A Parents' Guide to

facebook

By Anne Collier and Larry Magid

Co-Directors, ConnectSafely.org



ConnectSafely
Smart Socializing Starts Here™

iKeepSafe
PEACE OF MIND FOR FAMILIES ONLINE™

Table of Contents

INTRODUCTION 2
- What is Facebook? 2
- What do people do on Facebook? 2
- Why do young people use Facebook? 3
- Is Facebook safe? 3
- What are the risks involved in social networking? 4
- How do we parent Facebook users? 5
- Ways to monitor your child's Facebook activities 6
- Safety, privacy and reputation protection in the digital age 6
- Digital footprints & good reputations 7

HOW TO OPTIMIZE FACEBOOK SETTINGS FOR YOUNG PEOPLE 8
- Your children's profiles are a reflection on them 8
- Why children should be honest about their age 9
- Choose friends wisely 10
- Messages, Wall Posts & News Feed 11
- To limit what's on your child's profile 12
- See what your profile looks like to others 14
- Configuring who can see what you post 14
- Extra protections for minors 15
- Basic privacy controls 15
- Customizing privacy settings 16
- Limiting who can see your info or search for you 18
- Controlling who can see individual posts 20
- Lists: A powerful privacy feature 21
- Using the Groups feature 22
- Photos and tagging 24
- Controlling Facebook applications 26
- Limiting individual applications 27
- Facebook's location-sharing Places 28
- Reporting problems 31
- Preventing suicide and other self-harm 33

CONCLUSION 34

INTRODUCTION

Welcome to our guidebook for parents! It's designed to help you understand what Facebook is and how to use it safely. With it, you will be better informed and able to communicate with young Facebook users in your life. That's important because 1) if something goes wrong, we want our children to come to us and 2) as the Internet becomes increasingly social and mobile, a parent's guidance and support are ever more key to young people's well-being in social media and technology.

Note to readers: Facebook adds new features and updates old ones on a regular basis. This guide has the latest available information at time of publication. If you find anything in the guide that is out-of-date, please send an email to admin@connectsafely.org.

What is Facebook?

Developed in 2004 by then Harvard University student Mark Zuckerberg, Facebook is a social networking site used by more than 500 million people in every country on the planet, so far in 70 languages. The site's minimum age is 13, but teens represent only a minority population on Facebook. It's used by a lot of adults, certainly including parents. But not just individuals – Facebook's also used by businesses, organizations and governments all over the world, to send marketing messages, seek charitable funding and communicate with customers and constituents.

Facebook is certainly not the only social networking site. There are thousands of them, based all over the world, some general-interest social sites for people in a specific country and some for specific interest groups in many categories – students, sports fans, film aficionados, cooks, travelers, gamers, music lovers, etc. Some social sites are designed for use on computers, some just for mobile phones. Facebook is accessed by both.

What do people do on Facebook?

They chat, share photos (more than 100 million new ones each day!), post videos, stay in touch and share personal news, play games, plan meetings and get-togethers, send birthday and holiday wishes, do homework and business together, find and contact long-lost friends and relatives, review books and recommend restaurants, support charitable causes....

In fact, there's very little people *can't* do on Facebook. It's sometimes called a "social utility." Like a power grid, it provides the supporting infrastructure for the constantly changing everyday activities of hundreds of millions of users, 24 hours a day, 7 days a week. The amount of activity on Facebook is almost inconceivable. Every month, users add more than 30 billion pieces of content (comments, photos, Web links, blog posts, videos, etc.) to Facebook.

In effect, the "product" of Facebook is a living thing that changes constantly. Unlike the media we parents grew up with – books, newspapers, and even radio and television – it's "user-driven," the collective product of its millions of users' lives (not just their social lives), updated spontaneously, moment-by-moment around the world. It's a large swath of the wired and wireless social Web that increasingly mirrors all of human life.

Why do young people use Facebook?

For as many reasons as adults do. The research of psychologists and sociologists shows us that they use social networking sites for:

- Socializing or "hanging out" with their friends, for the most part friends at school
- Day-to-day news about their friends, acquaintances, relatives, and peer groups
- Collaborating on school work
- Validation or emotional support
- Self-expression and the identity exploration and formation that occurs in adolescent development
- What sociologists call "informal learning," or learning outside of formal settings such as school, including learning social norms and social literacy
- Learning the technical skills of the digital age, which many businesspeople feel are essential to professional development
- Discovering and exploring interests, both academic and future professional interests
- Learning about the world beyond their immediate home and school environments
- Civic engagement – participating in causes that are meaningful to them.

Is Facebook safe?

Just like communities in the physical world, no social networking site, virtual world, online game, or any other social-media service can provide a guarantee of 100% safety, Facebook included. Why? Because this is the social Web, and safety depends a great deal on users' behavior toward one another. Facebook provides safety and privacy features and education for its users. Parents would benefit from visiting Facebook's Safety Center, a comprehensive resource in the site with information for Teens, Parents, Educators, and Law Enforcement. That in-site safety information and this guidebook are important for the very reason that Facebook's "product" is produced by its users. Parents need to know that, on the social Web, safety is a shared responsibility – a constant negotiation between users (for example, all the friends in a photo being shared with other friends on the site), between users and the site, and between teen users and their parents.

So the short answer to that question is that, in this new, very social media environment, a user's safety depends on the user as much as on the site. That's why parents need to be informed and keep communication lines with their children wide open – because youth, like all Facebook users, are constantly communicating, posting, and sharing content in the site.

What are the risks involved in social networking?

Youth-risk research has recently made five important findings:

1. Young people who behave aggressively online are more than twice as likely to be victimized online, so children's own behavior in Facebook or any social site is key to their well-being on the social Web.
2. The most common risk young people face online is peer harassment or aggression – in other words hurtful, harassing, or defamatory behavior.
3. A child's psychosocial makeup and environment (for example, home and school) are better predictors of risk than any technology that the child uses, so...
4. Not all children are equally at risk online, and the children who are most at risk online are those who are most at risk in "real life," or offline.
5. Although, for the vast majority of youth, online social networking is largely a reflection of offline life, it can also amplify, perpetuate and widely distribute real-life problems or conflicts – very rapidly. Something posted in anger or on impulse is extremely difficult to take back, so it has never been more important for users (of any age) to think before they "speak," post, or send a text message.

Specific social networking risks include...

- Posting information about themselves that: a) could help strangers determine their physical location; b) could be used to manipulate them; or c) whether posted by them or others, could cause psychological harm or jeopardize reputations and future prospects
- Harassment or online bullying ("cyberbullying") on the part of your children or others'
- Spending too much time online, losing a sense of balance in their activities ("too much" is subjective, which is why parents need to be engaged)
- Exposure to inappropriate content (this too is subjective) – although, typically, worse content can be found out on the Web at large than in Facebook or other responsible social networking sites
- Potential for inappropriate contact with adults (parents need to ensure that social networking does not lead to offline contact unapproved by them and other caring adults in their children's lives)

- Damage to reputation or future prospects because of young people's own behavior or that of their peers – unkind or angry posts, compromising photos or videos, or group conflict depicted in text and imagery.

How do we parent Facebook users?

Just as in your child's offline life, you are key to helping him or her form a positive identity, maintain good relationships, and create a positive reputation on the social Web. We'll get specific in the how-to section, but here are a few basic social-Web parenting tips that would be very helpful to keep in mind:

Facebook use is very individual, which is why the No. 1 safety tip is "Talk with your child." Don't believe everything you read or hear about youth in Facebook, including in the news media, which often present a very negative picture. Adults who don't understand social media sometimes think of using Facebook as a single activity to which young people can get "addicted." If they're addicted to anything when using Facebook, it would be to their school friends or social experience. But even two children of different ages in a single family can use Facebook very differently. A recent study found that 1) even for avid young Facebook users, its use hasn't replaced their offline interests, such as sports or music, and 2) even when young people leave Facebook "on" all the time, it's often just "running in the background" as they do other things. If they're using Facebook while doing homework, parents may want to address the possibility of too much distraction from academic work.

As a parent, you are part of the solution when negative things happen, which is why you need to be informed not just about Facebook or social networking but also (and especially) about your children's use of them. They need your back-up.

Try not to overreact if something negative happens – another reason why it helps to be informed. An informed parent is a calm parent, and children are more likely to go to their parents when the conversation can stay calm and thoughtful. You can help them more when they choose to come and talk to you, so you'll want to maximize those opportunities for communication and support.

The well-stocked toolbox of today's parenting includes your family's values, household policies and rules (about, for example, how children use their time and when it's best to have digital devices turned off), and sometimes technology, or "parental control" tools, such as filtering and monitoring software products. If your child is uncommunicative about his or her online time, sometimes it helps to use monitoring software to know what kids are up to. It's usually best to be open with them about your use of a monitoring product, because if you do discover inappropriate Internet use, they won't be surprised that you know and turn the conversation into an argument about something other than their safety.

Facebook itself can be a great parenting tool. It can give you a rare window into your children's social lives as well as help you stay informed about their use of the site. In fact, ask your kids to show you how to set Facebook's privacy and safety features. Not only will you learn more about Facebook, you'll see how much they know about using the site wisely. If they haven't thought much about the privacy settings, use this guide to go through them together. After that, consider creating your own account on Facebook so you can "friend" your child. That's probably the best "monitoring tool" you could use. Many parents do. But do be careful about writing on their "wall" (Facebook page) or commenting on what they post; that might embarrass them, which can create an unnecessary unwanted communication barrier between you and your child.

Ways to monitor your child's Facebook activities

One way to monitor your child's Facebook activities, as we mentioned above, is to "friend" them and get them to friend you – then you can establish a family rule that says something like, "No one can block other family members from content any of us posts in Facebook." For parents' part – if you and your kids do become Facebook friends – resist the temptation to make public comments on their pages. Family members can always send each other messages, which are private like email messages.

Some kids might be willing to have their parents friend them but are embarrassed to have their parents' names show up on their friends list. Some parents solve this by creating an account under a different name, although it is a violation of Facebook's terms of service not to use your real name. Another approach some parents take is to require that they know all their children's passwords (email, instant messaging, social networking, etc.). We suggest this works better with younger children, because many teens would rather "go underground" (use other sites secretly) than allow parents that level of monitoring capability. The level of privacy a child has depends so much on the child and on a family's own policies and values.

It can also be helpful to type your child's name, address and phone number into a Web search engine such as Google or Bing to see if anything is being said about him or her on the Internet.

Another option is to subscribe to one of the new online reputation-monitoring services such as SafetyWeb or SocialShield, which can help you find out what your teen is posting online without your having to friend them in Facebook. These services charge a monthly fee.

Safety, privacy and reputation protection in the digital age

Before we go into detail about Facebook settings, some context on what it means to socialize and share personal information in a digital media environment might be helpful. In this section, we'll provide a bit of that background. And throughout this guidebook, we'll highlight some key parenting points for guiding young social networkers.

The meaning of privacy seems to be changing in today's *very social* media environment, and different from when we were children. Researchers say that people want to control their level of privacy rather than to be either entirely private (which defeats the whole purpose of socializing online) or entirely public online.

Sharing photos and information online has become part of how people stay in touch all over the world. Because using media is now a social experience, it's not a solitary activity, it's a shared or interactive one. And since photos and videos often depict groups of people, and one person's content and photos often appear on other people's pages and vice versa, safety and privacy in social media are also a shared experience – a negotiation. One person (your child or *you*) simply can't have complete control over anything he or she posts online, even when employing the strictest privacy settings.

> ***Safety and Reputation Point**: Whatever you post, positive or negative, can affect your relationships with people, how they feel about you and what they might say about you to others. We all need to remember that we're interacting with people in social networking sites – not text and images – even though the text and images are much more visible than the people.*

Young people's information-sharing in Facebook is very grounded in their "real world" relationships, peer groups and school life, research shows, and rarely with strangers. While that's very good, sometimes they're so focused on friends and peers that they don't think about how their content can be seen by or distributed to a much broader audience and be very difficult to take back. They may need their parents' help in understanding that it's almost impossible to control digital text, photos, video, etc., once it has been shared via phones and online.

> ***Reputation Point:** Even if your child's privacy settings are specifically set to Friends Only, there is a possibility that a friend can become an ex-friend or just try to play a prank on your child by copying and forwarding information that was meant only for friends. For this reason, it's important for users to be extremely careful about what they post online, even among their friends.*

Digital footprints & good reputations

Type in someone's name in a search engine and there is a chance you'll find out something about that person. That, along with the comments, photos, or videos they or others may have posted about them on a social networking site, are part of their "digital footprint." It's the accumulation of what we've left on the Internet from our online activities, including text messages on mobile phones, emails, online chats and even Web surfing.

Some people worry that *any* information posted about a young person online is bad, but positive posts can actually enhance teens' reputations – as long as

they don't include information that is not safe to share, such as their home address. Web pages, blogs, photos or status updates about their accomplishments in school or sports, for example, could actually improve their image. And, if someone does post something negative about your teen which can't be erased, it helps to have positive information out on the Net to counter-balance it.

> ***Reputation Point**: There is nothing wrong with having a digital footprint – hundreds of millions of people do now – but parents want their children's digital footprint to be a positive reflection on them. It's vitally important to be aware that we're leaving a trail of information and careful about what we say online. It's also good to be aware of what others are saying about us. The key to having a positive reputation online is being a good digital citizen: behaving civilly and respectfully toward others online and sharing positive information about oneself in blogs, social networking sites and other social media.*

HOW TO OPTIMIZE FACEBOOK SETTINGS FOR YOUNG PEOPLE

This section is a how-to guide for settings that help protect children in three key areas: safety, privacy and reputation. If you have any questions about specific settings or features, ask young Facebook users at your house! It's a great way to start a conversation (or have another) about how they're using the site.

Please don't be put off when we say "you" rather than "your teen" as we go through the settings. This is a parents' guide aimed mostly at helping you guide your child, but because so many parents now use Facebook themselves, this is for you too.

Your children's profiles are a reflection on them

More than the clothes you wear, the music you like, or the company you keep, your Facebook profile is a representation of you. Along with your profile photo or image and the photos of you that are shared by friends, your profile puts all the key information about you and your life in one place for an at-a-glance key to who you are. It's a little like a resume that is constantly being updated, but it's about all aspects of your life, it's multimedia, and it's updated by your friends too, not just you.

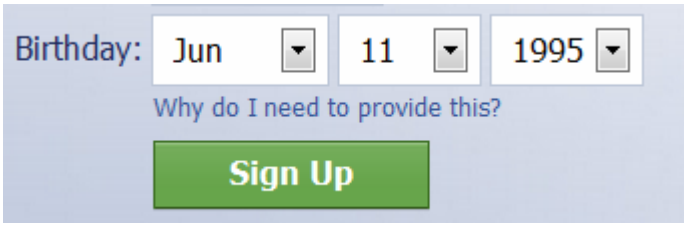
So it's very important to help our kids think carefully and often – really as often as they post photos and information – about what their profile says about them and who sees it. Working through the following how-to's for Facebook privacy will help you and your children think this digital self-representation through right now, but it's also a good idea to revisit those settings as kids mature and get ready for new phases of their lives.

***Safety, Privacy & Reputation Point**: What you say reflects on you. It always helps to think about the impact and audience when you post on someone's wall, "Like" or comment on someone's update or even support a cause. What might this say about you? If you just want to say something to a single friend, just send a private message or use Facebook chat. But remember that even that can be copied and posted somewhere else if the person didn't like what you said (or did)!*



Sample profile of "Cary Smarteen" shows her name, school, city, home town, relationship status, birthdate and 5 most recent photos – but "Cary" doesn't have to include all that!

Why children should be honest about their age



Facebook requires users to enter their real birthday. If they're under 13, they won't be allowed to sign up. If they're between 13 and 18, they will have some special protections just for minors.

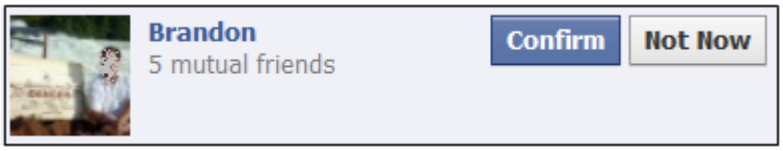
When you set up a new Facebook account, one of the first things you're asked to do is enter your full date of birth, including year. This is the only time that's required, and we recommend that it's the only time teens provide their birth year, whether asked for it or not. Birthdays are fine and can be left displayed in their profiles, but not the year. Friends usually know how old they are anyway, and it's usually not a good idea to share this information publically.

We strongly recommend against people lying about their age when they setup their account. There are both legal and child-development reasons why Facebook restricts membership to people 13 and older. In addition to complying with U.S. law, Facebook has created an environment designed only for teens and adults. The rules, policies, protections and safety education that Facebook has in place are all designed for people 13 and older.

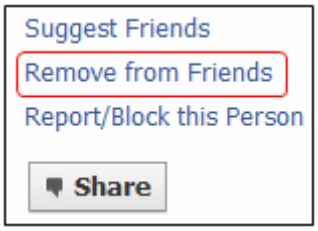
Having said that, we need to face reality. A July 2010 survey found that 37% of U.S. 10-to-12-year-olds were on Facebook, which means that every one of these children had to lie about their age to get on the service. Adults can discuss how good or bad this is for children, but it has become a fact of life we all face. If you have children under 13 who are on the service, we recommend that they cancel their accounts and that you encourage them to use more age-appropriate services. But if they are going to continue despite the site's restrictions, it's even more important to help them configure their privacy settings to the most restrictive level possible, and be sure to "friend" them or otherwise monitor their online use. Read on for how you can do that.

Choose friends wisely

After you or your teen has been on Facebook awhile, you will likely get friend requests. These are messages asking permission to be a Facebook "friend" with that person. Once you accept that request, you can see what they post and they can see what you post, subject to the privacy settings we cover later. If the request comes from someone you want to stay in touch with, you'll probably want to Confirm the person as a friend. But if you don't know that person from the real world or if you have any reason not to want to communicate with them on Facebook, you can click Not Now, and they will not be added. And if you choose never to add them, don't worry, they won't get a message saying you've rejected them.



Just as you can add friends, you can easily remove them by going to the bottom of their page and clicking Remove from Friends. Here, too, they will not get a message saying that they have been removed.



***Safety Point**: Research shows that aggressive behavior online increases the aggressor's risk. Bullying behavior can incite retaliation; online bullies and targets can switch roles in an instant – by typing comments or posting embarrassing photos in a chain reaction. So being kind or civil online isn't just a nice idea: it's also protective.*

Messages, Wall Posts & News Feed

There are several ways Facebook users can use the service to communicate with other people. One option is to send a Message that's basically like email (only the recipient sees the message). Another way is to write on someone's "wall," which can be very public. Depending on your privacy settings, what you write on a person's wall can be seen by all of your friends and possibly even a wider audience. Be careful not to make the fairly common mistake of using a wall to leave a private message.

Facebook has what it calls a News Feed, which is a stream of posts that users see on their Home pages – including posts from friends or in some cases friends of friends. Not everything that people post shows up in the News Feed, but a lot does. Posts can appear in the News Feed, subject to your privacy settings.

Facebook's 'email' service

In November 2010, Facebook introduced a change in its messaging system that enables users to get their own @Facebook.com email address. Called "Messages," this service, as it becomes available around the world, will make it possible for Facebook users to send or receive messages to or from anyone's email address. There will also be an option to send messages to friends' mobile phones, whether you're using your mobile phone or a computer.

The new service features a single mailbox called Messages, where all of your conversations (private messages, chat, text messages and, optionally, email) are sorted by person, so that all the communications you have with a single person are together. If it's available you'll find Messages right under News Feed in the left-hand column under your Profile photo.

For adults, the default setting is for everyone to be able to send you messages but, as with other aspects of privacy, "Everyone" is defined differently for minors. Only Friends and Friends of Friends can send messages to users under 18. Everyone else will get an automatic bounce-back reply. Both adults and minors can limit who can send messages to Friends Only.

To limit who can send you messages

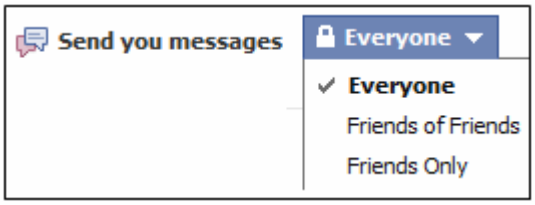
1. Click on Privacy Settings from the Account menu in the top-right corner of any page.



2. Click on View Settings from the Connecting on Facebook section near the top of the Choose Your Privacy Settings page.



3. Change the option to the right of Send you messages

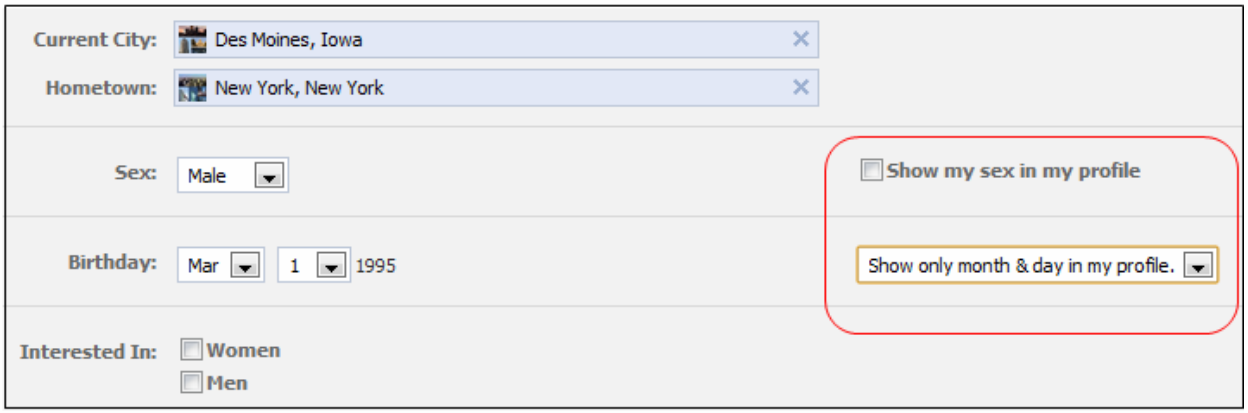


This service is being rolled out gradually, so it's possible that it may not yet be available for your account or in your region.

To limit what's on your child's profile

At any time, Facebook users can edit their page by going to their Profile and clicking Edit My Profile below their picture (or whatever image they've picked to represent themselves).

Although Facebook encourages members to add information to their profile, the profile is blank by default. Your children don't have to provide any information they don't want to include – even though there are places to enter all sorts of information. Decide with them what's best to leave blank.



What you see on the Edit My Profile page may vary, depending on age and privacy settings. You have to state your sex and year of birth but don't have to display them. (Not all fields are shown.)

The boxes in Basic Information and Likes and Interests can be great places for a teen to express who he or she is, but help your children give some thought to what they're posting in these sections of their profiles. Even something as innocuous as what's posted in Favorite Quotations can have an impact on their reputation, when combined with other information they share about themselves.

In particular, we suggest they give careful thought to whether or not it's appropriate to check the boxes next to Interested In and Looking For under Basic Information. Interested In (where you can choose Women or Men, or both or neither) is basically another way of stating one's sexual orientation – something teens might want to avoid. Looking For can be a way of specifying whether you are seeking a romantic relationship. Talk with your teens about what these settings would look like to friends, relatives, or strangers if they checked these boxes. In some cases, what they indicate could make them vulnerable to harassment or bullying.

Filling in Likes and Interests is generally fine and can help your child reach out to people with similar interests. On the other hand, depending on what's posted, it could also subject them to unnecessary scrutiny or bullying. Posting where they go to school in Education and Work is fine. Remind your teen to be very careful about what they put under Contact Information.

Even though Facebook requires users to state whether they're male or female when they register, the default setting is not to check Show my sex in my profile – and we recommend that teens leave it that way. The same goes for birth date. As we mentioned above, birthdays are fine but not year of birth. We strongly recommend that teens select Only show month & day in my profile or Don't show my birthday in my profile.

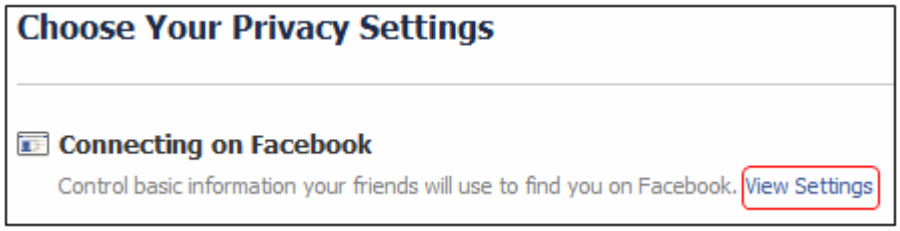
***Reputation Point**: In some communities, this can be a safety issue too: Teens might want to think twice before disclosing their political or religious views. Are those private matters for your family? You might want to talk with your children about what information is appropriate to share publicly, even to friends, who can share it with others.*

See what your profile looks like to others

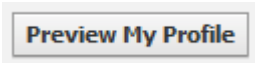
It may help young Facebook users to know how their profiles look to other people. View My Profile is a good place to start thinking about reputation management on Facebook. It also shows them how effective their privacy settings are.

To view your profile

1. Click on Account in the top-right corner of their Home page.
2. Click on Privacy Settings.
3. Click View Settings under Connecting on Facebook section.



4. On the right side of the gray bar at the top, click Preview My Profile.



Configuring who can see what you post

With a few exceptions, users can control who can see just about anything they post. And, for Facebook users under 18, there are even more levels of privacy protection. The exceptions are: Facebook displays all users' names, profile pictures, genders and the networks they belong to. However, even with these, you have some control. You or your teen don't have to post a profile picture (you can leave it blank or post a picture of an object or a cartoon character), and you don't need to belong to networks. You do need to provide your real name, which is a safety feature because it discourages people from pretending to be someone they are not.

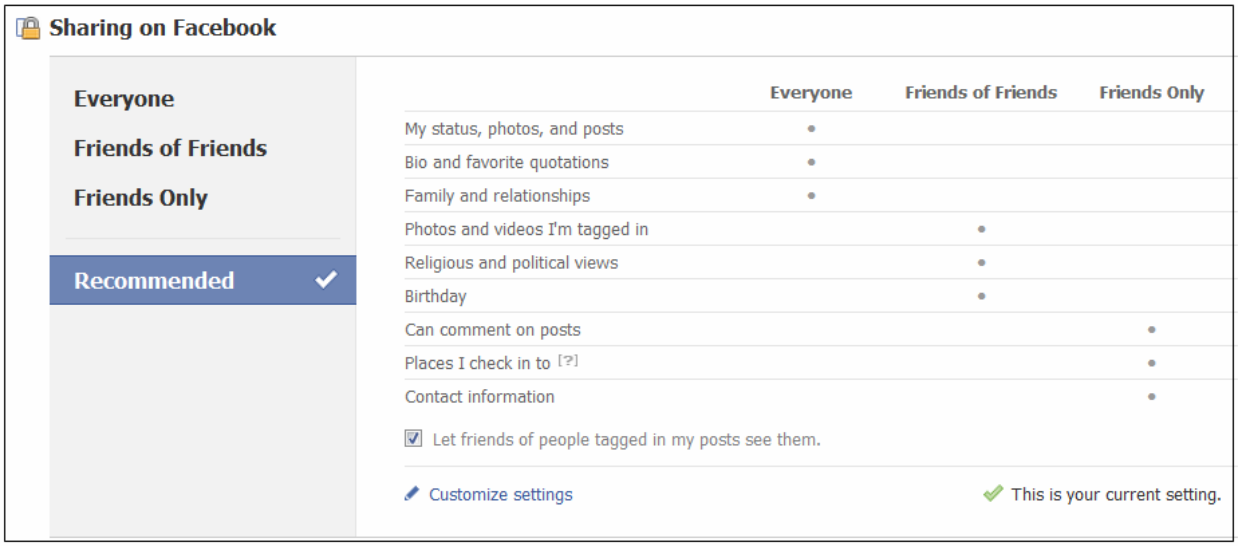
***Safety & Reputation Point**: Privacy is a double-edged sword. If your kids turn on maximum privacy settings (which we recommend) and make their groups Secret, it could also block parents from accessing that information. You should continue to have regular discussions with your teen about what they are posting on the service. But you also might consider that you can't know absolutely everything they're posting, just as you can't know what they're saying to their friends when you're not there. The good news is that you can see they are posting in public and, if you're their Facebook Friend, you can get a pretty good idea of what they're doing on the service.*

Extra protections for minors

There are extra protections for minors. For example, some of the privacy settings can be set to Everyone, which, for adults, means anyone with access to the Internet. But for minors, Everyone has a different meaning: Only the child's Friends, Friends of Friends and people in any verified school or work networks they have joined on Facebook. That means that, even if they wanted to, they couldn't use Facebook to share information to the entire world, regardless of how they configure their privacy settings. Of course, there is always the possibility that someone they do share with (such as a schoolmate) could copy or forward the information to another person or another site outside Facebook. If a child lies about his or her age and claims to be over 18, these protections won't be in place. That's why it's very important that children not lie about their date of birth when signing up for Facebook.

The only exceptions to Facebook's restrictive definition of Everyone where minors are concerned are in Search for me on Facebook and Send me friend requests. In those cases, everyone really does mean everyone but, again, teens can configure more restrictive access.

Basic privacy controls



Facebook's default privacy settings

Facebook's default privacy settings for people under 18 (see Recommended in the screen shot above) are the same as they are for adults, except, as we said earlier, Everyone is defined as only friends, friends of friends, and people in school or work networks. That alone provides a degree of protection, even if the teen does nothing to customize the settings. However, as you can see from the privacy settings screen, there are ways to expand or further restrict who can see your basic information.

For example, above Recommended are three other options. For adults, Everyone is extremely open because it can expose your status updates, comments, Contact Information and possibly even your location to anyone on Facebook, even if they're not a Friend or even a Friend of a Friend. That's why we don't recommend that for anyone.

If you or your teen checks Friends of Friends, that means that all of his or her friends' friends can see their information. While you do have control over who your friends are, you have no control over your friends' friends, which in some cases could add up to thousands of people.

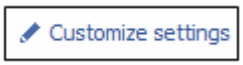
The Friends Only option is a more restrictive choice because it hides all of the information from friends of friends or people in a child's school network who are not on your child's friends list. With this option selected, only people the child has accepted as friends can access the information.

> ***Safety Point**: For maximum privacy, safety and security, we recommend that teens start by setting their privacy to Friends Only and then go to Customize Settings to consider even more private settings for some information.*

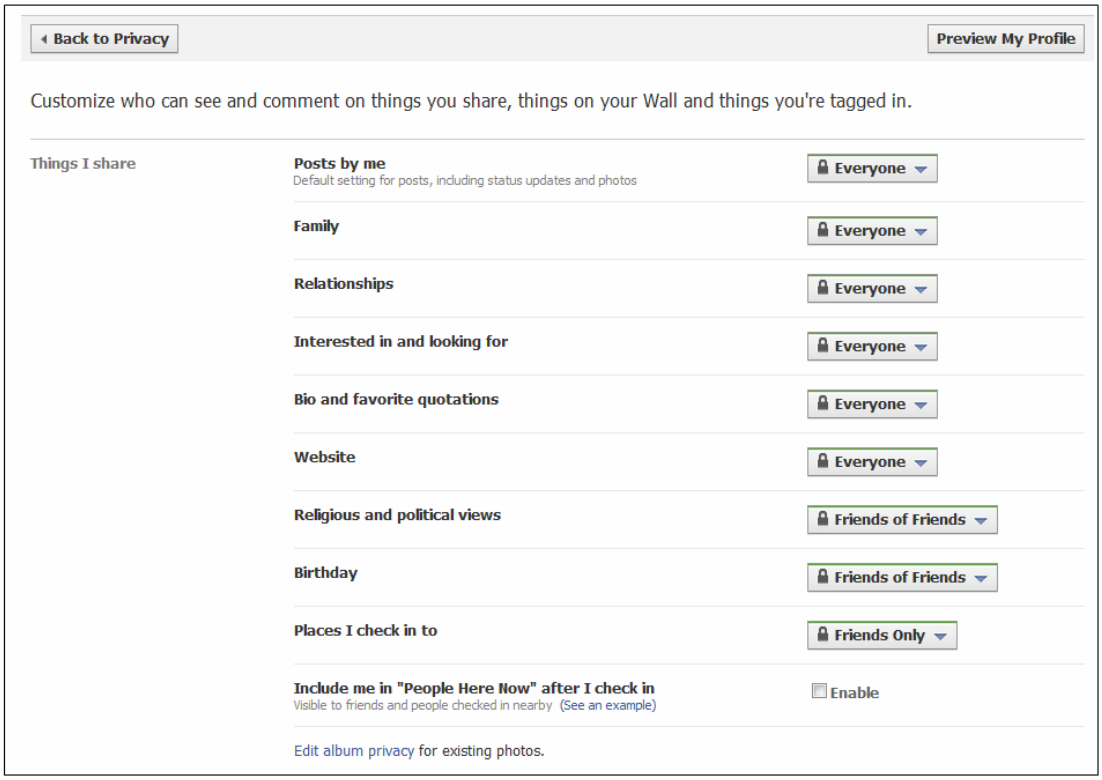
Customizing privacy settings

While many users know about these basic privacy settings, a lot of people don't know that they can be customized even further so that users can have a lot of control over who can see what.

Near the bottom of the Choose Your Privacy Settings screen is a link to Customize settings.



If you click on this link, you are taken to a page where you have a great deal of detailed control over your privacy.



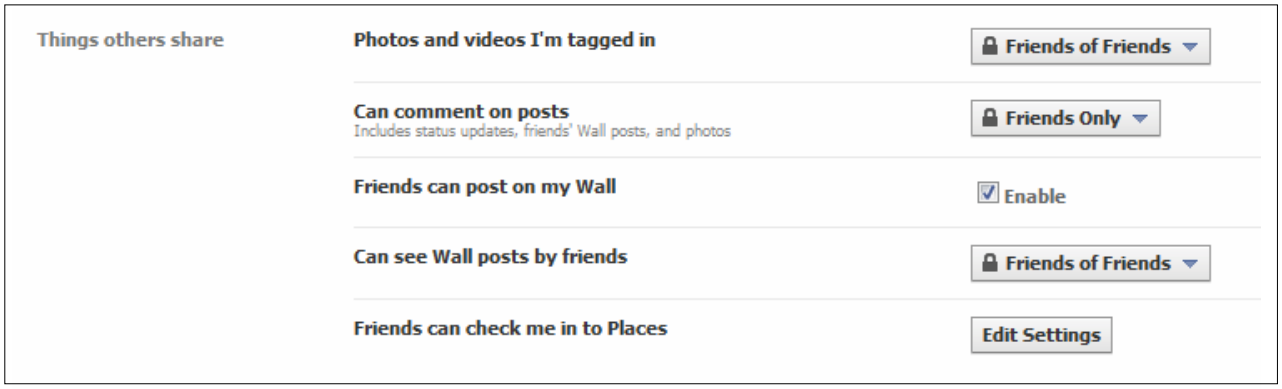
"Things I share" portion of privacy settings

The Customized settings page is divided into three categories: Things I share, Things others share and Contact information.

To the right of each item on the page is a drop-down box that lets you specify who has access to each of these items. For example, by default your posts can be seen by Everyone, but you can click on that box and change that to Friends of Friends, Friends Only and Customize.



The same choices are available for each item on this page. Pay close attention to items in the Things others share section. For example, by default Friends of Friends can tag, or identify, your teen in photos they post in their Facebook pages. You might want to limit this to Friends Only. [We'll get to the Places section later.]



"Things others share" section of privacy settings

Also pay attention to Contact information. By default it's Friends Only, but you might not even want your Facebook friends to know your phone numbers, address or even email address. There are two ways to prevent that: 1) Don't include it in your profile to begin with, and 2) use the Customize setting to even further restrict who can see that or any other information.

> ***Safety Point**: We do not recommend that anyone – especially minors – enter their home address. We also feel that teens should not enter their phone numbers, even though – by default – the information is available to Friends Only.*



"Contact Information" section of privacy settings: Consider limiting who can see your contact information.

Limiting who can see your info or search for you

> ***Privacy Point**: Your children can limit who sees their profiles. Regardless of what your teen enters in the profile, it's possible to control who has access to that information from the Privacy Settings page. We recommend that – at most – it be made available to Friends Only.*

As we said earlier, you can avoid putting some information in your profile but even if you do include your education and work, current city, hometown or likes, activities and connections, you can control who can see that information.

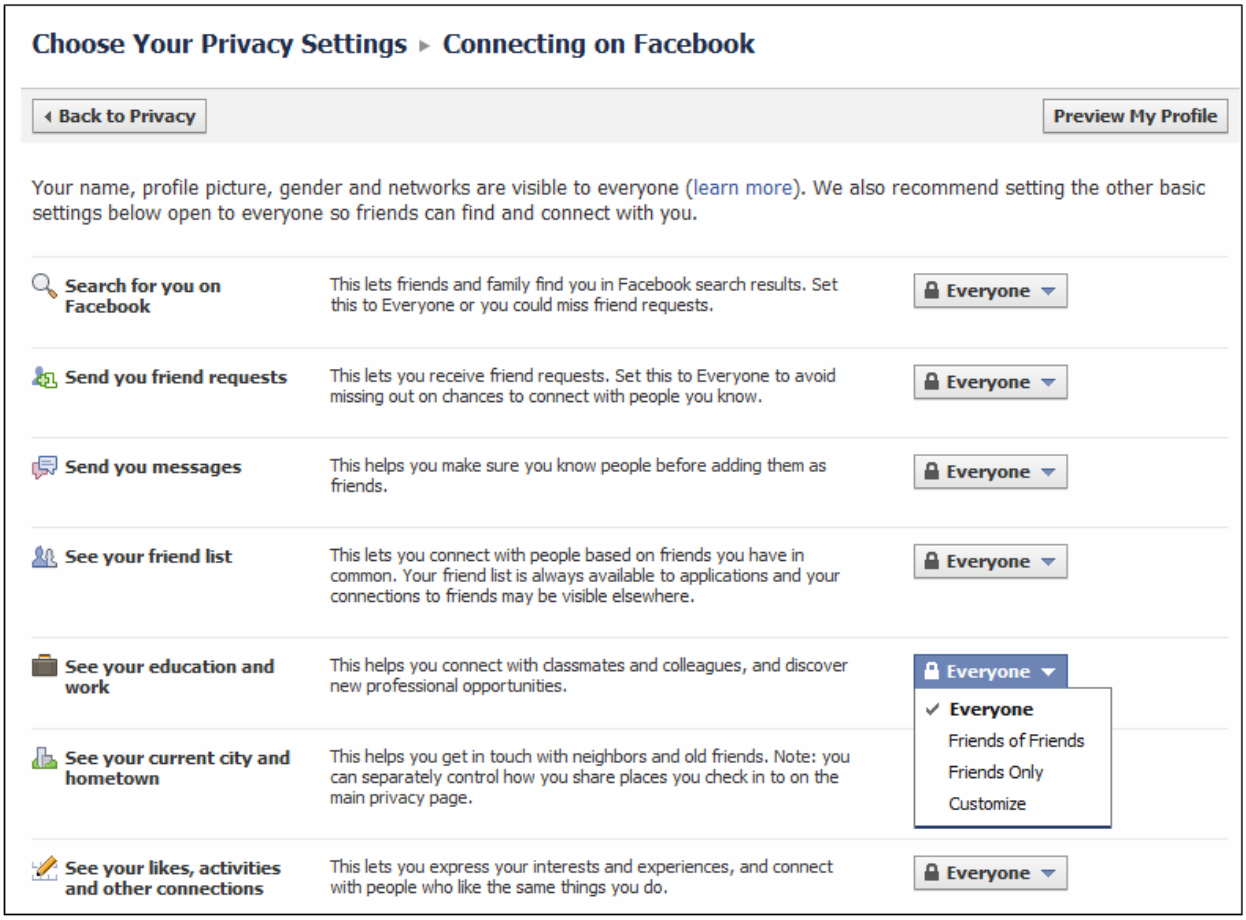
You can also control who can see your friends list and who can search for you on Facebook.

To restrict what people can see

1. Go to privacy settings
2. Click *View Settings* under Connecting on Facebook

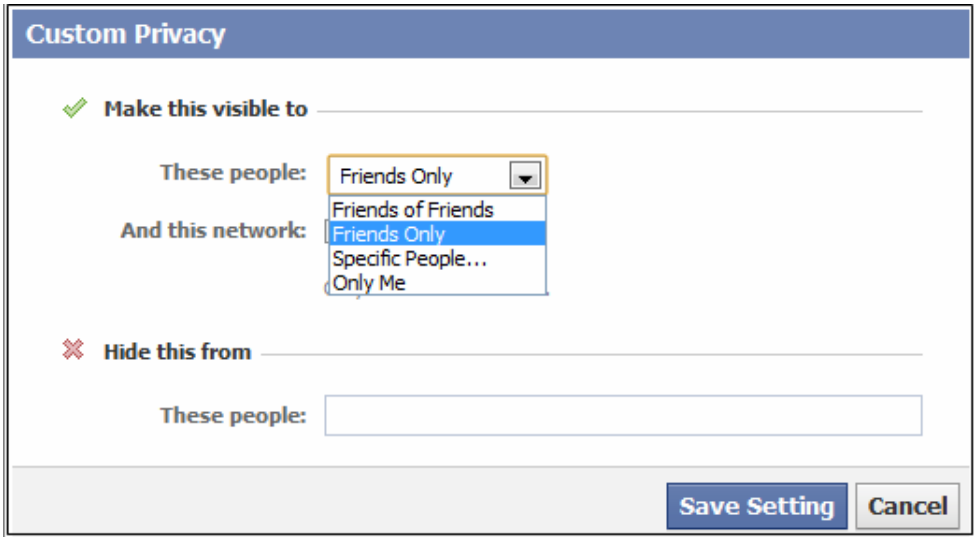


3. Change settings in the drop-down boxes to the right of each option



The Customize option

The Customize option in the drop-down box is a very powerful tool that lets you limit access to information to certain people, Lists or Groups of people or Only Me, which hides it from everyone except you. There is even a way to hide information from specific people or groups of people.



If you click on Specific People, you'll see a box where you can type in the names of the people with whom you wish to share that category of content. Only those people will be able to see it. Likewise, if you type names in the Hide this from box, you can prevent those people from seeing that category of information. If you choose Only Me, you are hiding it from everyone except yourself.

Controlling who can see individual posts

Facebook also lets you control who sees individual posts. So, regardless of your general privacy settings or even your settings by category, you can control who can see each status update, photograph, video or anything else you post right before you post it.

For example, if you're updating your News Feed status, you first type in what you want to say, then – before you click the Share link – click the little lock to the left of Share, and you will see the familiar drop-down box that lets you decide who can see that particular piece of content. As of this writing, Facebook was experimenting with ways to make this feature a bit easier to find, so what you see may be a bit different from the following screen shot.



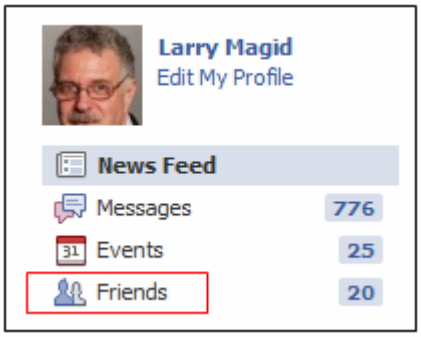
You can control who can see each individual post, photo or video.

Lists: A powerful privacy feature

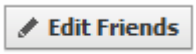
One of the most powerful Facebook privacy features is the ability to create specific Lists of Facebook Friends. Once you've created a List, you'll be able to aim information only to the people on that list (in effect, a "white list"). You can also block people on a list. You could, for example, have a list of just your close friends and relatives. You could have another list of people you're inviting to an event so only people on that list get photos from the event (and those not invited won't feel left out).

To Create a List

1. Go to your Friends page by clicking on Friends in the left column of your home page (below your picture)



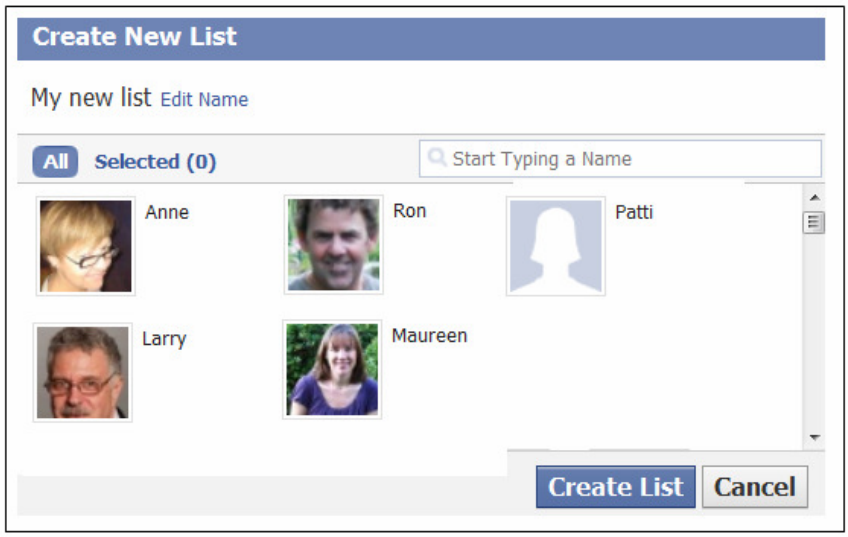
2. In the middle column (just below the blue status bar), you'll see a button called Edit Friends. Click on that button.



3. Click on the + Create a List button, just below the blue status bar.



4. Give the list a name and start typing the names of the people you want in that list, then click Create List when you're finished.



Now, when you type in content, you can click Customize and type in the list name. You can also go back to your privacy settings, click Customize for any category and type in that list name to restrict access to just people on that list. Later, you can add or remove people from the list.

Using the Groups feature

Another option is to create a Group. A Facebook Group is different from a list, because a Group is separate from the main Facebook grid. When you create a Group, you're the administrator of it, and you can limit status updates, photos, videos and any other content to only people in that Group. Groups can be any subset of your Facebook friends such as members of your family, a sports club, schoolmates or any other grouping you desire.

> ***Safety Point:*** *Be aware that any member of a Group can add members, which means that membership can get out of control very fast. The administrator can always delete members, but it can get hard to keep up when/if things go viral, after which it's hard to maintain control over information shared to the group.*

One difference between Groups and Lists is that any member of a Group can add members. All members can see the names of all other members but because any member can add a member, it is possible that people who perhaps shouldn't be in the Group could be added by another member. For example, if you had a Group made up of people on your football team, there would be nothing to stop one member from adding someone not on the team, and then that member could add more people. The only way to keep that from happening is for the administrator to stay aware of the membership list (more on that in a moment). Only administrators can remove members.

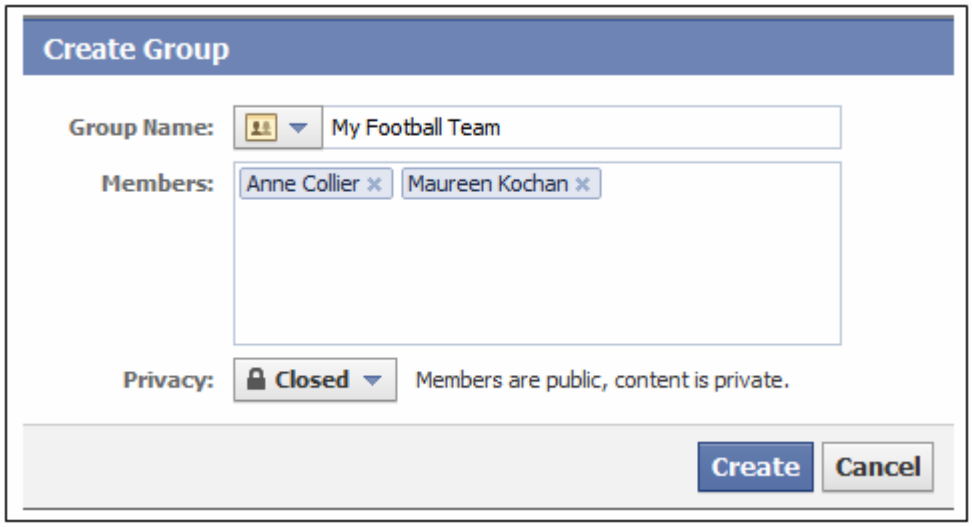
Another important point about Groups is that people can be added to a group who are not on your Friends list and anything you post in that group will be

seen by all Group members, including people who are not your Facebook friends.

> ***Reputation Point**: It's very important that you familiarize yourself with the subjects of Groups (or the type of information shared and whether it's appropriate for your child), because – as you'll see shortly – the names and membership even of Closed Groups can be public information. Users will want to think about how their Group memberships reflect on them.*

To set up a Group

1. The easiest way to set up a Group is to go to www.facebook.com/groups/. Then click on Create Group.

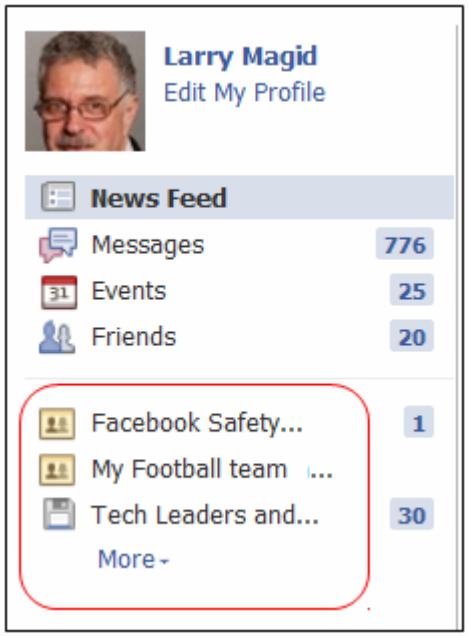


2. Give the Group a name, and start typing in the names of initial members. You can always add members later, and you can also rename the Group.
3. Designate if the Group should be Open, Closed or Secret.

   - Closed (the default) means that the membership list is public but the content is private (available only to members). Also, when you create the Group and add people, that information shows up on your News Feed, so even though others can't join without an invitation, they might know the group exists and who is in it (and maybe feel left out).
   - Open means that both the content and membership are public.
   - Secret (the most private) hides both the members' names and the content.

Safety, Privacy & Reputation Point: *We recommend that young people seriously consider making their Groups secret. They can still invite their friends, and members can still add other friends, but this allows for better privacy and possibly less peer abuse because the Group and its members won't show up on a Facebook search or in someone's News Feed.*

The list of Groups that you are in (regardless of who created them) is in the left column of your Home page.



Your Facebook Groups are listed on your home page.

Seeing who is in your Group

You can always see who is in any group you are in by clicking on the Group name in the left column of your Home page.

After clicking on the Group, click See All for a complete list of members. This is also the place where you can add members or leave the Group. Administrators can remove members of the Group.

Photos and tagging

With more than 4 billion photos posted on Facebook each month, photo-sharing is one of the most popular activities on the site, and tagging each other in photos is how users share photos on the site. Some teens rush home from school to find out how many photos they've been tagged in (Facebook says tagging is what "brings photos to life").

Tagging can be a good thing, because it helps you find pictures of yourself and others you care about, but there may be times when you want to "untag"

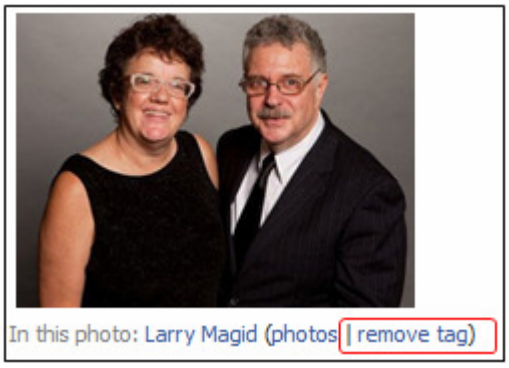
yourself from a photo to remove it from your profile and make it a bit harder to find. That can help you dissociate yourself from the photo, but it will not actually remove the photo from someone else's profile.

Only Friends can tag each other, and Facebook notifies users when they've been tagged. If they untag themselves from the photo, it will no longer be on their profile and may be harder to find via search, but untagging does not remove the photo from Facebook or the Web. Only the person who posted the photo can fully remove it, so if you want a photo removed, you'll need to ask the person to take it down. This illustrates why safety and reputation management is a shared experience on the social Web.

> ***Safety and Reputation Point:*** *In most cases photo-sharing and tagging are fine, but sometimes photos are used to embarrass, harass or cyberbully users. Tagging people in embarrassing photos can hurt their reputations and relationships with others. Disrespectful or unkind use of others' photos can be reciprocated, so it's good to remind your children to be respectful of others when they post photos – for their own and others' safety and reputation protection.*

To untag a photo

1. Click on Profile and then Photos.
2. Navigate to the Photo you wish to untag (the most recent are on top).
3. Click on the photo and check click on Remove tag next to your name.



To limit who can tag you

1. Go to your Privacy Settings page and select Photos and videos I'm tagged in in the Things Others Share section.
2. Change the setting to Friends Only or, to completely remove the ability for others to tag you, go to Customize and select Only Me.

As Facebook is making it increasingly easy to tag people, users need to be increasingly mindful of how and who they tag when they are being tagged themselves.

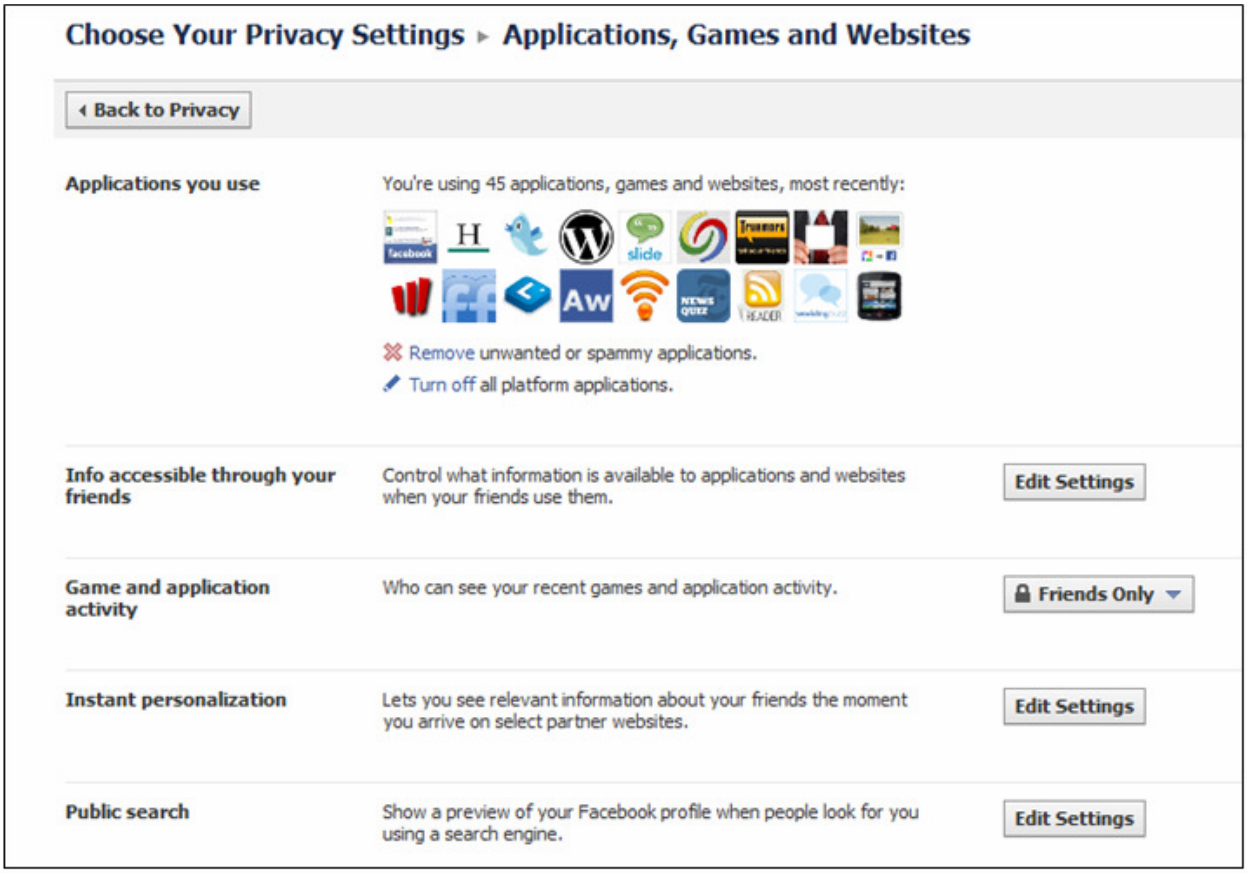
Reputation and Privacy Point: *Untagging a photo or preventing people from tagging you in photos doesn't remove pictures of you or prevent people from posting them. Anyone can still post any picture they want. It's also possible for people to include your name in a photo caption or a comment on a photo.*

Controlling Facebook applications

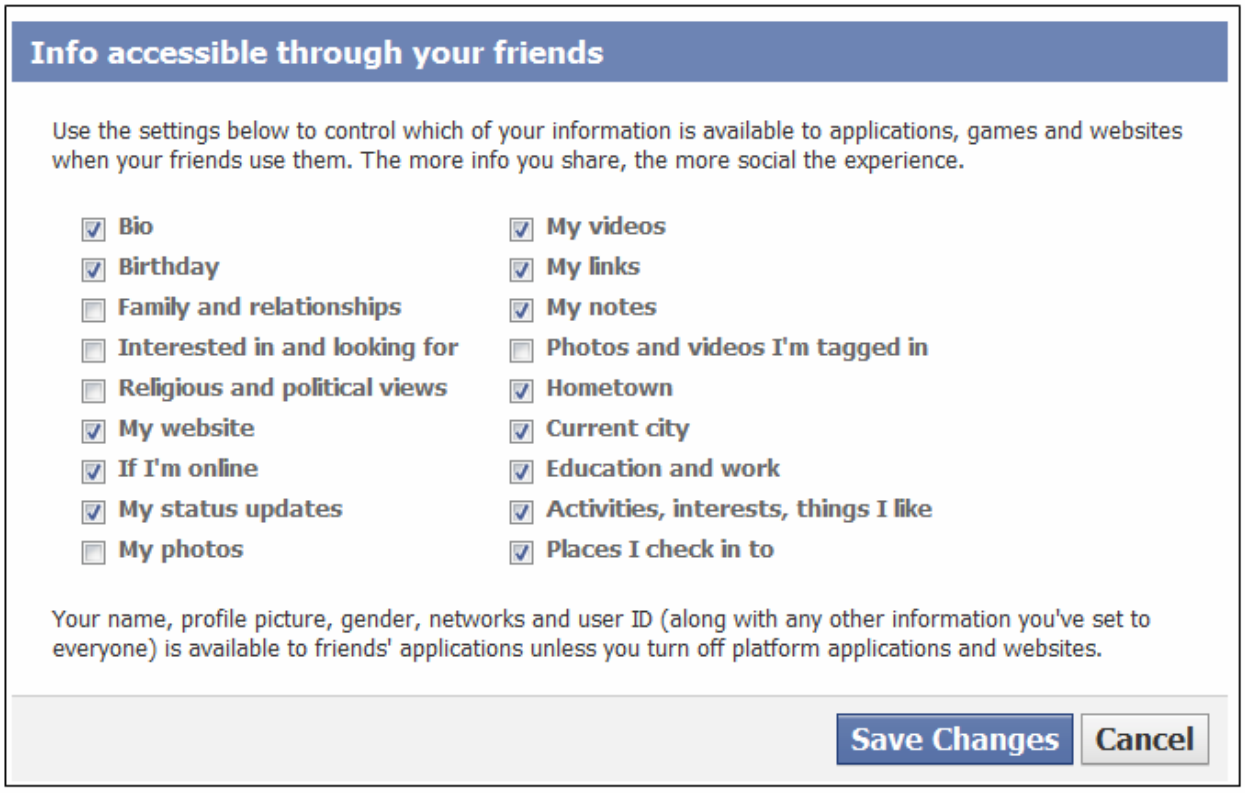
Facebook is home to many applications or little software programs that work within the service. Apps can be games, information services, quizzes or almost anything else that can be programmed on a computer. It's important to know that app developers can sometimes have access to your Facebook information, and there are some games that are able to share some of that information with your friends or others who play the game. But, as with other aspects of Facebook, you have control over what information they can access.

You can get to the Applications, Games and Websites setting page by clicking Edit your settings just below Applications and Websites at the bottom of the Privacy Settings page.

At this point, you'll see a page that allows you to adjust the overall settings for Applications, Games and Websites as well as the setting for each individual application.



For example, you can adjust what information is available to applications when your friends use them. Facebook says, "The more info you share, the more social the experience," but the other side of that is that the more you share, the more information you're giving out about yourself. It's a good idea to think about what information you want your children to share and be sure they limit it accordingly.



The types of information you can allow – or disallow – apps, games, and websites to share about you when friends use them.

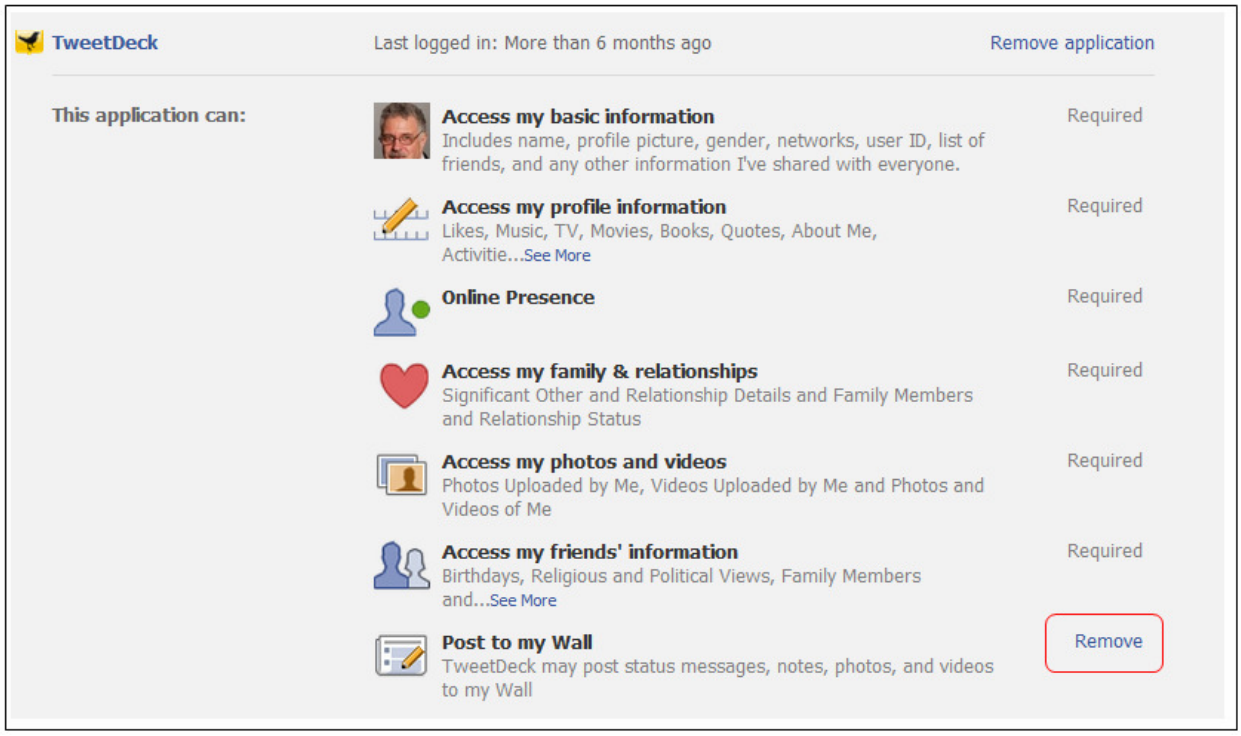
Limiting individual applications

You can also control individual applications. Going back to the Applications, Games and Websites control area, click Edit Settings to the right of the section on Applications you use.

That brings up a screen that lists all of your applications, and next to each is another Edit Settings link. Click on any of those, and you'll get yet another screen that tells you exactly what information the application can access.

Most of the information types are likely to be required so, if you're not comfortable with any of those, you'll have to remove the application entirely by clicking on Remove application near the top of that box. There may, however, be some options, such as the Post to my Wall option in the example below. In this case, you can keep the application but take away permission for specific actions by clicking on Remove next to Post to my Wall. If you click on

Remove, the application will continue to work, but it will no longer post to your wall.



Facebook lets you control what individual apps can access and post.

Facebook's location-sharing Places

Facebook Places is a service that uses the location services built into some mobile phones to "place" you in a specific location. Places isn't available in all countries and on all phones but – where it is available – it takes advantage of the GPS chip and other location technologies built into modern phones to automatically locate where you are.



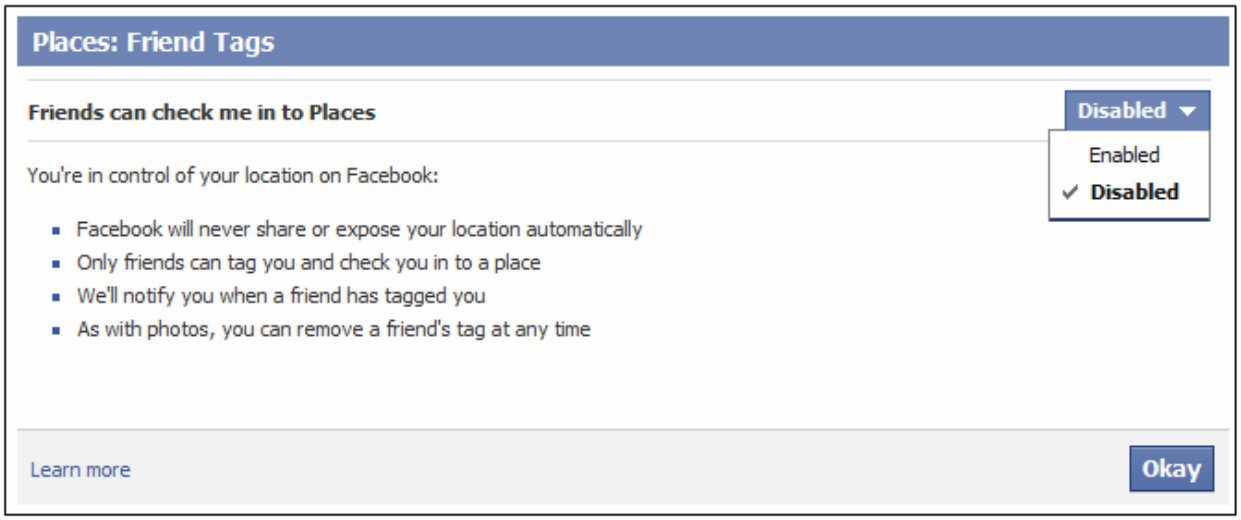
Facebook provides location-sharing for the iPhone (shown here) and other smart phones, so talk with your teens about whether they should share their physical location when mobile and, if they do, only with people they trust.

Not fully automatic

The first thing to know about Places is that it's not fully automatic. You have to "check in" yourself or be tagged by someone else at a location for Facebook to display where you are.

Disabling Places

Even if you don't use Places, there is the possibility that others could tag you at a location, and if you use it even once, there is the possibility that a friend would check you in to a place or location. The best way to prevent others from both tagging and checking you in is to disable Friends can check me in to Places. You do this in the Things others share section of your Privacy Settings. Click on the Edit Settings link to the right of Friends can check me in to Places and make sure it is Disabled.



You can disable friends' ability to check you in or tag you at a location.

> ***Safety Point**: Because physical location is a particularly sensitive issue, Facebook, by default, only shows your location to people designated as Friends, even if you have more open privacy settings for posts or other types of information. This is a helpful safety measure for teens, but we recommend that children under 16 disable Places.*

Special provisions for minors (under 18)

If a Facebook user is registered as under 18, the following restrictions are in place:

- Only his or her friends will see that the minor is checked in to a place. There isn't even an option to extend that beyond Friends.
- A minor's name will not be seen on an establishment's Here Now page by anyone other than his or her friends.

***Safety Point**: It's important to know that, once you've used the Places service and agreed to its terms, any of your Facebook friends can check you in to a location. That displays that you are there, just as if you had checked yourself in. But you can prevent this from happening by editing the default setting in "Friends check me in to Places" in the "Things others share" section of your Facebook customized privacy settings.*

Being Checked In or tagged

If you are Checked In or tagged by a friend, your presence at the location is seen by your friends and whoever the person who checked you in allows to see his or her posts, subject to their (not your) privacy settings.

The difference between being checked in and being tagged can be confusing. If you're checked in by yourself or by a friend, your presence at the location is visible to anyone who either you allow or your friend allows, based on your friend's and your privacy settings. For adults, your name will show up on the location's Places page and be visible by everyone. Minors who are checked in will also show up on that page, but their name will only be visible to their Facebook friends. If you are tagged by a friend, your presence at the location is seen by your friends or whoever they allow to see their posts, subject to their (not your) privacy settings.

***Privacy & Safety Point**: The only way to prevent being tagged or checked in with Places is to go to your Privacy Settings page and disable Friends can check me into Places.*



You can disable being seen in locations' "People Here Now" page.

To control who can see the places you've checked in

1. Click on Account in the upper-right corner
2. Click on Privacy Settings
3. Select Customize Settings.

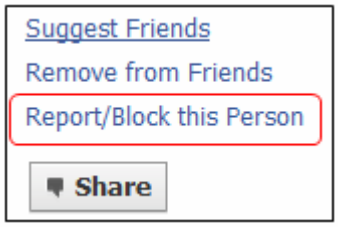
To the right of where it says Places I check in to, it probably has the default setting of Friends Only. You can change that by selecting another option. One of the options is Customize, which lets you further limit who can see your location to specific people, lists of people, or even Only Me. You can also opt out of People Here Now (which allows businesses to display who is at their establishment at that time) by unchecking Enable.

Reporting problems

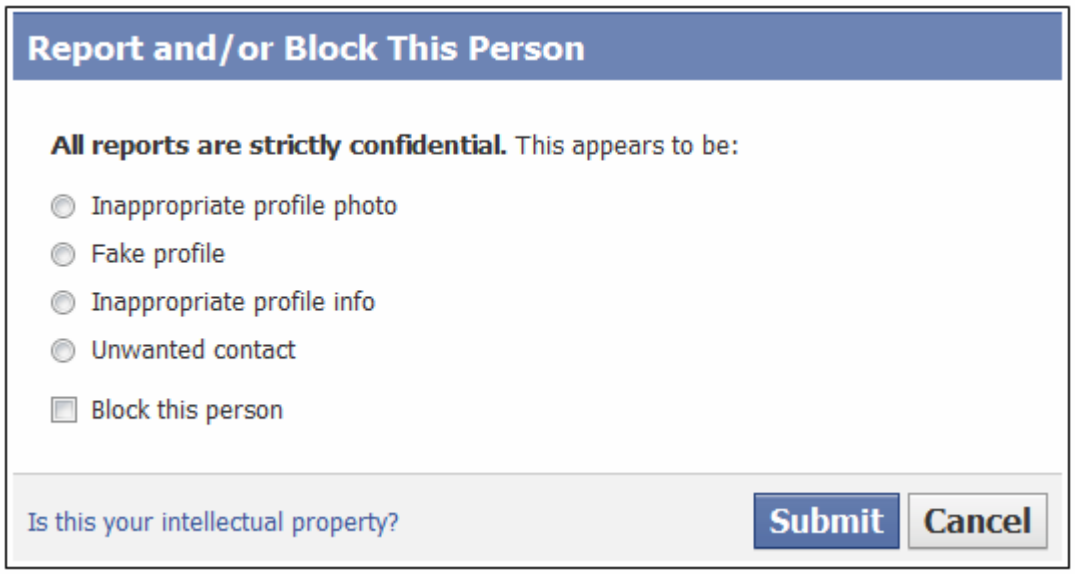
There are multiple ways to report problems and abuse on Facebook, depending on whether it's a specific piece of content (like a photograph) or a user's behavior.

> ***Safety Point**: If you or anyone you encounter online appears to be in immediate danger from another person or something they might do to harm themselves, call the appropriate authorities immediately. In the U.S., for example, you would call 911.*

If there is something a user is doing that you think violates the law or Facebook's terms of service, you can file a confidential report on any Facebook member by going to their page and down to the bottom left corner and clicking Report/Block this Person. That form can be used to report an inappropriate profile photo, a fake profile (the person is misrepresenting him or herself), inappropriate or offensive information on the profile or unwanted contact from that person.



You then give a reason why you are reporting and/or blocking the person (see screenshot below).

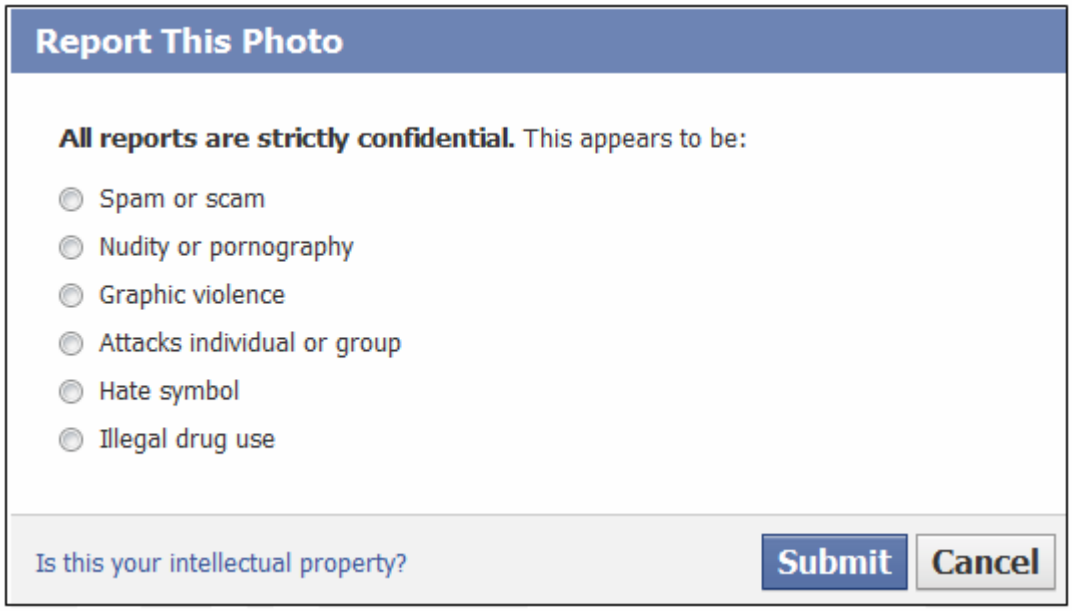


If you wish to Block as well as Report, click the check box next to Block this Person.

You can also report specific content. For example, if you see a thumbnail (small version) of a photo on someone's page, you can click on that photo and, just before it, there is an option to Report This Photo.



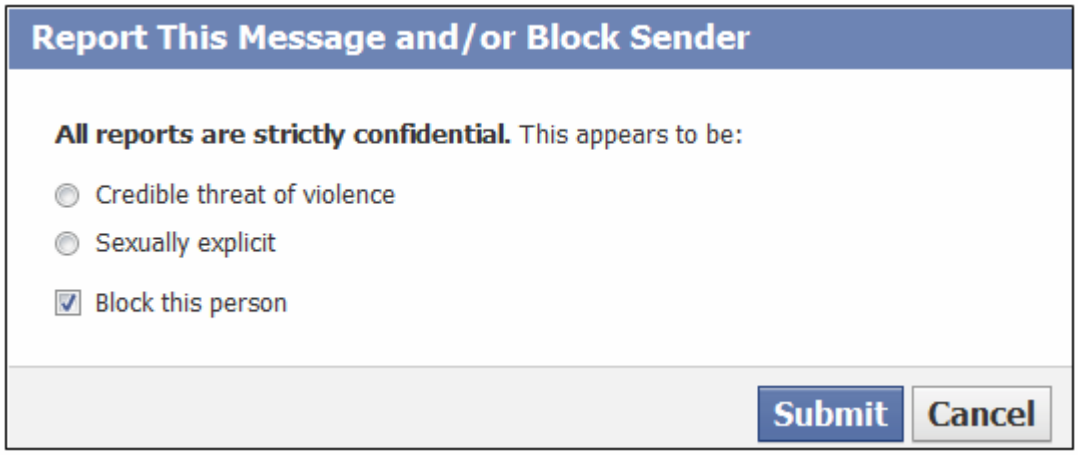
You can then place a check mark next to the option that best describes why you object to the photo.



And you can also report messages that you think violate Facebook policies by clicking Report to the right of the name of the person sending the message.



You can also report offensive messages.



As with reporting photos, you are asked to specify why, and you have the option to Block this Person.

All abuse reports on Facebook are confidential, so the person you're reporting won't know that you've reported them. Facebook will investigate and determine whether or not to remove the content or, in the case of repeat offenders, ban the person from the site.

Facebook says that if there is no violation of its Statement of Rights and Responsibilities, then "no action will be taken."

Preventing suicide and other self-harm

Because Facebook is a reflection of their lives, young people sometimes use the service to reach out for help or to express themselves in ways that indicate they have a serious problem, including eating disorders, drug or alcohol abuse or even suicidal thoughts (here is a list of suicide warning signs: www.suicidepreventionlifeline.org/GetHelp/SuicideWarningSigns.aspx).

If you suspect someone is likely to harm him or herself, contact local law enforcement immediately. You can also contact a helpline. For example, in the United States you could call the National Suicide Prevention Lifeline at 800-273-8255. The Lifeline offers free 24-hour support seven days a week. You can find information on suicide prevention hotlines in other countries at www.befrienders.org/.

If you see something on a person's profile that indicates that he or she is engaged in dangerous activity, see if you can find appropriate ways to reach

out. There are agencies in almost every country that provide information on and help for a wide variety of risky or self-destructive behaviors.

Facebook has a Help page on suicide that provides a link to where you can report suicidal content to the site. You can find it by searching for suicide in the Help Center or by going directly to www.facebook.com/help?faq=15538.

CONCLUSION

By now it should be clear that Facebook is a giant social networking site providing a large, diverse array of services and features. It is also a reflection of and platform for the thoughts, actions, creativity, and learning of a large cross-section of humanity. How people use the site is very individual, and keeping their experiences on the site positive depends a great deal on how they use it and interact with others on it. This is just as true for young Facebook users as it is for grownup ones.

Because Facebook use is based on real names and identities, it's directly tied to "real life" – in the case of young people, mostly school life and relationships. So, just as in offline life, children need their parents' help as they navigate both adolescence and the social Web. You can help them understand...

- How important it is for their own online well-being to be mindful of what they say, share, and upload (as well as send on mobile phones)
- How smart it is to present themselves in a positive light online
- How much better their online experiences will be if they stay on good terms with others in their online as well as offline communities.

We hope this guide helps you, fellow parents, to support your children's positive use of this very popular part of their lives, Facebook.

*"A Parents' Guide to Facebook" is online at **www.fbparents.org**, and our policy for reprinting or reposting content is at www.connectsafely.org/reuse.*

***About the Authors**: Anne Collier and Larry Magid are co-directors of ConnectSafely.org and co-authors of* MySpace Unraveled: A Parents Guide to Teen Social Networking. *Both served on the Obama Administration's Online Safety & Technology Working Group, for which Anne served as co-chair and Larry as chair of the education subcommittee. Larry is also founder of SafeKids.com, technology analyst for CBS News and has contributed to the BBC World Service, National Public Radio, the New York Times, Los Angeles Times, CNET and Huffington Post. Anne is also founder and executive director of the nonprofit organization Net Family News, Inc., and editor of NetFamilyNews.org. Until 1997 she worked on the print, radio, TV, and and Web editions of the Christian Science Monitor.*

© 2011 ConnectSafely.org and iKeepSafe Coalition (Rev. January 3, 2011)