to inappropriate content or sexual exploitation.

The internet isn't a thing, it's a place and it can be a very dangerous and scary place for young people to visit. Having no parental control of your child's access to the internet is like your child going to a distant city or foreign country without your permission. You may think your child is safe upstairs in their bedroom but who are they talking to, what are they seeing, experiencing, what advice are they being given, are they being blackmailed or being sexually exploited?

This information sheet will give you a snap shot of some of the popular applications (apps) and websites that young people use and visit.

Updated June 2014







This app allows users to interact in a question-and-answer format — with friends, peers, and anonymous users alike.

The app is rated ages 13+ and some young people have used the app for hurtful cyberbullying that has been linked to <u>suicides</u>. Some Derbyshire schools have sent home letters calling for students to stop using ask,fm because of its use in several cyberbullying incidents leading to attempted suicides, and its loose regulation and lack of monitoring. The site added a button where users can report abuse after <u>nationwide pressure</u>, but some parents feel it's too little, too late. Check out <u>Ask,fm Guide for Parents and Teachers</u>



Instagram

This hugely popular photo-sharing site is owned by Facebook, so you may be more familiar with it than with other photo-sharing apps. Users can add cool filters or create collages of their photos and share them across Facebook and other social media platforms. The app is rated 13+ and may be slightly tamer than Tumblr, but users can still find mature or inappropriate content and comments throughout the app (there is a way to flag inappropriate content for review). "Trolls" — or people making vicious, usually anonymous comments — are common. A user can change the settings to block their location or certain followers, but many users are casual about their settings, connecting with people they don't know well or at all. Check out A Parents' Guide to Instagram



Tumblr

Many children and young teens are also active on this 17+ photo-sharing app. It can also be used for sharing videos and chatting. Users can easily access pornographic, violent, and inappropriate content. It should also be noted that users need to jump through hoops to set up privacy settings — and until then, all of a user's photo and content is public for all to see. Mental health experts say that Tumblr can be damaging to adolescents' mental health because it tends to glorify self-harm and eating disorders. See the <u>safety rating</u> for this site.







MySpace

MySpace was the predecessor to Facebook but now teens are heading back to this network, but it's a little more dangerous now that all of their parents are gone. If your child has a profile on MySpace then it's important to check what the privacy settings are and who has access to the information.



Yik Yak

The producers of Yik Yak call it "the anonymous social wall for anything and everything." All users are anonymous (registration requires no personal information, other than a user's location), and their posts are called "Yaks" and show up in a live feed for other users — or "Yakkers" — in their area. The app's content-generation and moderation is entirely in the hands of its users (who can "vote" posts up or down in the news feed; after two "down" votes, a Yak disappears). The app is rated ages 17+ and targets college students, who can use it to spread the word about events or share their thoughts. But younger users are easily getting their hands on the app and using it to post hurtful comments and rumours about their peers.



Tinder

Tinder's developers describe the app as "the fun way to connect with new and interesting people around you." But it's mainly used as a dating tool or an anonymous meet locator by adults, college students, and even younger children. The app is rated ages 17+ but Tinder's privacy policy allows teens as young as 13 to register (the app connects with Facebook — which is also technically for ages 13+ — to pull in photos for users' Tinder profiles). Tinder helps people find others in their geographic location and allows users to view each other's' photos and start instant messaging once both people have "liked" one another. The geolocation features and anonymous nature of the app puts young people at risk for catfishing, sexual harassment, stalking, and worse.







Kik Messenger

Kik is a mobile app that people can use to text with friends at high speed and with more of a "face-to-face feel" than regular texting (users' profile pictures appear in a little bubble next to their text, and they can quickly text photos, sketches, or even pre-designed greeting cards to individuals or groups). The app is rated ages 17+, but there is no age verification so anyone can download it. Like some other instant messenger apps, Kik allows your child to connect with others using just a username (rather than texting from their phone number). Reviews in the App Store and Google Play store reveal that many people use Kik to meet strangers or for sexting. Click for further information about Kik Messenger.



Voxer

This walkie-talkie PTT (push-to-talk) app allows users to quickly exchange short voice messages. They can have chats going on with multiple people at a time and just have to tap the play button to hear any messages they receive. Although it largely has an adult following, it's becoming popular among teens who enjoy its hybrid style of texting and talking. Hurtful messages from cyberbullies can be even more biting when they're spoken and can be played repeatedly. Surprisingly, the app is rated ages 4+ in the App Store.



Snapchat

Snapchat is an app that allows users to send photos and videos that disappear from view within 10 seconds after they're received. It's rated ages 12+. Some young people are using the app to send risqué pics because they believe the images can't be saved and circulated. But it turns out that Snapchat pics don't completely disappear from a device, users can take a screenshot before an image vanishes in the app and other apps link to the Snapchat account and saves the pictures before it's opened in Snapchat. For further information see 'A Parents' Guide to Snapchat'.







Poke

Poke is Facebook's app that, similar to Snapchat, promises that photos sent will "self-destruct" within seconds after they're received. While Poke isn't nearly as popular as Snapchat, it is still gaining young users who can use it for sexting. Also like Snapchat, the images sent via Poke can be saved or viewed with certain workarounds. The App store rates it ages 4+ (but it is connected to Facebook, which is a 13+ site).



Vine

Vine is Twitter's mobile app that allows users to shoot and share short loops of video (6 seconds or less). It's rated 17+, but children and teens are still downloading it. As with any multimedia app, the content on Vine covers the spectrum. "With the most basic creative searching, young people can find nudity, sex, drug use, offensive language, hardcore sexuality, and more," in a review of the app. "While there are plenty of fun videos, even adults might be shocked at some of the things they find."



Whisper

This 17+ app's motto is: "Share Secrets, Express Yourself, Meet New People." Whisper lets users set up anonymous accounts to make their messages or confessions overlap an image or graphic (similar to e-postcards), which other users can then "like," share, or comment on. While it allows for creative expression, it can also take overly personal content viral. The app also shows a user's location. Although the app is geared toward older teens and adults, younger children are finding their way to it and there are reports of children being aroomed and exploited.







Shots of Me

Justin Bieber has <u>invested in this 12+ "selfie-only"</u> photo-sharing app in part because he was attracted to its "anti-trolling" aspect; it does not have a comment section under photos posted on the app. Instead of a public comment area, the app has a direct-messaging feature where users can only send private messages to one another. The anti-trolling feature might also help ward off cyberbullying among teens who like to put meanness on display (but teens could still be nasty via private message). The app does show a user's location and how long ago a photo was added unless those features are managed in the app's settings. Shots of Me is currently available only for Apple devices.



Omegle

Omegle is an app for chatting with "random strangers." When you open Omega, it chooses a random stranger for you to chat with. After meeting the stranger you can choose to keep talking or find someone else. Omegle can be used by adults to sexually exploit young people.



Chatroulette

Chatroulette is an online chat website that pairs random people from around the world together for webcam-based conversations. Visitors to the website begin an online chat (text, audio, and video) with another visitor. At any point, either user may leave the current chat by initiating another random connection. There are many chatroulette alternative sites; Bazoocam, FunYo, Roulettechat, Quierochat, Dirtyroulette, Chatpig, Chatxroulette, Live Cam4, Manroulette, Tinychat, Facebuzz, Chatrad, Flipchat, Gaypage & Cam Girls, all child participation should be monitored.







Facebook

The Global Social Media Impact Study 2013 found that teens have "lost interest" for Facebook — in part because their parents and other adults have taken over the domain and because their peers engage in too much "drama" on the site. But Facebook still remains the top social media site among young people, who say that their peers continue to stay on the site so they don't miss anything happening there. Your child may keep a profile on Facebook but may be much more active on newer platforms.

Meanwhile, Twitter use is rising among teens and WhatsApp being the No1 choice to send personal messages.

Online Gaming

You can play games online through your computer, smart phone and games consoles like the Nintendo Wii, Xbox 360 and Playstation. The consoles are basically computers designed specifically for game playing and they can be used on their own, but once connected to the internet each has its own website and extended community with millions of players. With all online activity there are dangers and adult supervision should be provided if your child is game playing online.

Video games are rated by PEGI (<u>Pan European Game Information</u>) and follow an easy to understand 'traffic light' system. Games rated 3 and 7 (green), 12 and 16 (amber) and 18 (red). The 12, 16 and 18 ratings are legally enforceable as the minimum age you need to be to buy the game.

PEGI sets standards for the age rating of interactive games, both online and offline. It gives clear advice on content to provide certainty for parents – and the strongest possible protection for children.





PEGI Age Ratings



The content of games given this rating is considered suitable for all age groups. Some violence in a comical context (typically Bugs Bunny or Tom & Jerry cartoon-like forms of violence) is acceptable. The child should not be able to associate the character on the screen with real life characters, they should be totally fantasy. The game should not contain any sounds or pictures that are likely to scare or frighten young children. No bad language should be heard.



Any game that would normally be rated at 3 but contains some possibly frightening scenes or sounds may be considered suitable in this category. Some scenes of partial nudity may be permitted but never in a sexual context.



Videogames that show violence of a slightly more graphic nature towards fantasy character and/or non-graphic violence towards human-looking characters or recognisable animals, as well as videogames that show nudity of a slightly more graphic nature would fall in this age category. Any bad language in this category must be mild and fall short of sexual expletives.



This rating is applied once the depiction of violence (or sexual activity) reaches a stage that looks the same as would be expected in real life. More extreme bad language, the concept of the use of tobacco and drugs and the depiction of criminal activities can be content of games that are rated 16.



This adult rating is applied when the level of violence reaches a stage where it becomes gross violence and/or includes elements of specific types of violence. In general terms it is where the level of violence is so visually strong that it would make the reasonable viewer react with a sense of revulsion. This rating is also applied where the level of sexual activity is explicit which may mean that genitals are visible. Any game that glamorises the use of real life drugs will also probably fall into this category.

The PEGI ratings are found on the front, back and spine of the game case. It should also be noted that the ratings relate to the content of the game and not to how difficult the game is to play. A chess game would probably have a 3 rating but would hardly be recommended for toddlers.





Game descriptors

As an additional aid to purchasers (particularly parents and carers) video games rated under the PEGI system will usually display one or more descriptors to give an indication as to the reasons why a game has been age rated at a particular age level. There are 10 possible descriptors.



The video game may refer to or depict the use of drugs.



The video game may be frightening or scary for young children.



The video game may contain depictions of or material which may encourage discrimination.



The video game will contain bad language. At a 12 rating this will be mild swearing but at a 16 rating and above it will include sexual expletives.



The video game may encourage or teach gambling.



The video game will contain depictions of violence



The video game may show nudity in a sexual setting



The video game may contain horrific sounds or horror effects which may be shocking or cause revulsion to the viewer



The video game may show sexual behaviour or sexual references



The video game can be played online possibly with or against other people

Allowing your child to use an age inappropriate game can increase children's aggression. Please read Dr Phil's article on <u>Children and Violent Video Games</u>.





Steps to help protect your child online.

Parents need to educate themselves and become comfortable with the Internet to communicate the dangers and risks of being online with your children.

Supervise your children on the Internet just as you would monitor what movies and TV shows they watch and the places they go with their friends.

You would not let your children open the door to a stranger, so don't let them spend long hours online alone. GetSafeOnline offer free expert advice around using and protecting yourself against the dangers online. You can also download free online access control software so you can track your child's use of the Internet and block objectionable material from reaching your household.

The NSPCC have created a suite of age appropriate Online Safety Checklists, <u>Under 5's</u>, <u>Primary Children</u>, <u>Teenagers</u> and <u>Safety Tips</u>.

But remember; no product can fulfil all your needs and there is no substitute for your involvement and supervision of your children.

Pay attention to your children because, if you don't, someone else may.

Here are a few tips to help you get started:

1. Place your computer in a common area of the house.

This is probably the most important thing you can do. Do not let your children be in their rooms all night on the Internet. The mere presence of parents can have a tremendous effect on a child's online activities. It's much more difficult for someone to sexually exploit a child when the computer screen is visible to a parent or other member of the household.

2. Educate yourself about computers and the Internet.

You need to know how to use the Internet in order to know what your children are doing on it. Take a basic computer class, check relevant sites or buy a book about the Internet. Check with your ISP (Internet Service Provider) for information on using all of their services. Go to some of the sites listed in "Resources" to help you get started.

3. Spend time with your children online.

Ask your children how they use the Internet and have them teach you about their favourite destinations. Make "surfing the Net" a family experience. Just as you look for good television programs for your children, take the time to find the best and most useful websites for them.

4. Make reasonable rules and set time and use limits. Enforce them.

You should set guidelines about what your children can and cannot do on the Internet. Try to understand their needs, interest and curiosity. But, you must set limits on when they may use the Internet and for how long. Use an <u>agreement</u> or <u>contract</u> for everyone to sign listing the rules about keeping safe online.

5. Educate yourself and your child about the dangers of the Internet.

Teach your children about sexual victimisation and other potential dangers of the Internet. Talk openly and honestly with your children about what they are doing online and what your concerns are.

6. Do not allow your child to go into private chat rooms, especially when you are not present.

Computer sex offenders will often meet potential victims using chat rooms. Later, they'll





attempt to communicate with young people by way of e-mail or instant messaging. If you can, try to keep your child out of chat rooms altogether. You never know who is in a chat room watching and waiting for a victim.

7. Reinforce the guiding rule, "Don't talk to strangers."

Tell your children what they are told online may, or may not, be true. No matter how much their online "buddies" seem like friends who share interests, they are still strangers. Remember, paedophiles pretend to be children.

8. Put accounts in your name and know your child's passwords.

The Internet account and primary screen name should be in your name, not your children's names. It's also a good idea to know your children's passwords and let them know you will check their online activity.

9. Never allow your children to arrange a face-to-face meeting with someone they met online without your permission.

Many predators want to meet a child for sexual contact. Your child should never meet a stranger alone in a face-to-face meeting. If you ever do agree to a meeting, make sure it is in a public place and accompany your child.

10. Do not let your child give out any personal information of any kind on the Internet.

Children should never give out their name, home address, telephone number or school name. They should be aware that even naming a friend, local sports team, shopping centre or community event could give away their identities. Also be aware that sharing photos could contain the details of the place it was taken in the metadata.

11. Do not let your child download or upload pictures without your permission.

Predators will often send photographs or visuals to children as part of a grooming process to gain trust. Some of the photographs may be pornographic and may even involve child pornography.

12. Utilise your Internet Service Provider's parental controls and commercial blocking and filtering software tools.

Most ISP's have parental controls – use them. Other filtering and monitoring software programs can be purchased separately. Monitors show a history of use so you can see where your child has been on the Internet. Filters block access to objectionable material. Remember, while parents should utilise monitors and filters, do not totally rely upon them. There is no substitute for parental guidance and supervision.

13. Be sensitive to changes in your children's behaviours that may indicate they are being victimised.

Be alert to personality changes. If victimized online, children may become withdrawn from their families or secretive about their activities. Computer sex offenders work very hard at driving a wedge between children and their parents.





14. Be alert to a teenager or adult who is paying an unusual amount of attention to your children or giving them gifts.

Most sexual offenders are not just satisfied with the computer. Eventually, they want to talk to the children on the telephone, engage in "phone sex" and set up a meeting. As part of a "seduction" process, a sexual offender may send letters, photographs, gifts or packages to potential victims. Some offenders have even sent children digital cameras and plane tickets.

15. Be aware of other computers your children could be using.

Your children probably use computers at the library, school, friends' houses – maybe even cyber-cafés. Talk to your children about other computers they use.

16. Be aware of your child using another person's screen name.

Watch for your child using an online account belonging to someone else in order to bypass filters or monitors on your computer. Computer sex offenders may provide potential victims with a computer account for communication with them.





i-Tune apps

- **4+** Applications in this category contain no objectionable material.
- **9+** Applications in this category may contain mild or infrequent occurrences of cartoon, fantasy or realistic violence, and infrequent or mild mature, suggestive, or horror-themed content which may not be suitable for children under the age of 9.
- **12+** Applications in this category may also contain infrequent mild language, frequent or intense cartoon, fantasy or realistic violence, and mild or infrequent mature or suggestive themes, and simulated gambling which may not be suitable for children under the age of 12.
- 17+ You must be at least 17 years old to purchase this application. Applications in this category may also contain frequent and intense offensive language; frequent and intense cartoon, fantasy or realistic violence; and frequent and intense mature, horror, and suggestive themes; plus sexual content, nudity, alcohol, tobacco, and drugs which may not be suitable for children under the age of 17.
- How do apps get their content ratings?
 The app developer fills out a form describing their application. The rating is then generated based on that description.
- Can parents restrict apps by content rating?
- There are steps that will prevent your child from downloading apps based on their rating. Note that they will still be able to SEE all the apps in the App store; but the option to download or buy them will be disabled if the rating is higher than parents you allow.
- Even with the restrictions in place, for younger children it's a good idea to review each app that a child wants to download or at least review it after-the-fact. Even an app rated 4+ may not be what you want your children to use