

Facebook Information and Advice

Useful Advice for Schools, Staff and Parents/Carers

What is Facebook?

Facebook is currently the world's most popular Social Networking site www.facebook.com Facebook is an American based company with over 750 million registered users, over 30 million of which are in the UK.

Facebook is only for users aged over 13 according to COPPA (Children's Online Privacy Protection Act - www.coppa.org); this is to protect children's privacy and to protect them from unsuitable advertising methods, it is not a measure of the suitability of the site such as with video games or films.

It is very easy for young people (or indeed adults) to enter an incorrect date of birth or false information to open a false or imposter account when registering as it is impossible for Facebook to verify every user. It is currently estimated that 43% of 8 – 12s have an online profile (timeline) on a social networking service (EU Kids Online, 2011). If a child can lie about their age to set up a Facebook account, then it is essential be aware that anyone can lie to create a Facebook account.

It is important to recognise that if we simply ban or tell children not to use sites such as Facebook then we will run the risk of driving any problems or incidents such as abuse or bullying underground. Adults should ensure that all children understand how to behave online in all circumstances and these skills should carry over to whichever site or system they are using.

It is essential that all Facebook users need to be aware of how to protect their information, how to report abuse or inappropriate content and that their parents/carers must be aware they are online.

If children or young people are using the site in an abusive way (e.g. to Cyberbully etc) then it is essential that they are reported and removed from Facebook. Evidence of Cyberbullying should be saved (e.g. messages, screen prints etc) and collected to help ensure that the sanctions can be implemented. (See the Cyberbullying Section for advice on how to deal with Cyberbullying)

Many schools choose to send letters to all parents reminding them about Facebook's age limit (13) when a concern is raised and advise parents to speak with their children about safe internet use and to be aware if their child is using Facebook under age. If the school are made aware of a child under 13 with a Facebook profile (timeline) then it is essential to discuss the concern with the child's parents/carers and recommend the profile (timeline) is deleted. Schools must be aware that this is an issue of parental responsibility as the access will be occurring outside of the school, However if the school feels that there is a Child Protection concern around the child's use of Facebook then the issue must be escalated in accordance with the school Child Protection and/or e-Safety procedures.

As Facebook is frequently blocked in school, the following information has been taken from Facebook's Help and Advice centre and is based on frequently asked questions to help inform schools, staff and parents/carers about what actions they can take about children and young people on Facebook.

Useful Tips for Young People:

- Visit www.facebook.com/safety for advice on staying safe on Facebook
- Make sure all of your online profile (timeline) are set to Private or friends only
- Do not share any personal information online e.g. what school you go to, your full name, any contact details etc
- Think very carefully about which photos and comments you share or post online –once a photo, video or message has been posted or sent, you can't remove it or take it back. Always remember than anyone could possibly see it (Would you say it in person or show it to your parents? If not then don't put it online)
- Use an internet nickname rather than your full name
- Consider using a cartoon picture or an avatar (picture to represent yourself)) for your profile or cover picture – never post pictures of yourself or your friends or family in school uniform
- Only use websites which are suitable for your age, if you're not sure then ask an adult first.
- Always remember, if you can lie about how old you are online, so can anyone else!
- Do not click on links or applications unless you can be sure of the content. Even if a link appears to be from a friend or is on a friends profile (timeline) or status is could be a virus or redirect you to nasty or illegal content.
- Make sure you only use Facebook to speak to people you know in the real world and if you do speak to strangers then be very careful what you say and what information you share with them
- Never arrange to meet someone you've met on Facebook without making it safe by taking an adult you trust with you. Always meet online contacts in a public place during the day – never go alone
- If someone says something on Facebook that makes you feel scared, worried or uncomfortable then make sure you report it to Facebook and/or the Child Exploitation and Online Protection Centre (CEOP) at www.thinkuknow.co.uk
- Visit www.thinkuknow.co.uk for more information on how to keep safe online

Useful links:

Facebook Safety Centre: www.facebook.com/safety

Facebook privacy settings: www.facebook.com/privacy/explanation.php

Report Abuse: www.thinkuknow.co.uk and www.ceop.police.uk



Facebook Click CEOP Page:

Facebook and the CEOP Centre have joined forces to make young people safer online by launching the new **Facebook 'ClickCEOP' Page**

Young users of Facebook and parents/carers are able to access advice, help and support directly from the CEOP Centre as well as from Facebook. Young people will be able to report instances of suspected grooming or inappropriate sexual behaviour directly from their profile (timeline) to specially trained investigators from CEOP.

CEOP's Facebook page (www.facebook.com/ClickCEOP) contains polls, news alerts and status updates. Young users (and any adults who 'like' the Click CEOP page) will receive regular messages from CEOP and its partner organisations who operate 'behind the button' to make children safer. Any Facebook user can like the Click CEOP page, as not only a constant source of help and reassurance but also as a strong visual signal to friends, family and others that they are in control online.

Facebook Information for Parents

<http://www.facebook.com/safety> features General Information, Addressing Personal Safety and Responding to Objectionable Content for Parents/Carers

Specific Questions for parents/carers: <http://www.facebook.com/help/?page=937>

“What happens if my Child has set up an account and they are under 13?”

Facebook requires its users to be at least 13 years old before they can create an account. Providing false information to create an account is always a violation of our Statement of Rights and Responsibilities www.facebook.com/terms.php

Applicable laws may give parents the right to access personal information their child has provided before Facebook follows its policy of promptly deleting such accounts. If you are aware of your underage child having an account on Facebook, you can show them how to delete their account by having them log into their profile (timeline) and following this link <http://tiny.cc/facebookdelete>

If you would like to report an underage user (under 13 years of age), please do so here: <http://tiny.cc/underageuser>

We will promptly delete the account of any underage user that is reported to us through this form. Alternatively, you can submit a request to Facebook here: <http://tiny.cc/facebookcoppa>

Please be aware that you will be required to submit a notarized statement declaring your rights as a parent or guardian immediately upon using this form.

Applicable laws may give parents the right to access personal information their under 13 year old child has provided before Facebook follows its policy of promptly deleting such accounts. Please be aware that you will be required to submit a copy of a notarized statement declaring your rights as a parent or guardian when submitting a report through this form: <http://tinyurl.com/childdatarequest>.

If you do not submit the necessary statement, we will not be able to provide you with any information and will delete the account.

“How can I request the removal of a photo or video of my child?”

Facebook removes content that violates the Facebook Terms, based on laws in specific jurisdictions. Use the Report link located near the photo or video to report the abusive content to us. Facebook offers additional privacy safeguards for people under the age of 18:

- Under 13 years old — Please submit a request to have the photo (<http://tinyurl.com/underagephoto>) or video (<http://tinyurl.com/underagevideo>) removed. We will review the content and remove if it contains an image of your child, he or she is under 13 years old, and you have filled out the report form accurately and completely. Please understand that we can only take action on reports that come from a parent or legal guardian of the person pictured.
- Between 13 and 17 years old – We can't help you directly unless required to do so by law. Please ask your teen to submit a request to have the photo (<http://tinyurl.com/undauthphoto>) or video (<http://tinyurl.com/undauthvideo>) removed.

Please be aware that we are only able to take action on reports that come from a parent or legal guardian of the child pictured in the reported content. If you are not a parent or legal guardian of the child pictured in the content you wish to report, please advise the appropriate parties to view this page and make the request.

“Can I monitor my child’s activity on the site?”

We appreciate your concern for your child's use of our website, but unfortunately we cannot give you access to the account or take any action on the account at your request. We are generally forbidden by privacy laws against giving unauthorized access to someone who is not an account holder. Please note that all users ages 13 and older are considered authorized account holders and are included in the scope of this policy.

We encourage parents to exercise any discretion they can on their own computers and in overseeing their kids' internet use. If you are a parent, you might also consider using software tools on your own computer in order to do so. Please do a search for computer-based Internet control technology on your preferred search engine to discover options that you may wish to pursue. Please talk to your kids, educate them about internet safety, and ask them to use our extensive privacy settings <http://www.facebook.com/settings/?tab=privacy>

If you would like to report an underage user (under thirteen years of age), please do so here <http://tiny.cc/underageuser>

If your child is experiencing abuse on the site, we encourage you to ask them to log in to their account and report it. Detailed information about reporting abuse is available on our Help Center's Report Abuse page: <http://www.facebook.com/help?page=798>


For more information, please review our Facebook Safety page: <http://www.facebook.com/security> .

What if my child sees inappropriate content or offensive material on the site?

Facebook takes the safety of its users very seriously and makes a significant effort to take down any objectionable material that may be posted on the site. We encourage users to report offensive timelines, messages, groups, events, shares, notes and photos. Reported items are then reviewed by Facebook administrators and removed if deemed in violation of our Statement of Rights and Responsibilities <https://www.facebook.com/legal/terms> . Users also have the option of "blocking" other users, which will ensure that they are unable to find them in a search, view their profile (timeline) or send them a message.

How can my teen report abuse?

The best way to flag abusive content on the site is to use the **Report** links that appear near the content itself. When a report is submitted, we will review it and take any action warranted by our Statement of Rights and Responsibilities. To submit a report, please take the steps listed below:

- Report a profile (timeline):
 1. Go to their profile (timeline)
 2. Click the  button
 3. Choose **Report/Block**
- Report a photo: Go to the specific photo and click the **Report This Photo** link that appears below the photo.
- Report an Inbox message: View the message and click the **Report Message** link that appears below the sender’s name. Note that you can only report messages from non-friends.

- Report a group or event: Go to its main page and click the **Report** link that appears below the group or event photo.
- Report a Page: View the Page and click the **Report Page** link that appears in the left column below the Page photo.

We also recommend that you consider blocking the user involved in the report. People you block won't be able to find you in searches, view your profile (timeline), or contact you with pokes, Wall posts, or personal messages. You can block people by adding their names to your block list at the bottom of the Privacy Settings page, or by checking **Block this person** when you report them. These people will not be notified when you block them, and any existing ties you have with them will be removed.

For all reports, be sure to follow the instructions carefully when choosing the report category.

Where else can I report inappropriate or objectionable actions that have been taken against children?

Facebook takes the safety of its users very seriously and takes significant efforts to make sure that the interactions encountered on the site are done so in a safe manner. We strongly urge all users to report suspicious people and inappropriate content when they come across it on the site. You can notify Facebook of any inappropriate people or content by clicking on the "Report" link located throughout the site. Users under the age of 18 are also encouraged to talk to a parent or a responsible adult immediately if someone online says or does something to make them feel uncomfortable or threatened in any way.

If you are living in the United Kingdom, under 18, and believe that an adult is acting inappropriately towards you on Facebook, please submit an online report to the Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk



(If you are a parent or other adult and concerned about a minor, you can also submit a report by accessing the Click CEOP Button.)

“What happens when I/my Child reports someone?”

Reporting a profile (timeline), group, page, or any other content doesn't guarantee that they or it will be removed. The Facebook community is extremely diverse. It's possible that something could be disagreeable or disturbing to you without meeting the criteria for removal <http://www.facebook.com/communitystandards>. That's why we offer personal controls, such as the ability to quietly cut ties with or hide people, pages, and applications that offend you. Content that does violate the Facebook Terms may be removed from Facebook and (in some cases) subject to legal or other action. The person reported is not notified of the identity of the person who made the report.

“How does Facebook’s Privacy work?”

Every Facebook user has the ability to customize his or her privacy settings. To edit the privacy settings for your own Facebook account, choose the "Privacy Settings" option from the Account drop-down menu available from the top right corner of every page.

- Control who can see your information from the Basic Directory Information section.
- Control who can see the content you share by selecting one of the three global privacy setting groupings (Public, Friends only or custom) in the "Sharing on Facebook" section. If you'd like to further customize these settings, click the "Customize settings" link.
- Control how your information is shared externally from the "Applications and Websites" section.
- Block specific people or applications from interacting with you on Facebook from the "Block Lists" section.
- Learn more about your privacy on Facebook here: <http://www.facebook.com/about/privacy/>

“Can I monitor my child’s activity on the site?”

Facebook is forbidden by federal and many state laws to give unauthorized access to someone who is not an account holder.

We encourage parents to exercise any discretion they can on their own computers and in overseeing their kids' internet use. Please talk to your kids, educate them about internet safety, and ask them to use our extensive privacy settings

<http://www.facebook.com/settings/?tab=privacy>

If you would like to report an underage user (under thirteen years of age), please do so here

<http://tiny.cc/underageuser>

If your child is experiencing abuse on the site, we encourage you to ask them to log in to their account and report it. Detailed information about reporting abuse is available on our Help Center's Report Abuse page: <http://www.facebook.com/help?page=798>

For more information, please review our Facebook Safety page:

<http://www.facebook.com/security> .

“How can I help my child use Facebook safely?”

The best thing to do is to talk to your children and teach them about Internet safety.

Remind them to:

- Never share their password with anyone
- Understand their privacy settings
- Report people or content that violate our Statement of Rights and Responsibilities
- Block anyone that might be sending unwanted content
- Useful Tips to share with Parents/Carers
- Discuss safe online behaviour with your child such as sharing personal information, making safe passwords and meeting online friends

Additional tips from e-Safety Officer:

- If your children are using online spaces such as Facebook when they are under 13, then it is important to talk with them about this and supervise such use. They should be aware that using Facebook under 13 is against Facebook's terms of service, and Facebook will delete any accounts of under 13s they discover. There are other more suitable online spaces designed for younger children and using these spaces can be a positive way to respond to social networking.
- Why not have a “family” Facebook page to use safely together or use your own profile (timeline) to role model positive online behaviour.
- Make sure you know what your children are doing online much like you would in “real” life.
- Make sure that your children are aware that people or websites can lie online.
- Be aware that children can access the internet in a variety of places (such as on a mobile phone or Games console or at a friend or neighbours house) and simply “banning” them from using Facebook might not always work. This could cause them to lie and hide their online activity from you.
- Make sure your child understands that online actions can have offline consequences – the law applies to the internet too and it’s sometimes easy to forget that the Police can act on online evidence.
- Visit <http://www.facebook.com/safety> and <http://www.facebook.com/safety/groups/parents/> and read the advice section for parents and teens.
- Visit www.childnet.com/kia for advice about social networking and an interactive guide for parents/carers
- Visit www.thinkuknow.co.uk/parents for more information on how to keep safe online
- www.kent.gov.uk/esafety - Kent’s e-Safety information for Parents and carers
- If using Facebook “Places” then visit <http://tiny.cc/safekidsgsp> and <http://tiny.cc/connectsafelygps> for some safety tips and considerations before using GPS or location based services

Facebook Privacy for minors (users aged 13 -18)

<https://www.facebook.com/help/?page=214189648617074>

Minors (users aged between 13 and 18) who use Facebook have a slightly different experience with privacy than adults.

(NB the following content does rely on the fact that children register using their correct date of birth – if a child sets up account stating they are over 18 then adult privacy settings will apply. This cannot be changed at a later stage)

How do Minors connect with other people?

Like adults, minors can appear in search results. Adults and minors can also receive a friend request from someone who is not already a friend of a friend, such as a family relative or a friend with whom they have no mutual friends. Because friend requests may come from people they don't know, minors should always be careful when accepting these requests.

Messages are handled differently for minors and adults:

Minors	Adults
Depending on their settings, minors may receive messages from people who are friends of friends on Facebook, which may include adults they don't know.	Depending on their settings, adults can be messaged by anyone on Facebook.

We encourage minors to visit their Privacy Settings page to manage and limit who is allowed to send them friend requests and messages.

How do minors share posts like photos and status updates?

Minors	Adults
Minors can share with a maximum of friends of their friends .	Adults can share posts with a maximum of everyone by posting as public .

How does tagging work for minors?

You can add tags of anyone — including people you don't know, any place, or any page (like a celebrity or sports team). When you add a tag of someone to your photo, status update or other posts, you may also be sharing the post with that person's friends. Keep in mind that the tagged person's friends might include adults you don't know.

Who can tag you?

Minors	Adults
Only friends of your friends can tag you in a post.	Any person can add a tag of you to their post

Who can see tags of you?

Visibility of tags of Minors is different for young people than adults. Visibility varies based on who added the tag and who is viewing the post.

Minors	Adults
<p>If a friend adds a tag of you, that tag is visible to any person who can see the post on Facebook and in third-party applications like quizzes and games.</p> <p>If a friend of a friend tags you, only your friends can see your name with a link to your profile (timeline). This visibility applies to Facebook and third-party applications like quizzes and games.</p> <p>If a friend of a friend adds a tag of you, non-friends will just see your name with no link to your profile (timeline).</p>	<p>If any person adds a tag of an adult, the tag has the same visibility as the post itself on Facebook and in third-party applications like quizzes and games.</p>

Who can add tags to your posts?

Any person who can see your posts may be able to add tags to them. Minors can share posts with a maximum of friends of their friends. We limit this when you're younger to help protect younger people's privacy.

Adding a tag of someone will share the post with that person's friends. You have the option to approve tags other people add to your posts before they appear, using a new Tag Review feature. To turn the feature "on" or "off," go to the How Tags Work setting in your privacy settings.

When you approve a tag, keep in mind that you are giving permission for the tagged person's friends to see your post, which might include adults that you do not know.

Minors	Adults
<p>For minors, the Tag Review setting is turned 'On' by default.</p> <p>You can turn this 'Off' if you want to allow friends to add tags to your posts without reviewing the tags first. You will always have to review tags from friends of friends.</p>	<p>For most adults, this setting is turned 'Off' by default so you don't have to approve tags that friends add to your posts.</p> <p>You can turn this 'On' if you prefer to approve tags added to your content before they go on Facebook.</p>

How do location services work for minors?

The sharing tool gives you the option to share where you are when you post. You can add location to photos and status updates. There are special safeguards for Minors:

Minors	Adults
When you first use the new sharing tool location feature is 'Off' by default. To turn it 'On,' simply click the button to add location to your post. This setting will continue to stay 'On' until you change it.	For most adults, when you first use the new sharing tool the location feature is 'On' by default. To turn it 'Off,' simply click the 'X.'

For a complete overview of how this works for adults, go to Share Where You Are: <https://www.facebook.com/about/location> .

How do privacy controls change when a minor becomes an adult?

When you reach a legal adulthood, we will notify you that you are now considered an adult on Facebook and remind you of the new privacy controls and sharing options available to you as an adult.

Here is what you will be notified of upon adulthood:

- You can now communicate with anyone on Facebook
- Any person can add a tag of you to their posts
- If someone adds a tag of you in a post and shares with Public, then that tag of you will be visible to everyone
- You have the option to be contacted by everyone via the Public setting

How does the Public setting work for minors?

The maximum amount of people minors can share with is friends of their friends. So, wherever minors see Public as an audience option, it means **friends of friends**. In contrast, when adults choose Public their audience selection includes **everyone on the internet**.

Why do minors see a Public sharing option for their profile (timeline) information?

Wherever minors see Public as an audience option, it means **friends of friends**. Once a minor reaches legal adulthood, the meaning for Public changes to **everyone on the internet**.

Example: If a minor chooses to share his hometown with Public, his hometown only displays to friends of friends. When he reaches legal adulthood, his hometown becomes available to everyone on the internet

Facebook Information for Educators

<http://www.facebook.com/safety/> : Features General Information, Addressing Personal Safety and Responding to Objectionable Content for Educators

<http://www.facebook.com/help/?page=937> – Specific questions for educators

“What should I do if I become aware of an underage user (under 13) with an account on Facebook?”

Facebook requires its users to be at least 13 years old before they can create an account. Providing false information to create an account is a violation of our Statement of Rights and Responsibilities www.facebook.com/terms.php

If you would like to report an underage user (under 13 years of age), please do so here <http://tiny.cc/underageuser>

We will promptly delete the account of any user under the age of 13 that is reported to us through this form.

NB: Addition from e-Safety Officer: Reporting an underage account to Facebook is a quick way to get a profile (timeline) removed. However, there is little to stop a child from re-registering with a new email address to open a new account. It is important therefore to address any concerns with the child and their parents/carers as the school will be unable to prevent the child or their parents/carers from setting up a new account.

“What should I do if I am aware of abuse on Facebook involving students?”

Facebook has report links on the site to help signal abusive content. We recommend that you ask the student involved in the abuse to report the matter using the instructions below:

- To report a profile (timeline), go to the profile (timeline) and click "Report/Block this Person" in the left column below the profile (timeline) photo.
- To report a photo, go to the specific photo and click "Report This Photo" below the photo.
- To report an Inbox message, view the message and click "Report Message" below the sender's name. Note that you can only report messages from non-friends.
- To report a group or event, go to its main page and click the "Report" link below the group or event photo.
- To report a Page, view the Page and click "Report Page" in the left column below the Page photo.
- If the student involved is unable to report the content, you can also report it yourself. Please note that we are unable to provide information about accounts on Facebook to anyone but the account holder.

<http://www.facebook.com/help/?faq=16339>

“How can I maintain a professional presence on the site separate from my personal profile (timeline)?”

Facebook offers several options that will allow you to do this:

- Create a friend list specifically for your students. This will allow you to control which parts of your profile (timeline) are visible to your students, keep track of the list's activity separately, and send bulk messages — like homework assignments and invites — to the group all at once. See <http://www.facebook.com/help/?page=768> for more details
- Create a page — *Ms. Smith's 9th Grade Science Class*, for example. Pages are great for broadcasting information to people on Facebook. Pages are free, you can control them with your personal profile (timeline), and they keep your profile (timeline) separate from your students. Anyone who "likes" your page will automatically receive updates. See <http://www.facebook.com/pages/create.php> for more details
- Create a group where you and your students can connect, share, and collaborate — *American Literature 101 Discussions*, for example — or a group where educators in your department can collaborate on lesson plans and share ideas. See <http://www.facebook.com/help/?topic=groups> for more details

NB: Addition from e-Safety Officer: The use of Facebook for professional purposes with students should **only** take place with full approval and support from your school Senior Leadership Team. It must be fully documented in the School e-Safety Policy and include appropriate training, risk assessments and awareness raising for all those involved and only for use with students who are able to use the site (e.g. 13 and over)

“What is the “Facebook in Education” Page?”

The “Facebook in Education” page is a resource for teachers, professors, administrators, counsellors and others who work in education. You can refer to this page for privacy tips to help you maintain both a personal and a professional presence on Facebook. You'll also find answers to common questions including how to report abuse to Facebook and the best way to use Facebook as a communication tool in your school. To become a fan of this page, click here www.facebook.com/education and choose the "Become a Fan" option at the top of the page. Facebook also has a document aimed at Teachers: Facebook for Educators: <http://www.facebook.com/safety/attachment/Facebook%20for%20Educators.pdf>

“What other resources are available regarding Internet Safety?”

Here are some websites with valuable information:

- A Thin Line: www.athinline.org
- Beatbullying.org: www.beatbullying.org
- Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk
- Childnet International: www.childnet.com
- Common Sense Media: www.common Sense Media.org
- Connect Safely: www.connectsafely.org
- Cyberbullying Research Center: www.cyberbullying.us
- FOSI (Family Online Safety Institute): www.fosi.org
- NetSmartz: www.netsmartz.org
- OnGuardOnline: www.onguardonline.gov
- Think U Know: www.thinkuknow.co.uk
- Webwise Kids: <http://webwisekids.org>
- Wired Safety: <http://wiredsafety.org>
- Facebook for educators: <http://facebookforeducators.org/>

Addition from e-Safety Officer: Useful links and resources can be found at www.kenttrustweb.org.uk?esafety

General Concerns: Facebook and Cyberbullying

www.facebook.com/help/?safety

We want Facebook to remain an environment where people can connect and share comfortably. Cyberbullying is defined as the use of any new technology to harass or intimidate someone and is considered to be abusive behaviour.

Accept Friend Requests Safely

In order to prevent harassment from strangers, be careful to accept friend requests only from people you know in real life. Also, remember to report any messages or profile (timeline) that look suspicious. Facebook is based on a real-name culture, and fake profiles (timelines) are regularly disabled when they're reported to us. Please also keep in mind that only confirmed friends can post to your Wall or contact you via Facebook Chat, so if you're worried that someone will make inappropriate posts or send offensive messages, just ignore that person's friend request.

Use the "Block" Feature to Stop Abusive Behaviour

A block prevents specific people from viewing your profile (timeline). When you block people, any ties you currently have with them will be broken, and these people won't be able to contact you through Facebook.

If you receive inappropriate or abusive communication, you can block the person by listing his or her name in the "Block People" box at the bottom of your Privacy Settings page. You can visit this page at any time by hovering your mouse over the "Settings" link at the top of any Facebook page and selecting the "Privacy Settings" option from the drop-down menu that appears.

Report Abusive Behaviour Directly to Facebook

The most efficient way to report abuse is to do it in the same place it occurs on Facebook. For example, if you receive a harassing message in your Inbox, you can report the message by clicking on the "Report" link next to the sender's name as you are reading the message. If you receive a harassing message from a person who is a Facebook friend of yours, you should remove the person as a friend and report the message.

Reporting the message as harassing will automatically add this person to your Block list. You can also use the "Report/Block person" link that appears at the bottom of the abusive user's profile (timeline). If you learn that someone is continuing to make abusive comments about you even after you've blocked them, you can ask a friend to report that person on your behalf. Reports are confidential and the user being reported does not know that they have been reported. After a report is submitted, we will investigate the issue and make a determination as to whether or not the content should remain on the site based on our Terms of Use.

A Facebook administrator looks into each report thoroughly in order to decide the appropriate course of action.

Restrict Privacy Settings

To restrict the amount of information that potential bullies may have access to, customize your privacy settings so that certain people can't access information like your Wall, photos, or profile (timeline).

You can also change your privacy settings if you are uncomfortable being found in searches or having your profile (timeline) viewed publicly.

Privacy on Facebook is controlled primarily from the Privacy Settings page. You can visit this page at any time by hovering your mouse over the "Settings" link at the top of any page of Facebook and selecting the "Privacy Settings" option from the drop-down menu that appears.

Respond to Abusers in the Right Way

Cyberbullies often seek a reaction from the people they harass. When they fail to get one, they often give up gradually.

Rather than responding to a bully via Inbox, a Wall post, or Facebook Chat, you can delete offensive posts from your Wall or messages from your Inbox and then use the "Block" or "Report" functions to resolve the issue safely. To delete an offensive Wall post, hover over the post in question, click the "Remove" button that appears, and select "Delete" in the dialogue box. To delete a message from Inbox, simply click the "Delete" button at the top of the message.

Only confirmed friends can post to your Wall or send you a message through Chat. If you are receiving posts and Chat messages you don't like, you should consider removing the sender from your friends list.

What should I do if someone who is being bullied asks me for help?

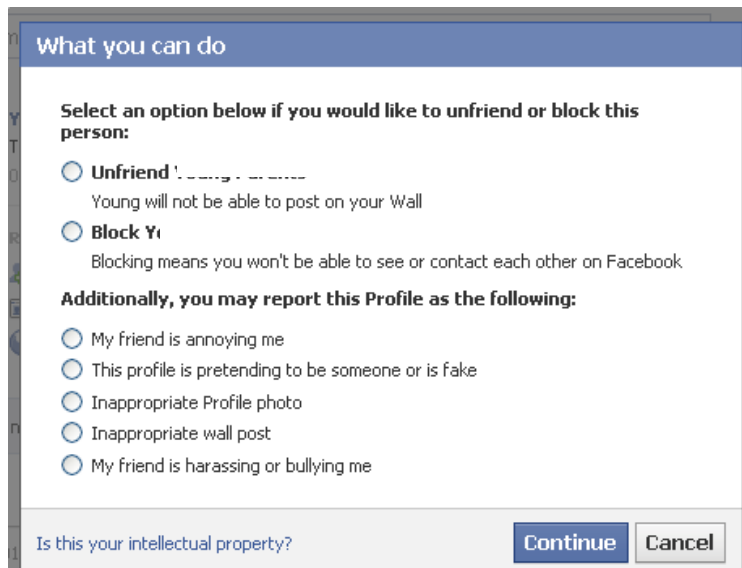
Help others address safety concerns by taking the following approach:

- **Block and report:** Make sure the bullying content has been reported to Facebook. We will review the reported content and remove anything that violates Facebook's Statement of Rights and Responsibilities. Remind your friend to block the person responsible without responding directly to the bullying or escalating the conflict in any way.
- **Restrict privacy settings:** Advise your friend to use account privacy settings to control who can view their profile (timeline). Access privacy settings by clicking on "Privacy Settings" from the "Account" drop-down menu in the top right corner of every Facebook page.
- **Evaluate and document:** Is someone at risk of physical harm? Contact your local law enforcement immediately if the bully has posted personal contact information or made specific threats of physical violence. Take screenshots of all bullying posts, and print them out to save.

Facebook provides more advice on reporting abuse and policy violations here:

<http://tinyurl.com/reportabusepolicyvio>

General Concerns: Reporting Abusive Content




“How do I report abusive Content?”

You may report abuse by using the proper "Report" link that appears next to many pieces of content on the site. You may also report another user by using the "Report/Block" link that appears at the bottom of a user's profile (timeline) page. If this does not resolve the issue, we suggest that you block the person by listing his or her name in the "Blocking People" box that appears at the bottom of the Privacy page. If you have already blocked an offender or have been blocked by an offender posting abusive content, please have another user report the abusive content or the offender through the one of the various "Report" links available on the site.

If you see something on Facebook that you believe violates Facebook's terms <http://www.facebook.com/terms.php>, you can report it to Facebook. To make a report, find the "Report" link that is nearest to what you want to report:

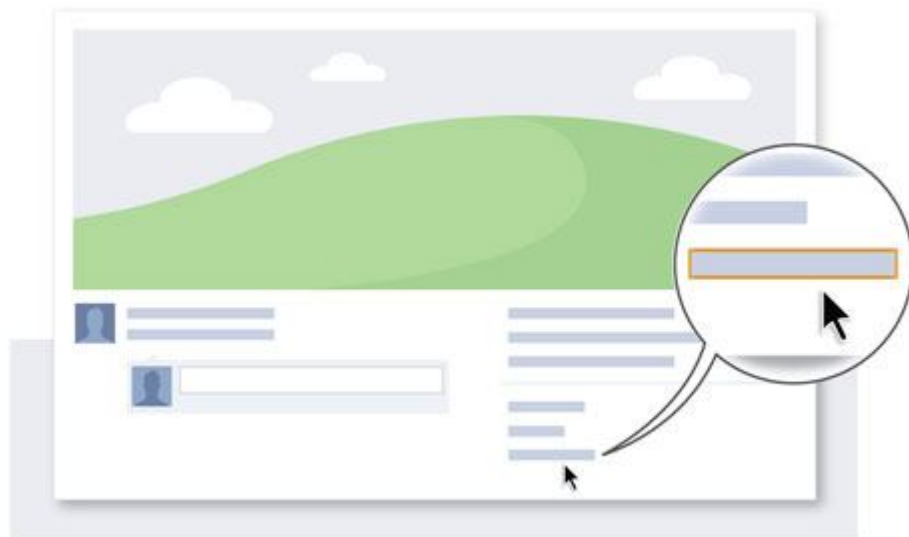
Reporting Timelines (Profiles)

1. Click the gear menu  in the top right side of the timeline you'd like to report.
2. Choose the **Report/Block** option to report the account to Facebook.



Reporting Photos & Videos

1. Click on the photo or video you want to report
2. Click the **Report This Photo** or **Report This Video** link that's located in the bottom right corner of the page



Reporting Pages

1. Click on the page you want to report
2. Click the **Report This Page** link that's located in the bottom left corner of the page




Reporting Messages

1. Open the message you'd like to report
2. Click to open the **Actions** menu at the top right corner of the message

3. Choose **Report as Spam** if the message is spam, or **Report Conversation** if the message is threatening, harassing or from someone whose account was hacked




Reporting Posts

1. Use your mouse to find the X or the arrow menu  in the right corner of the post you'd like to report
2. Click **Report post or spam**



Reporting Groups

1. Go to the group you want to report
2. Click  at the top right corner
3. Pick **Report Group** from the dropdown menu



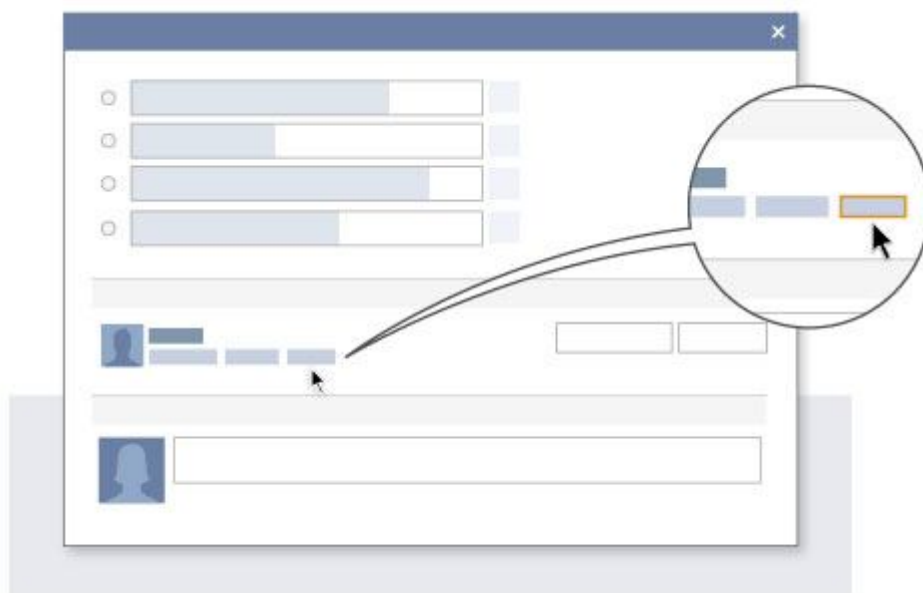
Reporting Events

1. Click on the event you want to report.
2. Scroll down to the very bottom of the event Wall and click the **Report Event** link. You may need to scroll down a few times to see this link.



Reporting Questions

1. Click on the title of the question. Then click the Report link under **Asked By**.
2. To report a **reply** to a question, hover over the post and click the X to report it.



Reporting Ads

1. When viewing the ad in question, hover over the ad and click the **X** to the right of the ad
2. Choose **Hide this ad** to report a specific ad, or **Hide all from...** to hide all ads from that particular advertiser



Posts on Your Timeline

1. Use your mouse to find the pencil icon in the top right corner of the post you'd like to report
2. Click **Report/Mark as Spam**
3. Choose the **Report** link to report to Facebook



Because of the diversity of the Facebook community, it's possible that something could be disagreeable or disturbing to you without meeting the criteria for being removed or blocked. For this reason, Facebook also offer personal controls over what you see, such as the ability to block, hide or unfriend people, Pages, or applications that offend you. Content that does violate our terms may be removed from our site and (in some cases) subject to legal or other action.

For information about what we allow and don't allow on Facebook, please read Community Standards: <http://tinyurl.com/facebookcommunitystandards>

“How do I report a fake or impostor Profile (timeline)?”

<https://www.facebook.com/help/?topic=reportabuse>

You can report a profile (timeline) that violates Facebook’s Statement of Rights and Responsibilities by clicking the "Report/Block this Person" link in the left column of the profile (timeline), selecting "Fake profile (timeline)" as the reason, and adding the appropriate information. Facebook reviews every report we receive in order to determine whether or not the content violates our Statement of Rights and Responsibilities, and will take appropriate action. Rest assured that these reports will be kept confidential. Fake profiles (timelines) created to imitate real people (impostor timelines) are not allowed on Facebook.

If someone created a profile (timeline) pretending to be you:

1. Go to the profile (timeline)
2. Scroll to the bottom of the left column and click **Report/Block This Person**
3. Click **This profile (timeline) is pretending to be someone or is fake**
4. Choose **Pretending to be me** from the type drop-down
5. Click **Continue** to submit your report

A friend can also report the fake profile (timeline): "If someone created a profile (timeline) pretending to be one of your friends" tell your friend to report this to us by clicking the **Report/Block This Person** link on the impostor profile (timeline).

If you're friend can't access the impostor profile (timeline) to report it:

1. Go to the profile (timeline)
2. Scroll to the bottom of the left column and click **Report/Block This Person**
3. Click **This profile (timeline) is pretending to be someone or is fake**
4. Choose **Pretending to be someone I know** from the type drop-down
5. Type in the name of the friend being impersonated
6. Click **Continue** to submit your report"

“How does someone who does not have an account report abuse?”

Someone who does not have an account can submit an inquiry or report abuse:

<http://tinyurl.com/tosviolation>

“What is Social Reporting?”

Social reporting is a way for Facebook Users to quickly and easily ask for help from someone they know and trust in the real world such as a parent or friend. To access Social Reporting users need to click on the “Report” link on profiles (timelines) and photos.

<http://tinyurl.com/fbsocialreporting>

Social Reporting in action:

Is this photo about you?

Yes, this photo is about me:

- don't like this photo
- This photo is harassing or bullying me

No, this photo is about something else:

- Spam or scam
- Nudity or pornography
- Graphic violence
- Attacks individual or group
- Hate symbol
- Illegal drug use

Is this your intellectual property?

Continue **Cancel**

What You Can Do

While Facebook can't remove unflattering photos from the site, you may:

- Send a message to Carolyn Wilson**
Ask Carolyn to remove the photo

Hey, I didn't like this photo. Please remove it.

- Remove Carolyn Wilson as a friend**
Carolyn will not be able to tag you in photos
- Block Carolyn Wilson**
You and Carolyn will become invisible to each other on Facebook, which means you can't see or contact each other

Continue **Cancel**

What You Can Do

Are you in physical danger? If so, please report this threat to a local authority. Please choose from the options below:

- Block Carolyn Wilson**
You and Carolyn will become invisible to each other on Facebook, which means you can't see or contact each other
- Get help from a trusted friend**
Forward this photo to someone who can help you in person
- Report to Facebook**

Continue **Cancel**

Report Photo

Learn more about how to handle harassment in our Safety Center.

To: _____

Message: Hi, this person is bothering me online and I'm not sure how to respond. Can you please help?



From the album: My "Friends"
By Carolyn Wilson

Continue **Cancel**

“How do I report an abusive application? What can I do if I believe an application is violating Facebook policies?”

You can report an app by clicking **Report/Contact this App** at the bottom of any page within the app on Facebook.

If you haven't installed the app, you can also click **Report App** on the app install screen:

https://www.facebook.com/help/?faq=248716141830800&in_context

“How do I report a convicted sex offender?”

Convicted sex offenders are prohibited from using Facebook. Once we are able to verify a user's status as a sex offender, we immediately disable their account and remove their profile (timeline) and all information associated with it.

We accept the following forms of documentation to verify someone's status as a convicted sex offender:

- Link to a listing in a national sex offender registry
- Link to an online news article
- Link to a court document
- Documentation verifying the report attached to the sex offender report form

If you are unable to provide documentation, we recommend that you ask a local law enforcement representative to contact us so we can take action on your report.

If you have encountered a profile (timeline) that may belong to a convicted sex offender, please report it (<http://tinyurl.com/fbdoffender>) and we will review the information.

“Where can I report inappropriate or objectionable actions that have been taken against children?”

Facebook takes the safety of its users very seriously and takes significant efforts to make sure that the interactions encountered on the site are done so in a safe manner. We strongly urge all users to report suspicious people and inappropriate content when they come across it on the site. You can notify Facebook of any inappropriate people or content by clicking on the "Report" link located throughout the site. Users under the age of 18 are also encouraged to talk to a parent or a responsible adult immediately if someone online says or does something to make them feel uncomfortable or threatened in any way.

If you believe that an adult is acting inappropriately towards a child/young person on Facebook, please submit an online report to the Child Exploitation and Online Protection Centre (CEOP): <http://www.ceop.police.uk/safety-centre/>



“How do I help someone who has posted worrisome content relating to eating disorders?”

If you have encountered content or photos that indicate someone is in immediate physical danger related to an eating disorder, please contact 999 or local law enforcement for help. If the threat is not immediate, you should call a family member or loved one who is close by the person you are worried about to try to help. We also recommend that you contact a local helpline to find out more information about how you can help a friend or loved one with a possible eating disorder.

Facebook is working with the National Eating Disorders Association to provide resources to our users and to support those struggling with an eating disorders, to find treatment referrals and how to help a friend. If you want to find out more about eating disorders, how to educate others and how to prevent them, visit B-eat (beating eating disorders), 0845 634 1414 or (beat youthline: 0845 634 7650); help@b-eat.co.uk; www.b-eat.co.uk

“How do I help someone who has posted suicidal content on Facebook?”

If you have encountered a direct threat of suicide on Facebook, please immediately contact law enforcement (Kent Police) or a suicide hotline such as the Samaritans.

- Contact the Samaritans at 08457 90 90 90 (UK) or 1850 60 90 90 (Republic of Ireland), or email jo@samaritans.org
- To report suicidal content to Facebook here: <http://tinyurl.com/suicidecontent>
- For resources about identifying and responding to suicide warning signals, click here: <http://www.facebook.com/help/?faq=20193>

General Concerns: Compromised and Hacked Accounts

Users can download a free guide to help improve awareness about Facebook Security: "OwnYourSpace: A Guide to Facebook Security": <http://tinyurl.com/ownyourspaceFB> . The guide will help users to understand how to protect your Facebook account, avoid scammers and configure advanced security settings. Users will also be aware of security features such as how to use one-time passwords, enable secure browsing and track account activity. The guide will also help users to understand what motivates account thieves and malware pushers and what they should do if an account is hijacked or hacked.

"What can I do to protect the security of my account?"

1. Never click suspicious links: It is possible that your friends could unwillingly send spam, viruses, or malware through Facebook if their accounts are infected. Do not click this material and do not run any ".exe" files on your computer without knowing what they are. Also, be sure to use the most current version of your browser as they contain important security warnings and protection features. Current versions of Firefox and Internet Explorer warn you if you have navigated to a suspected phishing site, and we recommend that you upgrade your browser to the most current version. You can also find more information about phishing and how to avoid it at http://www.antiphishing.org/consumer_recs.html and www.getsafeonline.org

2. Phishing is an online attempt to trick a user by pretending to be an official login page or an official email from an organization that you would have an account with, such as a bank or an email provider, in order to obtain a user's login and account information. In the case of a phishing login page, the login page may look identical to the login page you would normally go to, but the website does not belong to the organization you have an account with (the URL web address of the website should reflect this). In the case of a phishing email, the email may look like an email you would get from the organization you have an account with and get emails from, but the link in the email that it directs you to takes you to the above phishing login page, rather than a legitimate login page for that organization.

To prevent your account information from being obtained in a phishing scheme, only log in to legitimate pages of the websites you have an account with. For example, "www.facebook.example.com" is not a legitimate Facebook page on the "www.facebook.com" domain, but "www.facebook.com/example" is a legitimate Facebook page because it has the "facebook.com" domain. When in doubt, you can always just type in "facebook.com" into your browser to return to the legitimate Facebook site.

3. Have a unique, strong password: From the Account Settings page, be sure to use a different password than you use for other sites or services, made up of a complex string of numbers, letters, and punctuation marks that is at least six characters in length. Do not use words found in the dictionary.

4. Run anti-virus software: If your computer has been infected with a virus or with malware, you will need to run anti-virus software to remove harmful programs and keep your information secure.

- For Windows:

- <http://www.microsoft.com/protect/viruses/xp/av.msp>

- <http://www.microsoft.com/protect/computer/viruses/default.msp>

- For Apple/Mac OS:

- <http://support.apple.com/kb/HT1222>

“My account and/or login email address has been taken over by another person – Hacked account”

If you believe your account has been taken over by another person, the easiest way to solve this issue on your own is to reset your password. You can secure your own account by selecting the "Forgot your password?" link that appears above the on the login page. An email will be sent to you with steps for completing the process.

If this does not resolve your issue or your email address has also been compromised, please submit your report here: <http://tiny.cc/facebookhacked>

“My account has been used to automatically send spam or misleading links – Phished account”

Phishing happens when you enter your login credentials on a fake Facebook login page or download malicious software to your computer. This may result in messages or links being automatically sent to a large number of your friends. These messages or links are often advertisements encouraging your friends to check out videos or products.

To solve this issue on your own, please carefully follow the steps provided:

1. Run anti-virus software: If your computer has been infected with a virus or with malware, you will need to run anti-virus software to remove these harmful programs and keep your information secure.
 - For Windows:
<http://www.microsoft.com/protect/viruses/xp/av.msp>
<http://www.microsoft.com/protect/computer/viruses/default.msp>
 - For Apple/Mac OS:
<http://support.apple.com/kb/HT1222>
2. Reset password: If you know your password and would like to change it, you can do so from the Settings tab on the Account page or by selecting the "Forgot your password?" link that appears above the on the login page. Be sure to use a different password than you use for other sites or services, made up of a complex string of numbers, letters, and punctuation marks that is at least six characters in length. Do not use words found in the dictionary.
3. Never click suspicious links: It is possible that your friends could unwillingly send spam, viruses, or malware through Facebook if their accounts are infected. Do not click this material and do not run any ".exe" files on your computer without knowing what they are. Only log in to legitimate pages with the Facebook.com domain. For example, "www.facebook.example.com" is not a legitimate Facebook page, but "www.facebook.com/example" is a legitimate Facebook page because it has the "facebook.com" domain. When in doubt, you can always just type in "facebook.com" into your browser to return to the legitimate Facebook site. Also, be sure to use the most current version of your browser as it will contain important security warnings, protection features, and may warn you if you have navigated to a suspected phishing site.

You can find more information about phishing and online scams and viruses and how to avoid them at http://www.antiphishing.org/consumer_recs.html and www.getsafeonline.org



Facebook Security Guidance: <https://www.facebook.com/security>

General Concerns: Facebook Locations

<https://www.facebook.com/about/location/>

Sharing your location lets you tell family and friends where you are as you're posting. There are two main ways to do this.

1. Tell people you're at a specific place

To include a specific place when you post, like a restaurant or event, click the  icon and type in the name of the place or event. To say you're there with others, click the  icon and type in their names. As always, you can control who sees this post by choosing an audience before you publish it.

Others can add you to where they are, too. When friends tag you somewhere, that post shows up on your profile (timeline). If you want to review posts you're tagged in before they go on your profile (timeline), you can turn on Profile (Timeline) Review.

2. Include your general location

Instead of a specific place, you can choose to include the city or area you're in. This will appear next to the timestamp of your post. We'll suggest where you're nearby. If we're off or you don't want to say what city you're near, you can remove it by clicking the "x" that appears when you hover over the location tag.

You can also fill in your current city yourself. If you add your general location, it'll stay on for future posts until you shut it off. So, the next time you post, your general location will be added to that post. Once removed, it'll stay off until you add it back to your post.

How do I know when people tag me at a location or check me in somewhere?


You will receive a notification when you're tagged in a post, including those with location. You can also choose to approve all tags before they appear on your profile (timeline) by turning on Profile (Timeline) Review.

If you'd like, you can remove posts from your profile (timeline), remove a tag anytime, turn on the option to review all posts before they appear on your profile (timeline), or use the Profile (Timeline) Visibility setting to exclude some people from seeing tagged posts of you on your timeline.

How do I remove my location from a post before I share it?

We suggest a general location for your post. If our suggestion isn't accurate or you don't want to include it, you can remove it by clicking the "x" when you hover over the location tag. Then if you'd like, you can fill in your current city yourself.

How do I change or remove my location when I update my status on the iPhone or Android app?

Before you post your update, tap the  icon. If you want to **change** your location, you can select one of the places listed or search for one that's not listed. If you want to **remove** your location, tap the 'x' next to the current city at the bottom of the list.

General Concerns: Video Calling on Facebook

In July 2011, Facebook announced a partnership with Skype to add video calling to its service: <http://www.facebook.com/videocalling>

“What is Video Calling?”

Video calling allows you to talk to your Facebook friends face to face. All you need to do is to set-up the system and you're able to “call” any friend on Facebook. If your friend isn't available, you can leave them video message. You and your friend both need to have webcams and microphones set up and you will be able to see and hear each other in real time. If you call friends who don't have webcams, they'll be able to see and hear you but you'll only be able to hear them.

The time and date of each call you make is listed in your ongoing message history with each friend. The calls themselves are not recorded or saved. You can continue using chat and other Facebook features during your video call.

<https://www.facebook.com/help/video-calling>

“Who can I call on Facebook?”

Only your confirmed friends (people you have accepted onto your Facebook friends list) can call you on Facebook. You have the option to ignore any call you receive.

“How do I make myself unavailable for Video calling?”

When you are available for chat, you are also available for video calling. Keep in mind that only confirmed friends can call you on Facebook, and you always have the option to ignore any call you receive.

If you want to make yourself unavailable for video calling and chat:

1. Click the settings icon in the right corner of the chat list.
2. Click "Available to Chat" to remove the check mark.

“Can I block Specific friends from calling me?”

If you want to block a friend or group of friends from calling or chatting with you:

1. Create a friend list that includes the people you'd like to prevent from chatting with you.
2. Click the settings icon in the right corner of the chat list.
3. Select “Edit Availability...”
4. Check the box next to the friend list you'd like to appear unavailable to and click “Close”. You will no longer appear online to these friends.

To stop someone from contacting you, you can also unfriend the person or block the person from interacting with you in any way on Facebook.

“What can I do if someone is using Video Calling to harass me?”

Please keep in mind that only confirmed friends can call you on Facebook, and you always have the option to ignore any call you receive. If someone makes you uncomfortable, you can unfriend the person or block the person from interacting with you in any way on Facebook.

General Concerns: Other Queries

“How do I delete an account?”

If you deactivate your account from the "Deactivate Account" section on the Account page <https://www.facebook.com/editaccount.php>, your profile (timeline) and all information associated with it are immediately made inaccessible to other Facebook users. What this means is that you effectively disappear from the Facebook service. However, if you want to reactivate at some point, we do save your profile (timeline) information (friends, photos, interests, etc.), and your account will look just the way it did when you deactivated if you decide to reactivate it. Many users deactivate their accounts for temporary reasons and expect their information to be there when they return to the service.



If you do not think you will use Facebook again and would like your account deleted, please keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added. If you would like your account permanently deleted with no option for recovery, log in to your account and then submit your request here: <http://tinyurl.com/fbdeleteaccountform>

“How do I block someone?”

To block someone:

1. From your Account dropdown menu, select Privacy Settings (<http://www.facebook.com/settings/?tab=privacy>)
2. Next to Block Lists, click **Manage Block Lists**.
3. Enter the name or email address of the person you want to block in the appropriate field and click **Block**. People will **not** be notified when you block them.

If you can't find someone using this method, try going to the person's profile (timeline) page. You can block them by scrolling down to the bottom of the left column and clicking the "Report/Block This Person" link. Once you click this link, check the "Block this person" box and then click "Submit."

If you still can't block someone using the methods described above, it's possible that they have left Facebook or have restricted their privacy settings. You can still prevent them from viewing your profile (timeline) by adjusting your privacy settings (<http://www.facebook.com/help/?page=806>)

“What do I do if someone has posted a photo of me that I don't like?”

Facebook will only remove photos that violate our Statement of Rights and Responsibilities (e.g., pornography or copyrighted images). However, there are some things you can do if you don't like a photo of you on the site:

To remove your name from a particular photo, view the photo and click the "Remove Tag" link next to your name. It will no longer be linked to your profile (timeline) and your friend cannot "re-tag" you.

Remember that you can only be tagged in photos by your friends. If you are having problems with someone constantly tagging you in embarrassing photos, just remove them as a friend from the Friends page.

If you don't want the photo to be shown at all, please talk to the person who posted it. They should be respectful enough to remove unwanted photos. Unfortunately, Facebook cannot make users remove photos that do not violate our Statement of Rights and Responsibilities.

“What is tagging and how does it work?”

A tag links a person, page, or place to something you post, like a status update or a photo. For example, you can tag a photo to say who's in the photo or post a status update and say who you're with. Tagging people, pages and places in your posts lets others know more about who you're with, what's on your mind and where you are.

When **you tag someone**, they'll be notified unless you post to an audience of 'Only Me.' Also, if you or a friend tags someone in your post and it's set to Friends or more, the post is visible to the audience you selected plus friends of the tagged person.

When **someone adds a tag of you** to a post, your friends may see what you're tagged in on Facebook. The tagged post also goes on your profile (timeline). If you'd like, you can turn on Profile (timeline) Review (<http://tinyurl.com/profilereviewfb>) to review and approve each tagged post before it goes on your profile (timeline) or exclude some people from seeing tagged posts of you on your Wall.

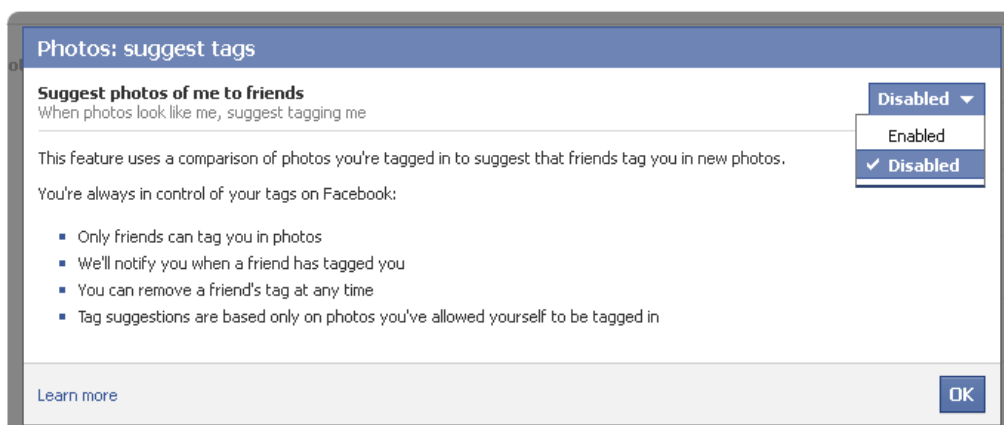
You can learn more about tagging here: <http://www.facebook.com/about/tagging>

“What is Facebook’s Facial Recognition?”

As your Facebook friends upload their albums, Facebook will try to determine if any of the pictures look like you (based on photos already tagged with your name). If they find what they believe to be a match, they may suggest that your friend tag the photo with your name.

Tag Suggestions are only made to people when they add new photos to the site, and only friends are suggested.

Users can choose to disable this feature in their privacy settings in the “Things others share” section by selecting the “Suggest Photos of me to my friends” option. You can then chose to enable to disable the feature.



“What are Friend lists?”

Friend Lists on Facebook enables users to choose what content is shared with specific groups of friends.

- **Smart lists** - smart lists create themselves and stay up-to-date based on profile info your friends have in common with you, like your work, school, family and city.
- **Close Friends and Acquaintances lists** - You can see your best friends' photos and posts in one place, and see less from people you're not as close to.
- **Better suggestions** - You can add the right friends to your lists without a lot of effort.

Friend Lists are completely optional. If you don't like lists, you don't have to use them.



Smart Lists

- Work
- School
- Family
- City

For instance, if you list Boston College as a school you've attended and your friends John and Sarah do too, then you would instantly have a smart list called "Boston College" with John and Sarah on it. This means that if you're having a college reunion, you can easily share photos with just your college friends, without bothering other people you know.

You can also add or remove friends manually to make the lists even more accurate.

Close Friends and Acquaintances Lists

- **Close Friends list** - Add your best friends to your Close Friends list and you'll see everything they post in News Feed. You can even jump straight to a view of your News Feed that only shows their photos and news. You can also receive notifications when they post updates, so you don't miss anything important.
- **Acquaintances list** - Add friends like old classmates or business contacts to your Acquaintances list and you'll see less of them in your News Feed. We'll still show you important things they post -- like when they get married or move to a new city -- so you don't lose touch completely.

You can add people to your Restricted list and they will only see your Public posts. You'll still be friends on Facebook so you can send them messages or tag them in a post if you want to connect to them from time to time.

Facebook doesn't create Close Friends and Acquaintances lists for you. Since these types of relationships are unique, it's important for you to decide who goes in your Close Friends, Acquaintances or Restricted lists - if you use them at all.

If you created your own lists in the past, you can still use them. You can also continue to create whatever lists you want in the future. When you post something to a list that you've created - including your Close Friends and Acquaintances lists - no one will be able to see the title of the list.

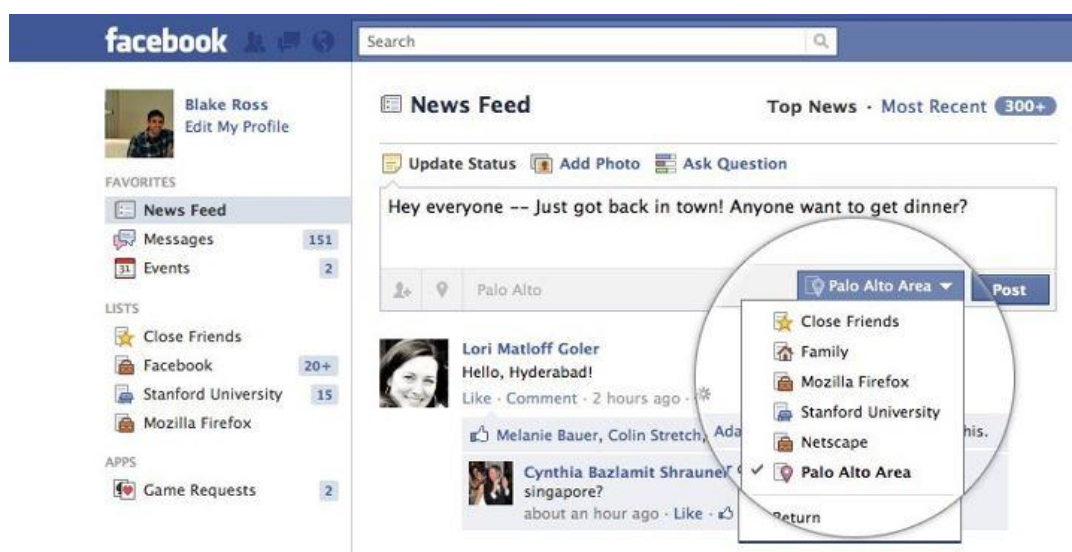
The people on the list you've shared with **will** be able to see each others' names. This gives them more context. For example, if I see that a post is shared with my five closest friends, I am much more likely to comment freely on it than I would be if I didn't know who else could see the post.

When you add someone as a friend or confirm a friendship request, you'll be able to add the friend to any of your existing lists.



Each of your lists has its own News Feed, where you can see just the photos, status updates and other posts from the people on the list. To view list News Feeds, look for the Lists section on the left side of your homepage and click the list you want to see.

Whenever you feel like sharing something with a narrower set of friends, simply use the dropdown audience selector in the sharing tool and pick one of your lists



You can also use lists to help control who sees what on your profile, using the audience selector next to each detail on your profile.

“How do I take a screen shot to document a problem?”

On a PC

With the content you want to save displayed on your screen:

1. Click the Print Screen button. (This button is located in different places. On many computers you'll find it in the upper right corner.)
2. Open Microsoft Paint: Select Start > All Programs > Accessories > Paint.
3. Click anywhere on the white part of the screen.
4. In the Edit menu at the top of your screen, select Paste.
5. Select File > Save As.
6. From the Save As menu in the pop-up box, select JPG.
7. Type in a filename for your image, choose a location on your hard drive to save to — many people choose the Desktop — and click Save.

On a MAC

With the content you want to save is displayed on your screen:

1. Simultaneously hold down the three keys: Shift and 4.
2. Press the spacebar. A camera icon will appear.
3. Tap the touchpad to take the picture. It should appear on your desktop as a file named Picture 1.

NB Additional Comment from e-Safety Officer: Do not take a screenshot of any indecent/illegal images of children. Report them to Facebook and use the web link to report the content to the Internet Watch Foundation www.iwf.org.uk

“What other Security Features does Facebook offer?”

Facebook offers a number of security features that help keep your personal information private, including remote logout, secure browsing, one-time password and more. Find all of these features on your Account Settings page, in the Account security section.

- Remote log out: Use remote logout to close any Facebook session that you may have left active on any computer or device, such as one at a cafe or your friend's house.
- Secure browsing: If you frequently use Facebook from unsecured public networks such as those in airports or cafes, consider enabling Facebook secure browsing, or HTTPS. This optional setting encrypts the information you send and receive. Read more about Facebook HTTPS here: <http://www.facebook.com/blog.php?post=486790652130>

<http://www.facebook.com/security>

“How can I make my profile/timeline private and find out more about online privacy?”

You can find detailed information on all of the privacy options offered by Facebook here: <http://www.facebook.com/help/?topic=privacy> and <http://www.facebook.com/settings/?tab=privacy>

To edit the privacy settings for your own Facebook account, choose the "Privacy Settings" option from the Account drop-down menu available from the top right corner of every page. From this page you can personalize your privacy settings for Profile (timeline) Information, Contact Information, Applications and Websites, and Search.

You can also read Facebook's Privacy Policy here: <http://www.facebook.com/about/privacy/>

Safety advice from Facebook

- Adjust your privacy settings to match your level of comfort, and review them often.
- Never share your password with anyone, and be cautious about posting and sharing personal information - especially information that could be used to identify you or locate you offline, such as your address or telephone number.
- Report users and content that violate our Statement of Rights and Responsibilities: <http://www.facebook.com/terms.php>
- Block and report anyone that sends you unwanted or inappropriate communications.

Remember that while Facebook has always been based on a real name culture, and using fake names is a violation of our policies, people are not always who they say they are. Use caution when accepting or sending friend requests, and keep in mind that it is always risky to meet anyone in person whom you don't know through real world friends.

Facebook Terms and Conditions

<http://www.facebook.com/terms.php>

e-Safety Officer Note: It is useful to refer to these terms when reporting inappropriate content or material or underage users to Facebook.

“Safety”

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments:

1. You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that is hateful, threatening, pornographic, or that contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third party application containing, or advertise or otherwise market alcohol-related or other mature content without appropriate age-based restrictions.
9. You will not offer any contest, giveaway, or sweepstakes ("promotion") on Facebook without our prior written consent. If we consent, you take full responsibility for the promotion, and will follow our Promotions Guidelines and all applicable laws.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack.
12. You will not facilitate or encourage any violations of this Statement.

"Registration and Account Security"

Facebook users provide their real names and information and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. You will not use your personal profile (timeline) for your own commercial gain (such as selling your status update to an advertiser).
- 3. You will not use Facebook if you are under 13.**
4. You will not use Facebook if you are a convicted sex offender.
5. You will keep your contact information accurate and up-to-date.
6. You will not share your password, let anyone else access your account, or do anything else that might jeopardize the security of your account.
7. You will not transfer your account to anyone without first getting our written permission.
8. If you select a username for your account we reserve the right to remove or reclaim it if we believe appropriate (such as when a trademark owner complains about a username that does not closely relate to a user's actual name).

Useful Links and Contacts

For help and guidance on issues or queries relating to Facebook, please visit <http://www.facebook.com/help/> and <http://www.facebook.com/safety/>

Other sources of help and advice for schools, parents/carers and young people

- www.thinkuknow.co.uk: register in teacher/trainer area to access resources
- www.ceop.police.uk
- www.virtualglobaltaskforce.com
- www.iwf.org.uk - Internet Watch Foundation
- www.childnet.com – Variety of excellent free resources for educators (KS1-4) and parents/carers – the “Know It All” covers parents/carers, primary, secondary, SEN and trainee teachers.
- www.bbc.co.uk/onlinesafety - BBC Portal and resources
- <http://en.teachtoday.eu> – Guidance, lesson plans and resources from Industry and teachers
- <http://clickcleverclicksafe.direct.gov.uk> – UKCCIS Click Clever Click Safe Campaign for CYP and parents/carers
- www.getsafeonline.org – Online Security advice
- www.go-on.co.uk – Free online Computer Courses
- www.digizen.org/cyberbullying: DCFS Guidance on Cyberbullying in School
- www.beatbullying.org
- www.cybermentors.org.uk - Free online mentoring from young people for young people
- www.childline.org.uk
- www.samaritans.org
- www.b-eat.co.uk
- www.youngminds.org.uk
- www.saferinternet.org.uk/helpline - UK Safer Internet Centre Professional Helpline

Kent County Council's e-Safety documents and resources can be found at www.kenttrustweb.org.uk?esafety

Schools and Settings in Kent can also contact the e-Safety Officer. esafetyofficer@kent.gov.uk or 01622 221469.