

Facebook: Information for Schools

What is Facebook?

Facebook is a popular Social Networking site www.facebook.com

Facebook is a US based company with over 500 million registered users - 20 million of which are in the UK.

Facebook is only for users aged over 13; however 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. 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. Ensure children know to behave online in all circumstance and these skills should carry over 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.

Useful Tips for Young People:

- Visit www.facebook.com/help/?safety=teens for advice on staying safe on Facebook
- Make sure all of your online profiles 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 that 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 picture – never post pictures of yourself or your friends or family in school uniform
- 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 or status it could be a virus or redirect 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

Facebook Click CEOP App

Facebook and the CEOP Centre have joined forces to make young people safer online by launching the new **Facebook 'ClickCEOP' application** <http://apps.facebook.com/clickceop/>

Launched on the 12th July, all young users of Facebook and parents/carers are invited to access the new ClickCEOP 'app' to their profile. They will be able to access advice, help and support directly from the CEOP Centre as well as Facebook. Crucially, young people will be able to report instances of suspected grooming or inappropriate sexual behaviour directly from their profile to specially trained investigators from CEOP. This is the outcome of collaboration between CEOP and Facebook who have combined Facebook's expertise in connecting and communicating online with CEOP's expertise in helping young people stay safe.

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. CEOP's new Facebook page (www.facebook.com/ClickCEOP) contains polls, news alerts and status updates. The page will look at topics that teenagers care about, such as celebrities, music and exams and will link these subjects to questions about online safety.

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.



If children 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 kept (e.g. messages, screen prints etc) to help ensure that the sanctions can be implemented. (See the Cyberbullying Section for advice on how to deal with Cyberbullying)

Many schools send letters to all parents reminding them about Facebook's age limit (13) and advising parents to speak with their children about safe internet use and to be aware if their child is using Facebook under age.

As Facebook is frequently blocked in school, the following information has been copied from Facebook based on frequently asked questions to help inform schools about actions they can take about young people on facebook and incidents of Cyberbullying.

Facebook Safety Centre: www.facebook.com/help/?safety

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

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

Facebook Information for Parents

www.facebook.com/help/?safety=parents features General Information, Addressing Personal Safety and Responding to Objectionable Content

“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 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 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

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

Facebook removes photos or videos that violate our Statement of Rights and Responsibilities in some way. You can report an abusive photo or video by using the "Report" links located near most pieces of content on the Facebook to report offensive material.

If your child is between the ages of 13 and 18, we will not be able to assist you directly, unless required by law. Please advise your child to log in to their own Facebook account and visit the Help Centre. They can take the appropriate steps from here to receive additional support.

If your child is under the age of 13, and you would like to request the removal of a photo containing an image of them, please do so here: <http://tiny.cc/underagephoto>

If your child is under the age of 13, and you would like to request the removal of non-photo content (i.e., a video) containing an image of them, please do so here: <http://tiny.cc/underagecontent>

We will remove a photo of your child that you report to us provided that your child is pictured in the photo, is under 13 years old, and you have filled out the appropriate contact form in its entirety.

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.

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

All abuse reports on Facebook are confidential. The user that you are reporting will not know that you have reported them. After the report is submitted, Facebook investigates the issue and makes a determination as to whether or not the content should remain on the site based on our **Statement of Rights and Responsibilities**. In certain situations, the circumstances require more severe action. For instance, users who repeatedly violate our Statement of Rights and Responsibilities can be permanently banned from the site.

Please be aware that not all reported content will be removed. A Facebook administrator looks into each report thoroughly in order to decide the appropriate course of action. If no violation of our Statement of Rights and Responsibilities has occurred, then no action will be taken.

“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 four global privacy setting groupings (Everyone, Recommended, Friends of friends or Friends only) 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://tiny.cc/facebookprivacyex>

“How does Facebook privacy work for minors (under 18s)?”

Minors (anyone under 18) who use Facebook have a slightly different experience with privacy than adults. Both adults and minors have some basic information (name, profile picture, gender and networks) appear when people navigate to their profile. This information may be accessed by applications that they and their friends use. Adults and minors both appear in search results on Facebook. However, minors do not have public search listings (can be found via public search engines) created for them.

The "Everyone" setting works differently for minors than it does for adults. When minors set information like photos or status updates to be visible to "Everyone," that information is actually only visible to their friends, friends of friends, and people in any verified school or work networks they have joined. The only exceptions are for "Search for me on Facebook" and "Send me friend requests", where if the minor has set those to "Everyone", we respect the "Everyone" setting.

(NB this does rely on the fact that children register using their correct date of birth)

“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 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 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.
- Make sure your child understands that online actions can have offline consequences.
- Visit www.facebook.com/help/?safety=parents
- 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 Places

www.facebook.com/help/?page=1080

What is Facebook Places?

“Places” is a location based Facebook feature. “Places” allows Facebook users to see where their friends are and share their location in the real world using a GPS (Global Positioning System) enabled device such as a mobile phone. When you use Places, you can see if any friends are currently “checked in” and located nearby. You can “check into” nearby Places to tell your friends where you are, tag your friends in the Places you visit, and view comments your friends have made about Places you visit. Facebook “Places” aims to enable users to connect with people in a new way and make real life links and if you are responsible and careful there can be some benefits to most users. However, “Places” does bring about several privacy and security risks especially for children or more vulnerable adults, as they may not consider the full implications and consequences of sharing either their own or their friends’ real world location online.

Your location is not automatically shared by Facebook and is only shared when you (or your friends) check in to a Place. Facebook users have control over whether and with whom they share check-ins. However Facebook “Places” is an Opt Out rather than Opt in application, so all users need to be aware how to ensure they use it appropriately (if at all).

How can I change the settings?

In the “Customize settings” section of your main privacy settings, select the drop-down box next to “Places I check in to” and select one of the four recommended settings: Everyone, Friends and Networks, Friends of Friends, or Friends Only. Alternatively, you can make the locations you check in to visible to or hidden from specific people by clicking “Custom” - you can also choose “only me” which is the most restrictive setting and is the closest option to opting out.

If you don't want your friends to be able to check you into Places, (meaning friends can share your current location with others), then select the drop down box in “Things Others Share” called “Friends can check me in to Places.” If you don't want your friends to be able to “check” you into places then set this to “Disabled”. Keep in mind that if you enable this setting then any friend could potentially check you in any place even if you are not there. If a friend has tagged you in a Place and you would like to remove your name, then go to the Place story (which can be found on your profile, your friend's profile, or the Place page) and select “Remove Tag.” You will no longer be connected to that Place. Only your confirmed friends on Facebook are able to tag you in a Place and only if you have enabled them to do so.

How does Places Privacy work for Users who are under 18?

Facebook have reduced the visibility of information for anyone under 18 (assuming they signed up with the correct date of birth). With the Places application in particular, under 18s will only be able to share their locations with people on their friends list on Facebook (it is essential that young people understand this when accepting online friends or setting up a profile). Even if they have set all other information on their profile as visible to “Everyone”, the settings for places will automatically be restricted and only their friends list will be able to see Places he or she has visited.

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 profiles that look suspicious. Facebook is based on a real-name culture, and fake profiles 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. 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. 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.

You can also change your privacy settings if you are uncomfortable being found in searches or having your profile 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.

Reporting Abusive Content

www.facebook.com/help/?safety

“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 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.

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, go to the profile and click "Report/Block this Person" in the left column below the profile 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.

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

You can report a profile that violates Facebook's Statement of Rights and Responsibilities by clicking the "Report/Block this Person" link in the left column of the profile, selecting "Fake profile" as the reason, and adding the appropriate information.

The following categories of profiles are prohibited on the site:

- Profiles that impersonate you or someone else
- Profiles that use your photos
- Profiles that list a fake name
- Profiles that do not represent a real person
- Profiles that have been hacked
-

Be sure to choose the correct report type to help us verify the 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.

Information for Educators

www.facebook.com/help/?safety=educators : Features General Information, Addressing Personal Safety and Responding to Objectionable Content

“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.

“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.

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.

<http://www.facebook.com/help/?faq=16908>

“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, go to the profile and click "Report/Block this Person" in the left column below the profile 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?”

If you are a teacher and have a personal profile, you can consider creating a group or a Page specifically for interacting with students, parents, or colleagues.

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)

Some ideas to consider:

Pages: Pages are for broadcasting information to people on Facebook. For example, you could create a Page called "Ms. Smith's 9th Grade Science Class" where you post daily homework assignments. Anyone can become a fan of a Page on Facebook. People who choose to become a fan of a Page will see updates on their profile.

To create a Page, click here www.facebook.com/pages/create.php

Pages are free, you can control them with your personal profile, and they keep your profile separate from your students.

Groups: Groups make it easy for members of a community to connect, share and even collaborate on a given topic or idea. For example, you could create a group called "American Literature 101 Discussions" where you and your students can contribute to group discussions. Or you could create a group for all of the educators in your department to collaborate on lesson plans and share ideas.

To create a group, click here www.facebook.com/groups/create.php

Friend Lists: Friend Lists provide organized groupings of your friends on Facebook. For example, you can create a Friend List specifically for your students. Then you can control which parts of your profile are visible to this entire list. You can also filter your view of each list's stream of activity separately on the home page, or send messages and invites to this group of people all at once. To learn more about creating and managing Friend Lists, click here www.facebook.com/help/?page=768

“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.

“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>

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

Compromised and Hacked Accounts

“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 also find more information about phishing and how to avoid it at http://www.antiphishing.org/consumer_recs.html and www.getsafeonline.org

Other queries

How do I delete my account?

If you deactivate your account from the "Deactivate Account" section on the Account page <https://www.facebook.com/editaccount.php>, your profile 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 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: https://www.facebook.com/help/contact.php?show_form=delete_account

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

You can report an application for abuse by clicking "Report/Contact this Application" at the bottom of any canvas page within the application.

If you are not currently using the application but would like to report it, simply go to the application's Profile Page on Facebook, and click "Report Application" towards the bottom of the left column. To get to the Profile Page, follow these steps:

1. Enter the application's name in Search.
2. Scroll down and click to see more results. (Do not click on the application's "Game" result — this will take you to the application's Canvas Page rather than its Profile Page.)
3. You should be able to locate the application that you're looking for under Applications. Click the "View Application" to the right of the search result to view the application's Profile Page.

In addition, we'd recommend that you contact the developer who created the application directly so they're aware of your report. You can report this to the developer by going to the application's Profile Page and clicking "Contact Developer" towards the bottom of the left column, or by clicking "Report/Contact this Application" at the bottom of any canvas page within the application.

How can I make my profile 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/?page=25#!/privacy/explanation.php>

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 Information, Contact Information, Applications and Websites, and Search. For more information on the privacy settings offered by Facebook as well as answers to common questions about privacy, please refer to the [Privacy section](#) of the Help Centre. <http://www.facebook.com/help/?page=419>

You can also read Facebook's Privacy Policy [here](#):
<http://www.facebook.com/help/?safety=general#!/policy.php>

Safety advice from Facebook

- Adjust your [privacy settings](#) to match your level of comfort, and review them often.
<http://www.facebook.com/help/?safety=general#!/settings/?tab=privacy>
- 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/help/?safety=general#!/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

www.facebook.com/terms.php?ref=pf

NB: 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 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).