Tennessee v. Meta
Case No. 23-1364-IV

DX3535

A Parents' Guide to

Facebook

(Revised 2012 Edition)

By Anne Collier and Larry Magid

Co-Directors, ConnectSafely.org



ConnectSafely
Smart Socializing Starts Here™

iKeepSafe
PEACE OF MIND FOR FAMILIES ONLINE™

February 2012 (Rev. 2/18/12)

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
  - Social reporting 5
- Why children should be honest about their age 5
- How do we parent Facebook users? 6
  - Ways to monitor your child's Facebook activities 7
  - Scams, spam, phishing and social engineering 7
- Managing reputation in the digital age 9
  - Digital footprints & good reputations 10
- Your children's timelines are a reflection on them 10

HOW TO OPTIMIZE FACEBOOK FOR YOUNG PEOPLE 11
- How Facebook is organized 11
  - Timeline 12
  - Friends 17
  - News Feed 17
  - Subscribe 18
  - Photos and tagging 18
  - Apps 21
  - Lists 23
  - Groups 23
  - Messages 24
- Managing your privacy on Facebook 25
  - Special safeguards for teens 26
  - Facebook's new, simplified 'inline' privacy settings 27
  - Customizing who you share with 28
  - Limiting who can find you in search 28
  - Default privacy from apps that don't have inline controls 29
  - Download your whole Facebook history 29
- Facebook for mobile 30
  - Checking in to a location 30
  - Being checked in or tagged 31
- Reporting problems 32
  - Reporting a person 33
  - Reporting specific posts 34
- Preventing suicide and other self-harm 34

CONCLUSION 35

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 If you find anything in the guide that is out-of-date, please send an email to admin@connectsafely.org.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 800 million active users 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 250 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 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 for all Facebook users with special areas 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 negotiation between users (for example, between people in a family photo posted by one family member in it), 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 on the site.

What are the risks involved in social networking?

Youth-risk research has made five key findings:

1. Young people who behave aggressively online are more than twice as likely to be victimized online, so children's own behavior on Facebook or any social space online or on phones is key to their well-being there.
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 physical environment (for example, home and school) are better predictors of risk than any technology 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 quickly. 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...

- Harassment or online bullying ("cyberbullying") on the part of your children or others'
- Posting information about themselves that: a) could be used to embarrass or manipulate them; b) could cause psychological harm; c) could be used by criminals to steal their identity or property or – though very rare – determine their physical location to cause physical harm
- 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
- 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 on 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).

Social reporting

Later, in the "Reporting problems" section, we talk about how Facebook's new social way of reporting problems works, but we'd like to highlight it here as well because it's one of the best ways to deal with some of the issues we're talking about here. Social reporting is Facebook's way of letting users reach out to people in their lives to help solve problems – from minor issues like a photo of them they don't like to comments that may be annoying or inappropriate. Sure, there may be times when we need help from Facebook's support staff or even law enforcement, but the vast majority of cases are about interactions in offline life, where it's usually the people involved (or others in their lives) who resolve an issue. That's why Facebook has created a way for you to reach out either to the person who posted something you're unhappy with or others (such as friends or family) who might help resolve something.

Why children should be honest about their age



Facebook requires users to enter their real birth date. If they're under 13 and truthful about their age, they won't be allowed to sign up. Facebook has some special protections for people under 18.

When you set up a new Facebook account, one of the first things you're asked to do is give your full date of birth. This is the only time that's required, and we recommend that it's the only time teens provide their birth year. 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 publicly.

Because of the extra protections Facebook provides 13-to-17-year-old users (see below for details), we recommend that people be truthful about their age when they set up their account. There are legal reasons why Facebook restricts membership to people 13 and older, but in addition to complying with U.S. law, Facebook has created an environment designed 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, there's a certain reality we all face. When we hear from our children that "all" their friends are on Facebook, there could be some truth to that. 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 in today's social media environment. If you have children under 13 who are on the service, we recommend 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, to "friend" them or otherwise unobtrusively monitor their Facebook use and talk about how safety and privacy are a responsibility they and their friends share. Read on for how you can do that.

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 see or hear about youth on Facebook or in the news media, which often present a very negative picture. Adults who don't understand social media sometimes think of 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 – which is what Facebook is all about for most teens. So the context for what happens on Facebook is really their lives, especially school life, not really Facebook (why we brought up "social reporting" right up front).

It's not an add-on to "real life." For teens, Facebook use is much more a tool for conducting their social lives than a separate or additional activity. 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.

Ways to monitor your child's Facebook activities

If you haven't already, 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. After that, you can establish a family rule that says something like, "No one can block other family members from content any of us posts on Facebook." For parents' part – if you and your kids do become Facebook friends – resist the temptation to make public comments on their pages; that might embarrass them, which can create an unwanted communication barrier between you and your child. 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 reluctant 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 online reputation-monitoring services, which can help you find out what your teen is posting online without your having to friend them on Facebook. Some of them charge a monthly fee.

Scams, spam, phishing and social engineering

This guidebook is mostly about young people's use of Facebook, but we would be remiss if we didn't mention the security of the devices and networks they use to access the service. Facebook itself is relatively secure but, for the simple reason

that so many people around the world are using it, there are scam artists who target people on Facebook just as they do in email and on many other sites.

On Facebook and everywhere else in digital media, critical thinking is your best defense. If something is too good to be true, it's too good to be true. If a message from a friend sounds a little strange, it might be someone posing as your friend. Don't be "socially engineered." Scams are called "social engineering" because they use tricks, not sophisticated technology, to get you to take some action that could jeopardize your security or privacy.

These security threats are not unique to Facebook, but Facebook users need to be aware of them. Here are some examples:

- **A "phishing attack" could** be an email message with a link to what looks like the Facebook log-in page but is really an imposter page that records your username and password so the phishers can use your account to send spam messages or malicious links to your Facebook friends, etc.
- **Malicious programs** like Koobface can spread via spam email and Facebook messages that encourage you to click on a link or download malicious software ("malware").
- **"Clickjacking" and "Likejacking"** use links too. What may look like a Facebook post with a link to tantalizing content could redirect you to a site that plants malware on your device or posts bad links on your own Facebook profile that make it look like you "like" a Web site or someone else's post. It can also trick you into revealing confidential personal information. If someone asks you to copy and paste some text into your browser window or to modify your browser settings, it could be a trick. Don't do it.
- **Fake apps**: We sometimes hear about apps or programs that do things not supported by Facebook, such as, "see who viewed your timeline." Be alert and avoid using them!
- **Money transfer scams**: If you hear from a friend who says he or she is stuck in some far-away place and needs money for a flight home, that friend's Facebook account was probably hacked. Before sending money, give your friend a call to check it out! That goes for "charities" seeking donations, Nigerian-type scammers looking for help with transferring large amounts of money, and contests offering big winnings if you "click here."

A little critical thinking goes a long way. Friends and family members can look out for each other. Encourage your kids to talk to you or each other if something seems sketchy. If you think your account has been hijacked, go to www.facebook.com/hacked to report a compromised account. And last but not least, be sure you're using up-to-date security software on your computer and make sure your computer (or smart phone) operating system and any apps or programs you're using are up-to-date. For more information, go to www.facebook.com/security.

Managing reputation in the digital age

Before we go into detail about Facebook features, some context on what it means to socialize in a digital media environment might be helpful. We'll provide a bit of that background in this section and throughout, in the form of key parenting points for guiding young social networkers.

The meaning of privacy is changing in today's *very social* media environment. It's not exactly as it was when we were children. It's more about the context in which information is shared. Rather than being either entirely public or entirely private (which defeats the whole purpose of socializing online), people want to have control over their *level* of privacy as well as how much and to whom they're sharing.

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 and one person's content and photos – even location – often appear on other people's pages and vice versa, as we mentioned above, safety and privacy in social media are also a shared experience – a negotiation. It's simply impossible for one person (your child or *you*) to have complete control over what 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 on Facebook is very grounded in their "real world" relationships, peer groups and school life and rarely has anything to do 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 stop or end the distribution of 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 just Friends, 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 someone's name into a search engine and there's a good 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. Web pages, blogs, photos or status updates about their accomplishments in school or sports, for example, can improve their public 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 counterbalance it.

> ***Reputation Point**: 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.*

Your children's timelines are a reflection on them

Like the clothes you wear, the music you like, or the company you keep, your Facebook profile (now called timeline) is a representation of you online. Along with your profile photo or image and the photos of you that are shared by friends, your timeline 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 also multimedia, it's about all aspects of your life – and it can be 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 anything – about what their sharing says about them and who sees it. Working through the how-to's in the following section will help you think this digital self-representation through together right now, but it's also a good idea for everybody to revisit those settings as they change or 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 page, "Like" something, 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)!*

HOW TO OPTIMIZE FACEBOOK FOR YOUNG PEOPLE

This section is a how-to guide for safe, positive Facebook use. It's written with an eye to protecting young people in three key areas: safety, privacy, and reputation. If you have any questions about settings or features not covered here, 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, it's for you too!

How Facebook is organized

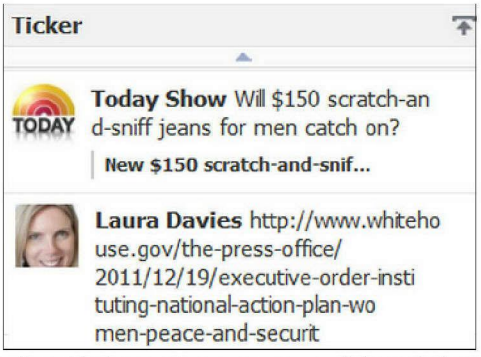
When you sign in to your Facebook account, you may notice your name in the upper right corner and the word Home to its right. There may be other options in this corner too, but everyone has these two. Clicking on your name brings up your Facebook timeline, and Home brings up your home page. Generally speaking, timeline is more about what people see of you, and Home more about what you see of others on Facebook.



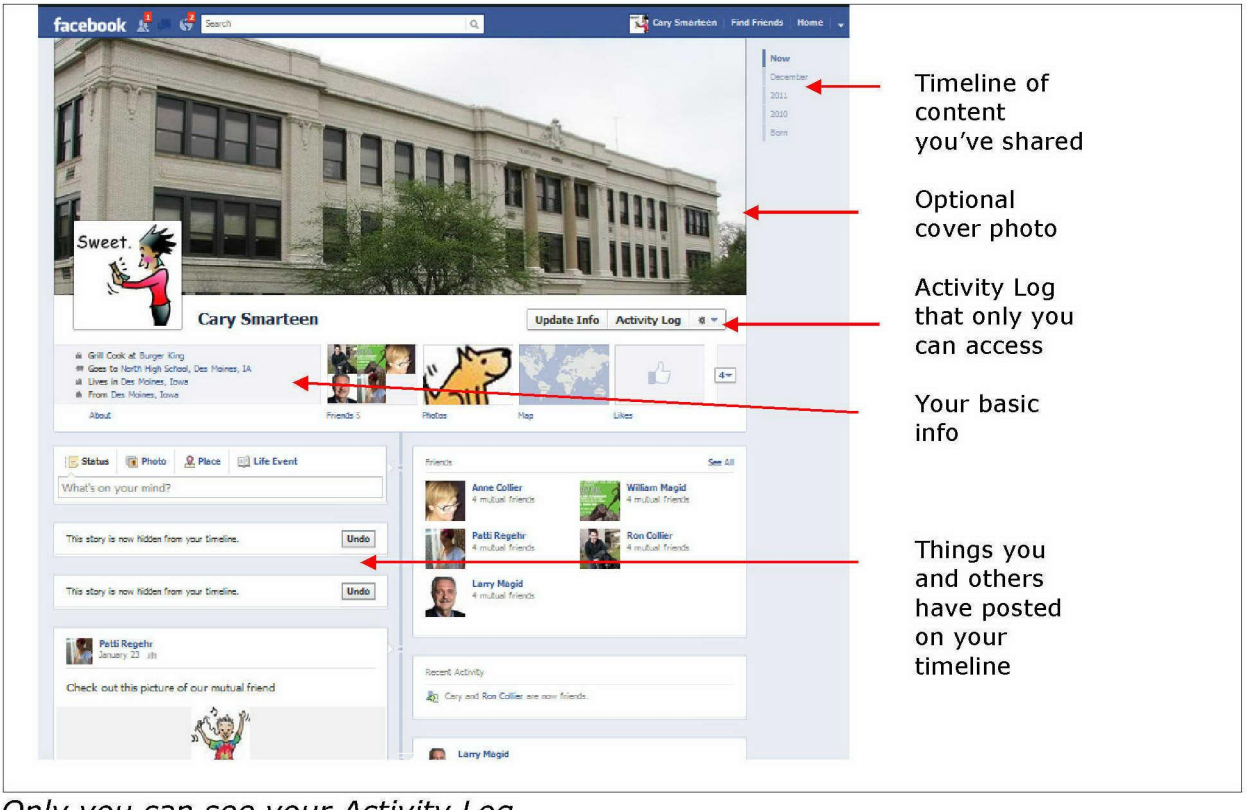
Facebook Home page is organized into three columns.

Your home page is organized into three columns. In the middle column is your News Feed, which is all the things that your friends and others you connect with are saying. The left column is a dashboard of sorts. By default, it's set to News Feed, but the second option – Messages – changes the middle column to display messages between you and others on Facebook. Below that is a link for Events that shows events that might interest you. Next comes Lists (more on that later), as well as pages from businesses and organizations that you follow and any apps you've installed or groups you belong to. If some of these don't make sense yet, they will by the time you finish this guide. The right column contains links to people you may know, including people Facebook suggests you might want to friend (based mostly on Facebook friends in common), advertisements and a ticker with up-to-the-minute updates from your friends. You can hide the ticker by clicking on the arrow at the top right.

At the bottom of the right column is a Chat area where you can have a live text or video chat with friends who are online at the same time you are.



The ticker shows your friends' posts in real time, as they post them. You can hide the ticker by clicking on the arrow in the upper right corner.



Only you can see your Activity Log.

Timeline

What used to be called your Facebook "profile" has been updated and is now called "timeline." On the right side of that page are the years of your life (you can add events that predate when you started using Facebook), which gives people the ability to go back and look at highlights, including pictures and posts that you've shared on the service. The visibility of this timeline is subject to your privacy settings and who you choose to share the information with.

***Privacy Point**: Facebook gives you lots of control over what appears on your timeline, including the posts and activities presented by year in the little timeline on the right-hand side. We encourage users of all ages to curate that timeline thoughtfully – at least go through it and see how public each entry is – because this feature makes it a lot easier for people to find old posts and activities of yours, and maybe you and your kids want to leave some parts of your past behind!*

In addition to your Facebook profile photo, you have the option to display a "cover photo" that says something about you or your interests.

Your timeline (often called "wall" as well as "profile") also features content that others have posted. This can include text, photos, videos or links to Web sites. Even though it's content from other people, it's a reflection on you (or your child), so it's important that people check in on their timeline and delete any posts they don't feel are appropriate.

Controlling or removing what others post

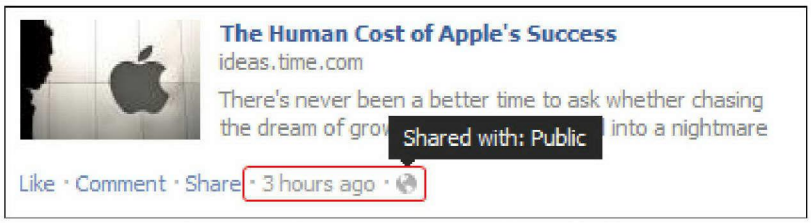
Only you and your friends can post on your timeline. To turn off your friends' ability to post, click the little down arrow on the top right of your screen and select Privacy Settings. Then click Edit Settings next to How You Connect and click on Friends next to Who can post on your timeline? to change the setting to Only Me.

You can hide or delete any posts to your timeline at any point. Hover over the post till you see a little pencil to the right and then click on that pencil and select Delete Post, Hide from Timeline or Report/Mark as Spam. You can also delete comments on your timeline by clicking on the X to the right of the comment.

Who can see your comments to posts

If you comment on someone's post, anyone who has access to that post also has access to your comment, regardless of your privacy settings. So if someone posts something that can be seen by "Public" and you comment on that post, your comment can be seen by everyone (anyone on Facebook or even anyone on the Internet).

You can actually see the audience of a post before you comment by hovering your mouse over the audience selector icon (a globe for public, silhouettes for friends, etc.) below the post.



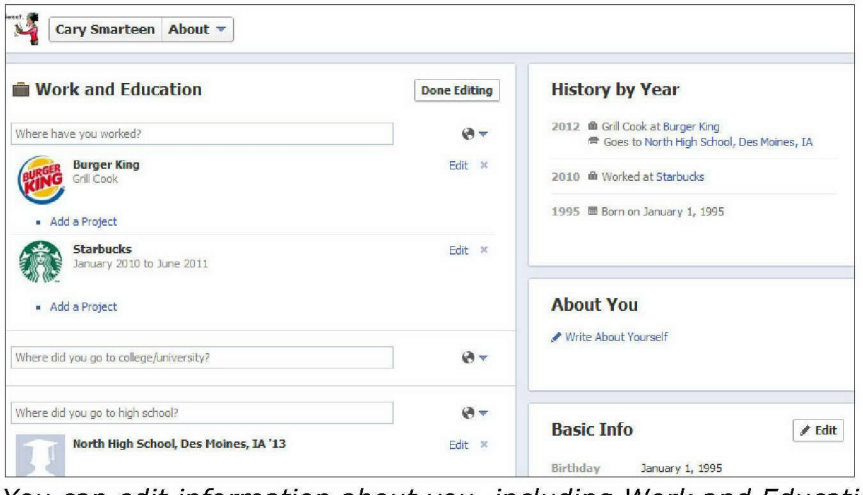
Hover over the audience selector icon below a post to see who else can see it. That same audience can see any comment you add.

Limiting what information is displayed on your timeline

At any time Facebook users can edit their timeline by clicking Update Info near the top right of the page (below the big cover photo, if you have one).



Although Facebook encourages members to add information to their timeline, most of the fields are 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 together what's best to leave blank.

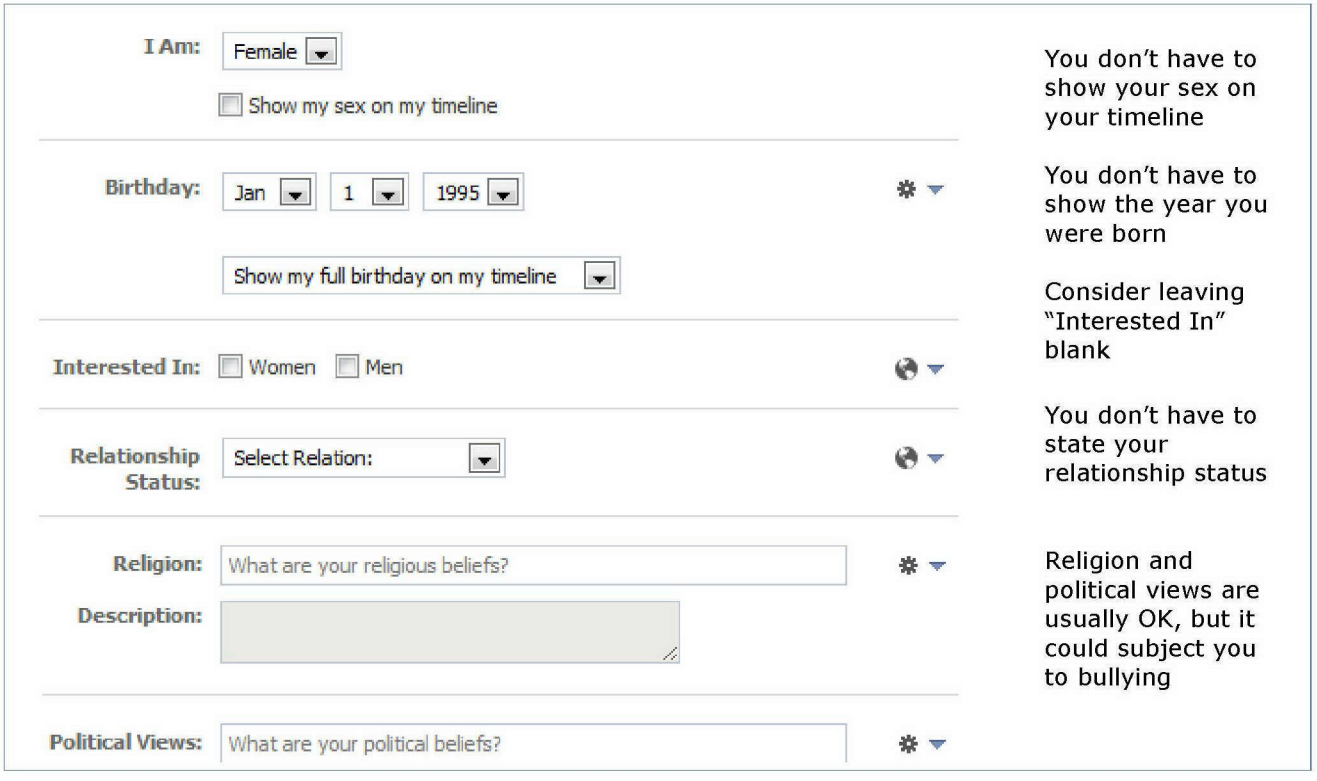


You can edit information about you, including Work and Education, where you live, your Relationships and Family and Basic Info.

The boxes in Basic Info and About You can be great places for a teen to express who he or she is, but help your children think about 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.

Also, put some thought into whether or not it's appropriate to check the boxes next to Interested In and Relationship Status. 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. Relationship Status is where you declare what type of relationship you are in (single, married, "it's complicated," etc.). Talk with your kids about what these settings would look

like to friends, relatives, or strangers, if they checked these boxes. In some cases, even what they enter for religious and political views could make them vulnerable to harassment or bullying.



You can limit what you disclose and who sees it by clicking on the audience selector icon to the right of each item.

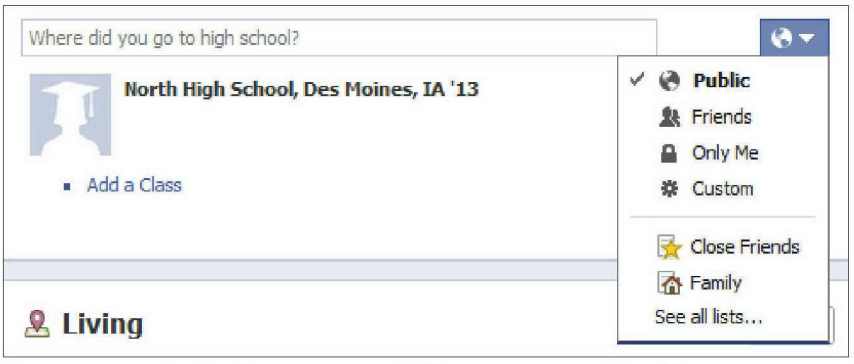
Even though Facebook requires users to state whether they're male or female when they register, the default setting is not to check Show my sex on my timeline – and we recommend that teens leave it that way. The same goes for birth date. As we mentioned above, birthdays are fine but not year of birth.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

Note the down arrow ▾ to the right of each option. It's there so you can decide who can see the information.

> ***Reputation Point:*** *Teens might want to think twice before disclosing their political or religious views. Are those private matters for your family? In some communities, this can be a safety issue too. 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.*

Controlling who sees each timeline item

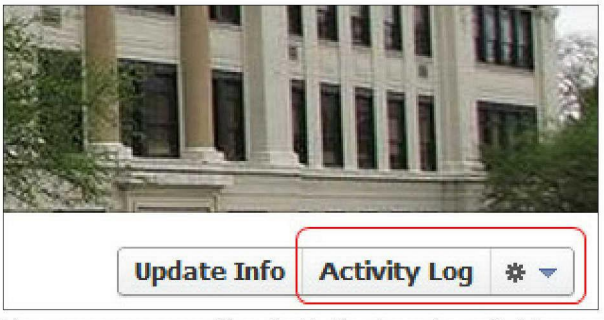
Your teen can control who can see any item in their timeline by clicking on the audience selector icon to the right of each listing.



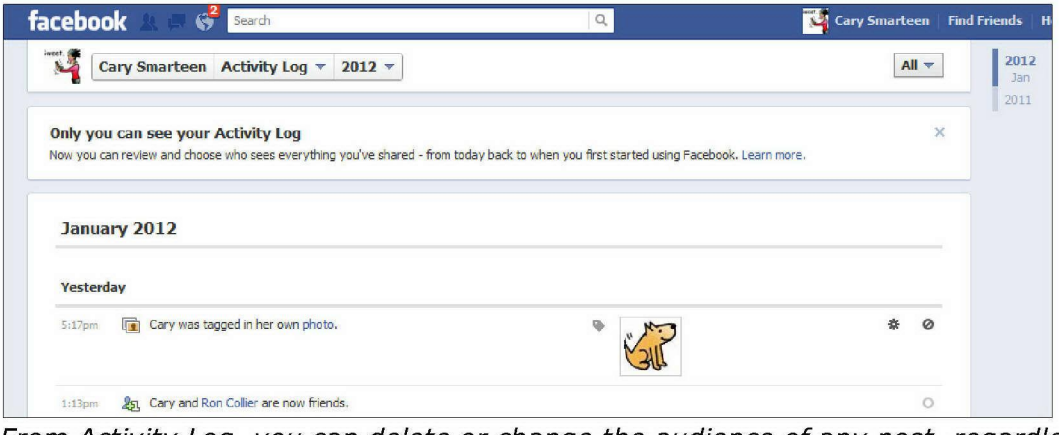
You can control who sees each item on your timeline.

Activity Log

Your Activity Log, which only you can see, is a great tool for reviewing everything you've ever shared on Facebook since the day you opened your account. Not only can you see everything, you can also go back and adjust the privacy settings for each "story" or post – or delete it entirely. If it's something you want to keep but not share, consider changing the setting to Only Me by clicking on the audience selector icon to the right of the activity and changing the setting.



You can access the Activity Log by clicking on your name in the blue bar to the top right of the screen and then Activity Log just below the cover photo.



From Activity Log, you can delete or change the audience of any post, regardless of how old it is. Notice the down arrow to the right of "All" in the upper right corner. Click on that to review a specific category (posts, photos, etc.).

See how your timeline looks like to others

It may help young Facebook users to know how their timeline looks to other people. You can do that by clicking the down arrow to the right of Activity Log, selecting "View As," and then typing in the name of a friend to see how they see your timeline.

Friends

Shortly after you or your teen has been on Facebook, 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 be in touch with, you'll probably want to Confirm the person as a friend. But if you don't know that person offline or if for any reason you don't want to communicate with them on Facebook, you can click Not Now, and they will not be added. And if you choose not to add them, don't worry, they won't get a message saying you haven't added them.



When you get a friend request, you have the option to confirm – or not.

Just as you can add friends, you can easily remove them by going to their timeline, clicking on the friends icon at the top of their page and selecting Unfriend. Here, too, they will not get a message saying 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 you can help your kids understand that being kind or civil online isn't just nice, it's protective.*

News Feed

News Feed is Facebook's way of keeping you up to date on the information your friends share. It's a stream of posts that users see on their Home pages – including posts from friends and in some cases friends of friends. Not everything that people post shows up in the News Feed, but a lot does. What posts show up is subject to their privacy settings.

When you post a status update, a photo or any other content, people in your Facebook community will see it on their own home page, subject to your privacy settings. Not everything you post will necessarily be seen by all of your friends. Facebook has software that tries to figure out who you're closely connected with

and displays it on their news feeds. The important thing to remember about this feed is that people can see what you post without having to go to your timeline.

Subscribe

In Fall 2011, Facebook added a new feature called "Subscribe" that enables adults on Facebook to allow others to read their public posts and view their timeline. It's used by a lot of celebrities, journalists and politicians, but any adult can allow people to subscribe to their timeline. Unlike a friend request, the person whose page you're subscribing to doesn't have to accept each new subscriber. Since people under 18 can't post to the public, minors can't let people subscribe, but they can subscribe to other people's timelines. When you subscribe to another person's timeline, the person doesn't necessarily see what you've posted (unless it's directly to them or on their wall), but parents should be aware that teens can use the subscribe feature to keep up with celebrities, other public figures or any other adult who allows others to subscribe. For example, any Facebook member can visit facebook.com/larrymagid or facebook.com/annecollier to subscribe to our pages. You can also visit facebook.com/connectsafely, which is our organization's page on Facebook.

Photos and tagging

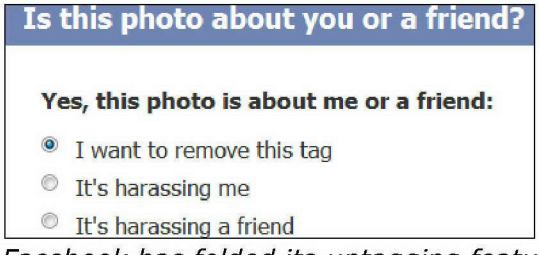
With billions of pictures posted on Facebook each month, photo-sharing is one of the most popular activities on the site, and tagging each other in photos on the site is how users share photos. Some teens rush home from school to find out how many photos they've been tagged in (Facebook says tagging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

Anyone can tag anyone else, and Facebook notifies users when they've been tagged. 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 or remove it from your timeline. Untagging or removing a photo from your timeline doesn't actually remove the photo from someone else's timeline, but it helps to dissociate you from it so that people are a lot less likely to find the photo by searching for you. 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. Facebook gives you the option to do that with "Social Reporting" (more on that under "Reporting problems" below). 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 your timeline and then Photos, which is near the top (below and to the right of your profile picture).
2. Navigate to the photo you wish to untag.
3. **Click** on the photo and then on the gear icon ⚙ to the right of the picture, then select Report/Remove Tag. Even though untagging is part of the reporting process, it does not necessarily generate a report to Facebook, to the person who tagged you or to the person who posted the photo.



Facebook has folded its untagging feature into its reporting tool. Don't worry, by untagging yourself from a photo you're not getting anyone in trouble. You're just removing the tag.

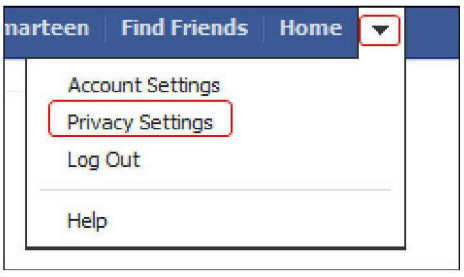
To control tagging of your content

As of Fall 2011, users can now control what happens when people tag you or your content. For example, you can now turn on Timeline Review (which is off by default), which enables you to manually approve posts that you're tagged in before they go on your timeline. Tag Review allows you to review any tags your friends add to *your* content before it appears.

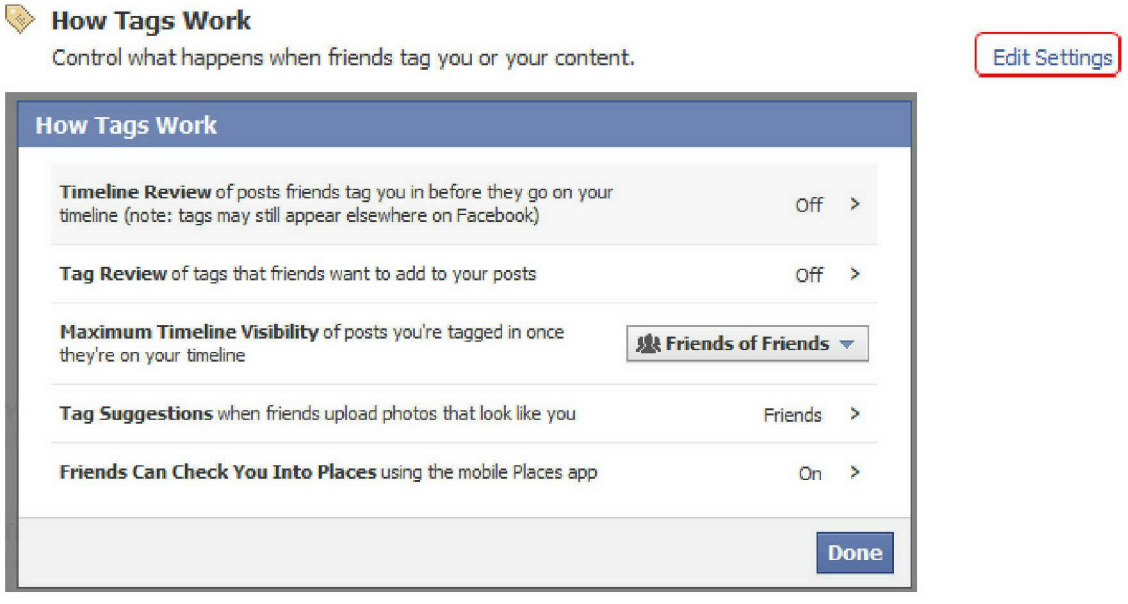
By default, both are off for friends, although you are required to approve a tag if the person who tags you isn't a friend.

To enable Timeline Review and Tag Review

1. Click on the down arrow ▾ at the top right of any page and select Privacy Settings.



2. Click on Edit Setting to the right of How Tags Work.

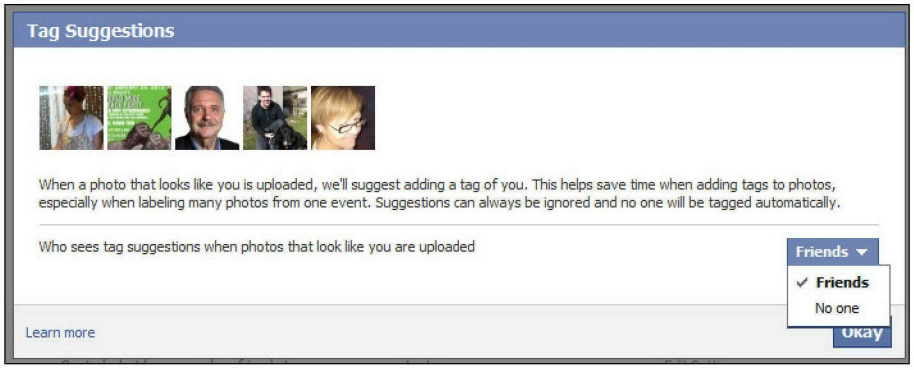


3. By default, Timeline Review and Tag Review are Off. Click on the word Off, and then change Disabled to Enabled.



Reputation & 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 as long as it meets Facebook's guidelines. It's also possible for people to include your name in a photo caption or a comment on a photo.*

Tag Suggestions



Facebook now has a feature that analyzes photos to see if they look like you and, if so, suggests that the picture might be of you, to make it easier for friends to tag it. It uses facial recognition technology, but it's very limited in how it works. It doesn't go randomly through all pictures on Facebook but *only works with pictures of people who are friends*. So, if Anne uploads a bunch of photos including one of her friend Larry, Facebook will offer to help her tag those photos and suggest that it's Larry. But if you're uncomfortable with this, you can turn it off, using the same dialog box as turning off Timeline Review and Tag Review. Although some people worry about facial recognition, we think Facebook is very responsible about how it's using the technology and see no reason to turn this off.

Apps

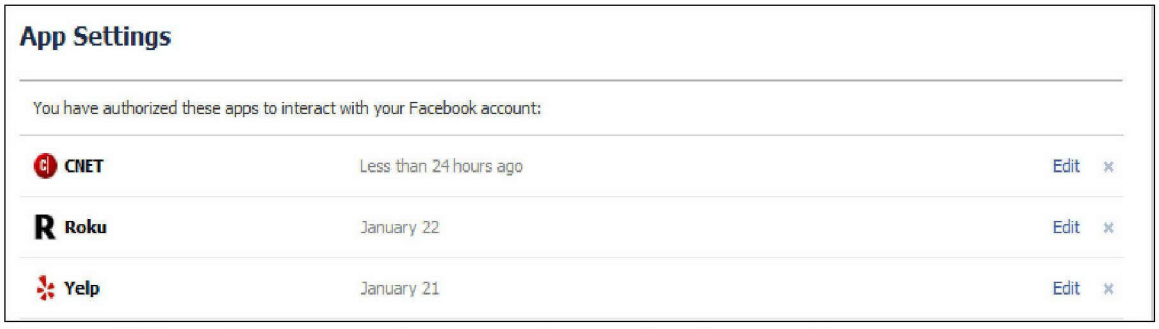
Facebook is home to many applications or little software programs that work within the service. On a typical day, Facebook users install more than 20 million apps and each month more than 500 million people use a Facebook app.

Apps can be games, music services, news sources, 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.

When you install an app it will ask permission to use and/or share your personal information, which can both include your public information and your list of friends. It may also ask permission to share other information including your posts and may also ask if it can post to your wall.

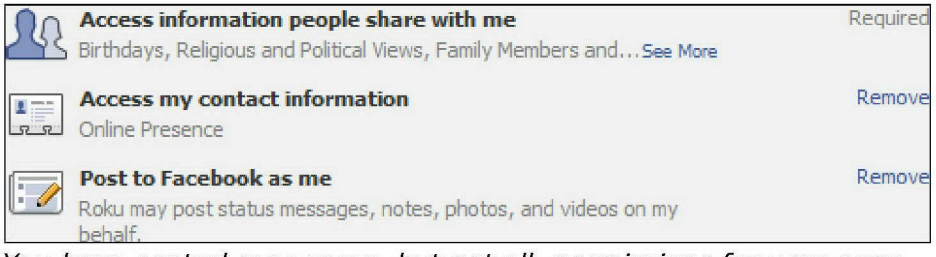
You can review and change any permission from the App Settings page, which you can get to by clicking on the down arrow next to Home, selecting Account Settings and then clicking on Apps on the left side of the page.

At this point, you'll see a page with a list of your installed apps with the ability to edit settings for any of your apps.



Click on Edit next to any app to change the app's privacy settings.

Some of the app settings are required (the only way to remove them is to uninstall the app) but others can be removed or changed.



You have control over some, but not all, permissions for your apps.

For example, you can adjust what information is available to apps 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.

Facebook's rules prohibit app developers from asking permission for any personal information that they don't need to run the app. For example, a birthday card app would ask permission to access your friends' birthdays because it's necessary to run the app. They can't sell or use the information for other purposes.

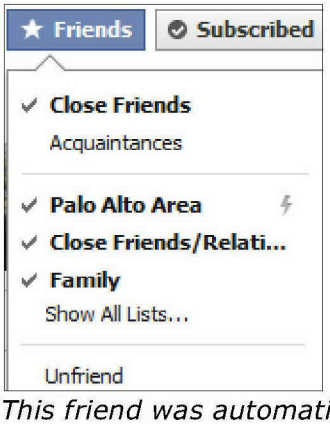
> ***Parenting Point**: There are hundreds of thousands of Facebook apps, and even though Facebook tries to police them with strict privacy and security rules, there is always the possibility of a rogue app or an app that's hacked or leaks information. Talk with your teens about checking with their friends or using a search engine to find out more about apps before installing them and to pay close attention to apps' privacy settings.*

Lists

One handy feature is the ability to create 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).

Facebook will automatically create some "smart lists" for you, based on things you have in common with people such as family, neighborhood, co-workers or schoolmates.

To see if a person is in one or more or your lists, go to their profile and hover over the Friends button near the top right.



This friend was automatically put in the Close Friends and other lists.

Remove someone from a list or add them

To remove someone from a list, simply click on any checked item to uncheck it. You can add them to a list by clicking on an unchecked item or you can "unfriend" them completely.

Groups

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's possible for people you don't necessarily want in the Group to be added by another member. 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.

There are three types of Groups: Open, Closed and Secret. Anyone on Facebook can see and join an Open Group. Anyone on Facebook can even see a Closed Group, as well as a list of its members, but only group members can see posts in the group. A Secret Group can't be found in searches and can't be seen by anyone outside the group.

***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 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.*

Messages

There are several ways people can use Facebook to communicate with each other. Besides writing on someone's wall, or timeline – which is very public –one option is to send a Message. Facebook's messaging system is like email in a lot of ways. It actually enables users to get their own @facebook.com address. Called "Messages," this service makes it possible for Facebook users to send or receive messages to or from anyone's email address. There is also an option to send messages to friends' mobile phones, whether from your mobile phone or a computer.

The 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. You'll find Messages right under News Feed in the left-hand column of the Home page.

For adults, the default setting is for everyone to be able to send you messages, but only friends and friends of friends can send messages to users under 18. Both adults and minors can limit who can send messages to only Friends.

> ***Safety & Privacy Point**: Be careful not to make the fairly common mistake of entering a private message on someone's wall where everybody can see it. Instead, click on "Message" under the large cover photo to send your friend a private message.*

To limit who can send you messages

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



2. Click on Edit Settings to the right of How You Connect.

3. Change the option to the right of Who can send you Facebook messages?

Managing your privacy on Facebook

With a few exceptions, users can control who can see just about anything they post – photos, text, whatever. And, for Facebook users under 18, there are even more levels of privacy protection (see below). However, some information is always public, including users' names, profile pictures, and the networks they belong to. But even with these, you have some control. You 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 holds people more accountable for what they post and discourages them 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.*

Special safeguards for teens

Parents may want to know that Facebook has safety and privacy settings for users under 18 which provide them with more protection. These include:

- **Search**: Teens can't be listed in public searches. Adults can, though they have the option to opt out.
- **Tagging**: Only friends and friends of friends can tag teens. Anyone can tag adults. If a friend tags a minor, the tag is visible to anyone who can see the post on Facebook or within apps and games. If a friend of a friend tags a minor, it's more restrictive. In that case only the teen's friends will see a link to the tagged content. The ability to review tags is on by default for teens and off by default for adults.
- **Audience**: The maximum audience that a teen can share with is friends of friends. Adults can share with the public. Teens can, however, post in a public forum, and any comments they make to a post can be seen by anyone else who can see that post.
- **Location-sharing** is turned off by default, but teens can turn it on. For adults it's on by default.
- **Subscribe**: It's not possible to subscribe to a teen's posts or timeline because they can't post to the public from their timeline. Teens can, however, subscribe to anyone's posts.
- **Friend requests**: Only friends and friends of friends can send messages to teens.
- **Messages** is turned off by default, but teens can turn it on. For adults it's on by default.
- **Chat**: Teens can only chat with friends.
- **Advertising**: Facebook will not display advertisements to teens about adult content, alcohol, dating, gambling and lotteries, health and fitness and subscription services.

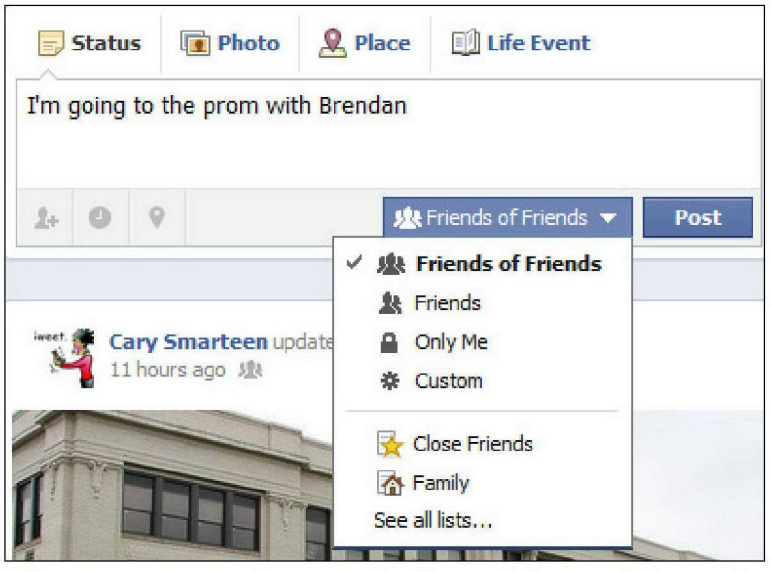
Those are the defaults for teens vs. adults. Now let's look at the options all users have to control their privacy in more detailed, granular ways.

Facebook's new, simplified 'inline' privacy settings

In August 2011, Facebook greatly simplified its privacy controls by creating what it calls "inline privacy settings."

What this means is that users will be able to control who gets to see each post, photo or other content more easily and right when they're creating the post. Whenever you post content, there is an opportunity to decide who can see it. For example, you can choose to share a particular post with just your Facebook friends, friends of friends, a particular list (such as Family or Close Friends), a specific friend or two or Only Me which means you're not sharing it with anyone.

Another important change is that Facebook is dropping the term "everyone" as a sharing option because people found that confusing. Adults can post to "Public," which can be anyone on Facebook or even anyone on the Internet.
In most situations, minors (users under 18) will not have the option to share with the public. They will be limited to friends and friends of friends.



Whenever you post any content – a status update, a photo or anything else – you'll see an audience selector icon. For minors, the maximum is friends of friends, but you can restrict it further by clicking on that icon and selecting a narrower audience.

> ***Privacy & Safety Point:*** *Whenever you change the audience, Facebook keeps that setting in place the next time you post. So if you usually post to friends but just posted something to friends of friends, it's important to remember to set it back to friends the next time you post.*

Privacy Point: *Friends of friends includes your friends as well as their friends. The theory is that people who are friends of friends have something in common. Still, just because someone is a friend of a friend doesn't necessarily mean that you want to share everything with them. So even though young people can share with friend of friends, it's a good idea to think carefully before doing–to make sure you're not sharing things with people you don't really know.*

Customizing who you share with

The Custom option in the drop-down box when you share content is a very powerful tool that lets you limit access to what you share to specific people – a List or Group of people or Only Me. There is even a way to *hide* information from specific people or groups of people.



Customizing privacy makes it possible to be very granular when it comes to sharing. You can share with specific people or lists of people. You can even hide the post from specific 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.

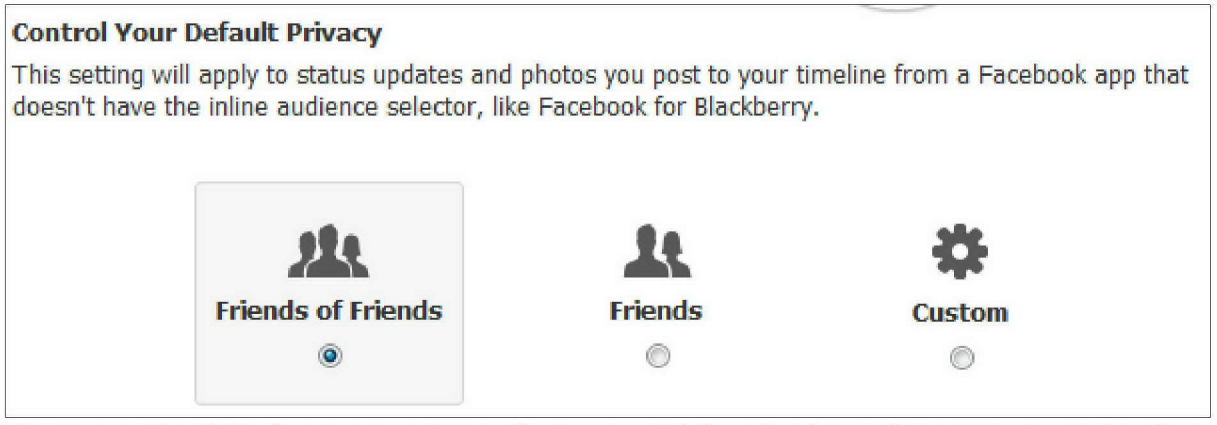
Limiting who can find you in search

Facebook has a search tool that allows users to find people. It's there to help find people who are already your Facebook friends, or others – such as former classmates or old friends – who you may wish to send a message to or add as a Facebook friend. Teens can't be found in public searches but adults can. However, even adults can opt out of being found in search by clicking on the

down arrow at the top right of any page, selecting Privacy Settings, clicking Edit Settings next to How You Connect and changing Who can look up your timeline by name or contact info.

Default privacy from apps that don't have inline controls

Thanks to inline controls, most of Facebook's default privacy settings have been eliminated, since you get to make that decision every time you post. However, there are some situations (like accessing Facebook on some mobile devices) where inline privacy controls aren't available. In that case, you can select the default controls by clicking on the down arrow at the top right of any page, selecting Privacy Settings and clicking on Friends of Friends, Friends or Custom. If you select Custom, you will be able to limit your choices even further, such as specific people or lists.



These are the default privacy options for teens. Adults also have the option to make their posts public. These apply only to certain apps that don't offer inline controls. In most situations, you will decide who can see your content each time you post.

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.

Download your whole Facebook history

Besides the new Activity Log feature described above, another way you can see everything you ever posted to Facebook is to download your entire record on Facebook to a file on your computer, where you can keep it forever – even if you later decide to leave Facebook. The file, which of course you can print out and file as a hard copy, will include any photos or videos you've shared on Facebook, your posts, messages and chat conversations – even your friends' names and some of their email addresses. It's a good way to have a permanent record. Be sure to keep this file secure, because it contains *all* your timeline information.

To download the file, click on the down arrow at the top right of any page, select Account Settings, and then click Download a copy of your Facebook data at the bottom of General Account Settings.

Facebook for mobile

Increasingly, people access Facebook via smart phones and other mobile devices, including Android phones, iPhones and a variety of tablets. In some countries, a lot of people don't have access to computers but do have mobile phones. But even in the U.S. and other developed countries, a lot of people – especially young people – prefer accessing Facebook from their mobile device while they're on the go. As of early 2012, more than 350 million active users access Facebook through their mobile devices worldwide, and this number is expected to grow significantly.

For the most part, the mobile experience on a smart phone is pretty similar to the Web experience, though the user interface is, of course, a bit different.



This is the Facebook iPhone app, which is similar to the Android version. The look of the page, though smaller, is similar to what you see on a computer.

> ***Parenting Point:*** *When kids access Facebook from their mobile device, they're often away from home or any adult supervision. Also, regardless of where you put your home computer or what parental controls you might have on it, they won't necessarily affect your child's mobile device (though there are mobile parental control apps you can get for that). It's very important that you talk with your teen about the responsible use of cellphones and tablet computers too, regardless of where they use them. Everybody should be careful about what's being shared with the apps they download or their phone's camera. Apps have been known to share whole contact lists, and photos have been known to embarrass or worse. Families need to be talking about responsible, mindful use of these powerful tools.*

Checking in to a location

One of the features on Facebook's mobile applications is the ability to "check in" to a location, which is a way of telling people where you are or have been. While

it can be fun to share your location, it can also be dangerous in some situations, so young people need to understand that this feature should be used cautiously.

When you check in, Facebook will use your phone's geo-location features (including GPS and proximity to local Wi-Fi stations and cellular towers) to try to locate places near you. Often it will find more than one nearby place so you're asked to choose the best match. If it can't find you, you can always type in your location.

It's also possible to "tag" friends who are with you at a place. That means that not only can your child indicate where he or she is, but friends can too. If you have "push notifications" for Facebook enabled on an iPhone or Android phone, you will be notified that someone has checked you in.

It's possible to turn off the ability for friends to check you into places, and we recommend that parents discuss this option with their teen.

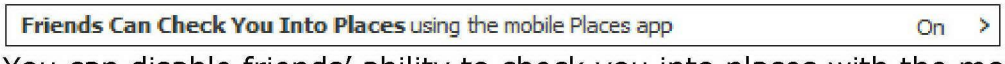
Being checked in or tagged

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.

There are some special protections for teens in Facebook for phones. Only friends will see that they're checked in to a place. There isn't even an option to extend that beyond friends, and a minor's name will not be seen on an establishment's Here Now page by anyone other than his or her friends.

To disable the ability for friends to check you in:

You can disable your friends' ability to check you into places, which we think is a good idea for teens. To do this, select Privacy Settings from the down arrow in the top right corner of any page and then click on Edit Settings to the right of How Tags Work and change it from On (Enabled) to Disabled.



You can disable friends' ability to check you into places with the mobile app

> ***Privacy & Safety Point***: *The difference between being checked in and being tagged can be confusing. What's important to know is that, if a friend checks you in, your presence at that location may be visible to people your friend shares with – not just the people you share with.*

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 photo) 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.*

"Social Reporting" is a new way to report problems on Facebook that was introduced in 2011. With it, users have the option to report mean or bullying behavior – as well as annoying or inappropriate photos and other problems – to someone who can help them in their offline life. That's an important addition because what happens on Facebook is mostly just the expression of "real world" relationships and socializing. Because of that, reporting something to customer-service people at Facebook is rarely the ultimate solution to that problem. The solution to issues in a relationship usually comes from the people in it or people around them who know and care about them.

Here's how Social Reporting works: If people want to report a photo, for example, and click on "Report" under it, they'll get a pop-up window asking if the report is about them or a friend. If it's about them, they can choose "I don't like this photo of me" or "It's harassing me." They can also choose "It's harassing a friend."



Facebook asks you to detail what's wrong with a photo you're reporting.

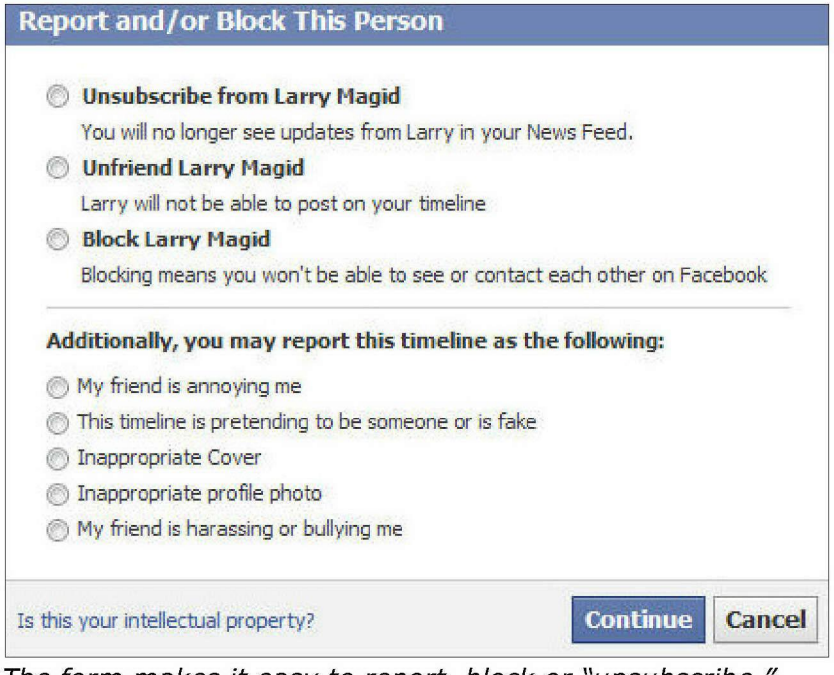
If it's harassment, they'll have the option to block the person who posted the photo or "Get help from an authority figure or trusted friend." If they choose the second option, Facebook lets them forward the photo (with Facebook's standard message or one the user writes) to someone they think should know about it or could help them deal with it. The user will be able to send the message and photo either via email to someone outside of Facebook or via in-site messaging to a fellow Facebook member.



Getting by with a little help from your friends

Reporting a person

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 by going to the user's page and clicking on the down arrow just below their cover photo and clicking Report/Block.

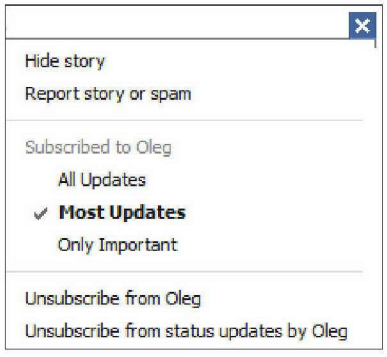


The form makes it easy to report, block or "unsubscribe."

The form allows you to report an inappropriate profile photo, a fake profile (a person misrepresenting him or herself), inappropriate or offensive information on the profile or unwanted contact from that person.

Reporting specific posts

You can also report posts that you think violate Facebook policies by clicking on the X or down arrow to the right of the post and selecting Report story or spam.



You can report any story, photo or message and use the same form to limit what you see from that person.

> ***Parenting Point**: 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 U.S. 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.

Our organization, ConnectSafely, has a page with resources for youth in crisis that you can access at www.connectsafely.org/yic.

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, Forbes, San Jose Mercury News, CNET and Huffington Post. Anne is also founder and executive director of the nonprofit organization NetFamilyNews, Inc., and editor of NetFamilyNews.org. Until 1997 she worked on the print, radio, TV, and Web editions of the Christian Science Monitor.*

© 2012 ConnectSafely.org and iKeepSafe Coalition (Rev. 2/18/12)