A Parents Guide to Device Safety

CYPSC
CHILDREN & YOUNG PEOPLE'S SERVICES COMMITTEES
Wicklow

CYPSC
CHILDREN & YOUNG PEOPLE'S SERVICES COMMITTEES
Wicklow

The following information is brought to you by Co. Wicklow Children and Youth People's Services Committee [CYPSC]. This booklet aims to provide a range of information on how to keep children safe online and how to protect their personal information from predators and hackers. If you require further information please visit www.webwise.ie where you will find information, advice and free education resources addressing a range of internet safety issues and concerns. Webwise offer advice and support for young people, teachers and parents.

The information in this booklet has been reproduced from 'A Parents' Guide to Device Safety' by kind permission of its authors and we acknowledge their work from which we have borrowed completely. The development of the Donegal booklet was a project of the Safe and Secure Subcommittee of the Donegal CYPSC. The project was led by Donegal Youth Service and supported by Donegal CYPSC through seed funding from the Department of Children and Youth Affairs.

Donegal Youth Service
Youth Work Ireland

CYPSC
CHILDREN & YOUNG PEOPLE'S SERVICES COMMITTEES
Donegal

For more information on Co. Wicklow CYPSC please contact:

Fionnuala Curry, Co-ordinator
fionnuala.curry@tusla.ie or visit www.cypsc.ie

087 6043511

Tusla, Wicklow Primary Healthcare Centre, Knockrobin, Rathnew, Co. Wicklow

TABLE OF CONTENTS

Secure Apps 3
Parental Controls 7
Restriction settings 9-11
Bluetooth 12-14
Facebook Privacy 15
Privacy settings 19-20
Setting up an e-email 23-24
Scams 25-26
Youtube SafeSearch 28-29
Xbox 31-37
Playstation 4 38-42
Nintendo Switch 43-47
Location 46
Location Settings on Android 47
Location settings on iOS 48
How to delete Location history 50

MOBILE PHONES & TABLETS

WHAT IS AN APP?

A mobile application, commonly refered to as an app, is a type of application software design to run on a mobile device.

SECURE APPS

MAKING YOUR MOBILE DEVICE SAFE

"Qustodio" Parental Control

With Qustodio you'll have more information to help protect your kids against the ever growing number of serious online issues such as viewing inappropriate content, cyberbullying, cyberpredators and screen addiction. With the online dashboard and Parents' app you'll be able to see how your child uses devices, apps and the web. Works on Windows, Mac OS X, Android, iOS and Kindle.

COST: FREE / Year Pricing Plans from €29.95

PROS: Each child's settings apply to multiple devices. There is a time scheduler for Internet, device use, applications. Offers powerful social monitoring location, call blocking, panic button for the Android version.

CONS: iOS edition limited in features. No gaming control. The parental notification are sent only by email, not text.

"Kaspersky Safe Kids"

Offers well-rounded, very affordable parental control and monitoring, and it doesn't limit the number of child profiles or devices you can cover. It's an excellent choice.

COST: FREE / €14.95

PROS: No limit on devices or child profiles. Flexible control of your device usage time. The content filter can block bad sites or just warn. Geofencing for mobile devices. Extensive alert system. Social network monitoring. Can block or time-limit apps. Inexpensive.

CONS: Call and text monitoring is Android-only. No application control under iOS.

Norton Family Premier

Lets parents track and manage their children's use of Windows, Android, and iOS devices. Its completely Web-based configuration and wealth of features make it a great choice for parental control.

COST: FREE / €39.99

PROS: Settings apply across Windows, Android, and iOS devices. There are no specific limit on number of devices. Flexible content filtering. It also has video tracking. Controls SMS contacts on Android. There is also location supervision via mobile devices. configuration and reporting. Most features available in free edition.

CONS: No Mac support. Limited iOS support. Limited social media tracking.

ContentWatch Net Nanny 7

With configuration and reporting moved to the Web, ContentWatch Net Nanny 7 is a full at home in the modern multi-device world of parental control, and it still has some of the the best content filtering around. The Net Nanny 7 programme is a parental control that is recommended Editors' Choice.

COST: Family Pass $74.99 / €66 Euro per year (Covers 5 devices)

PROS: Supports Windows, Mac, Android. Web-based configuration and reporting. Powerful filtering. Cross-device Internet time allowance. Email notifications. App control for Android mobile devices. Most features available in free edition.

CONS: Some minor features of previous edition omitted. No comparable iOS support.

PLEASE NOTE!

The free versions of all apps will have limited options compared to their paid for counterparts. The Reviews listed above are based on the Premium 'Paid' versions of the apps.

For more options please visit:
https://uk.pcmag.com/parental-control-monitoring/79219/the-best-parental-controlapps-for-your-phone

WHAT ARE PARENTAL CONTROLS?

Parental controls are features which may be included in digital television services, computer and video games, mobile devices and software that allow parents to restrict the access of content to their children.

How do I set up parental controls on Android?

1.

On the device you want parental controls on, open the Play Store app.

2.
In the top left corner, tap Menu Settings Parental controls. Turn “Parental controls” On.

3.
Then create a PIN. You then have the option to choose what content you want to filter or restrict.

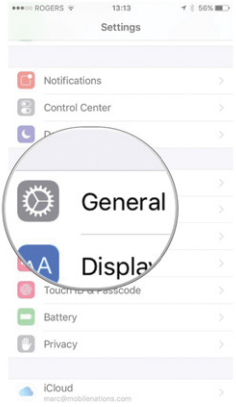
DID YOU KNOW?

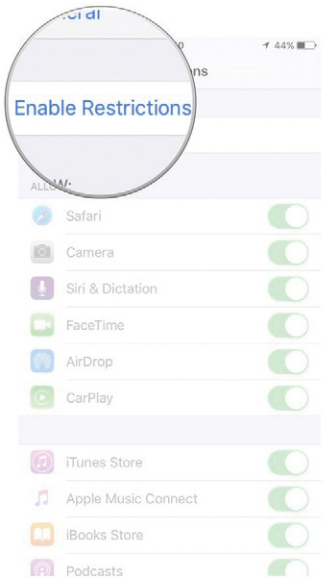
Ireland has determined 13 as the age of digital consent for data purposes, but in an annual report by Cybersafety Ireland, 52% of 11-12 year olds had a social media profile and one in five 9-10 year olds have a social media profile.

How do I set up parental controls on iOS 11 or earlier?

1. Launch the Settings app on your iPhone or iPad.

2. Then Tap on “General”.
Tap on “Restrictions”.
Tap on “Enable Restrictions”.





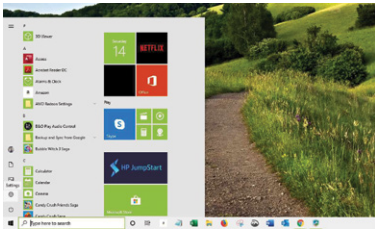
3. Type in a passcode. Make sure it is a passcode you will remember as you will need it for when you need to disable restrictions again.

PARENTAL CONTROL ON PC

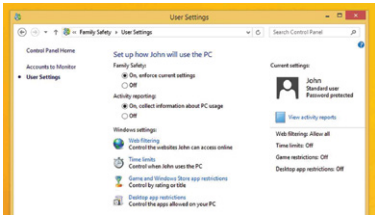
DID YOU KNOW?

32% of children have either never spoken to their parents/guardians about online safety or have not done so in the last year.

Cybersafety Ireland (2017 statistics)



1. First open control panel. You can open it using the Start menu. Click the bottom-left Start button on your desktop to open the start menu, type control panel in the search box and select *Control Panel* in the search results.



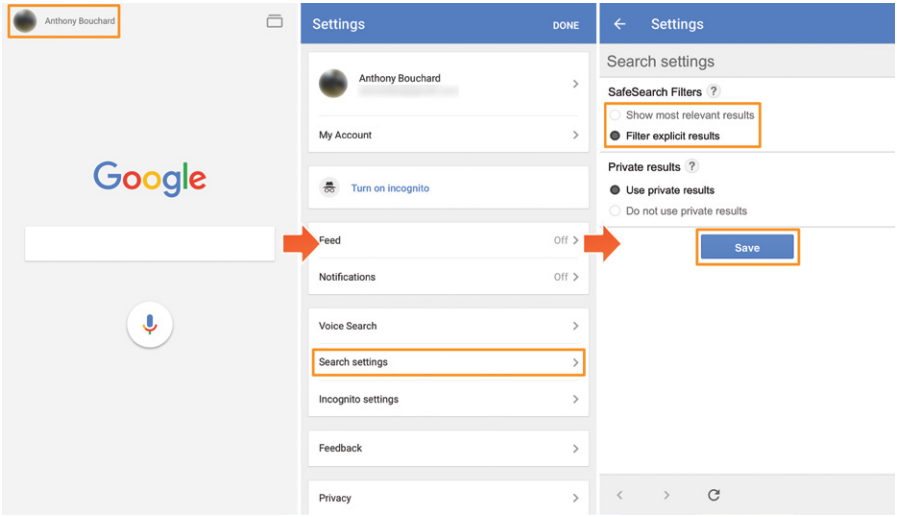
2. Click on *User Accounts* and *Family Safety*, then click on *Set Up Parental Controls For Any User*. Click the child's account.

Under Parental Controls, click On, *Enforce Current Settings*. Under Activity Reporting, click On, *Collect Information About PC Usage*.

For more information on limiting settings go to: www.laptopmag.com/articles/limited-user-accounts-windows-10

GOOGLE SAFESEARCH

How to access google safe search on mobile



How to set up Parental controls in Chrome browser

1. Open your Chrome browser.

2. Click on the main menu button, located in the upper right-hand corner and represented by three vertically-aligned dots.

3. Chrome's Settings interface should now be displayed in a new tab.

ADDING RESTRICTION SETTINGS

Set Content & Privacy Restrictio ns on iPhone

1. Go to *Settings* and tap *Screen Time*.

2. Tap Continue, then choose *"This is My [Device]"* or *"This is My Child's [Device]"*.

   > If you're the parent or guardian of your device and want to prevent another family member from changing your settings, tap *Use Screen Time Passcode* to create a passcode. Then re-enter the passcode to confirm.

   > If you're setting up Screen Time on your child's device, follow the prompts until you get to *Parent Passcode* and enter a passcode. Re-enter the passcode to confirm.

3. Tap *Content & Privacy Restrictions*. If asked, enter your passcode, then turn on *Content & Privacy*.

Prevent iTunes & App Store purchases

You can also prevent your child from being able to install or delete apps, make in-app purchases, and more. To prevent iTunes & App Store purchases or downloads:

1. Go to Settings and tap *Screen Time*.

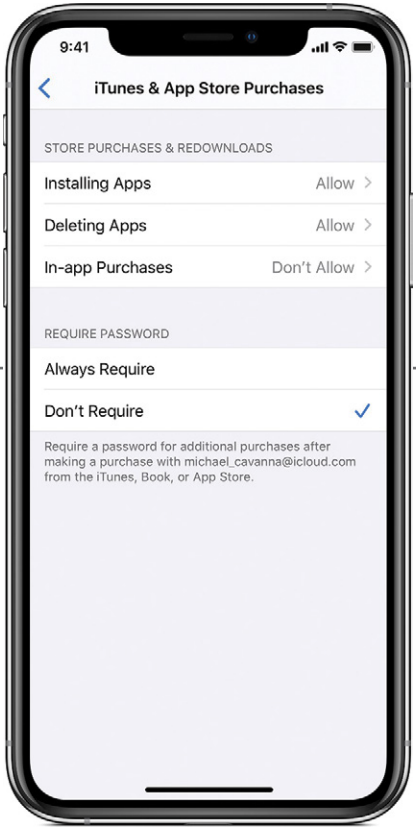
2. Tap *Content & Privacy Restrictions*. If asked, enter your passcode.

3. Tap iTunes & *App Store Purchases*.

4. Go to Settings and tap *Screen Time*. Tap *Content & Privacy Restrictions*. If asked, enter your passcode.

5. Tap iTunes & App Store Purchases. Choose a setting and set to *Don't Allow*.

You can also change your password settings for additional purchases from the iTunes & App Store or Book Store. Follow steps 1-3, then choose Always Require or Don't Require.

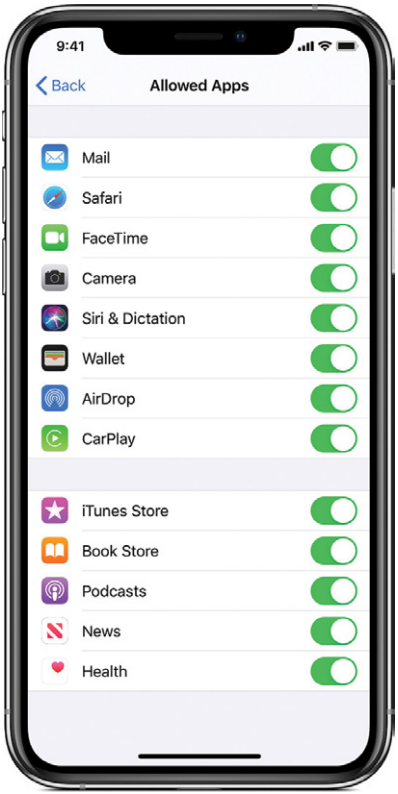


HOW TO ALLOW BUILT-IN APPS AND FEATURES ON IOS

You can restrict the use of built-in apps or features. If you turn off an app or feature, it won't delete it, it's just temporarily hidden from your Home screen. For example, if you turn off Mail, the Mail app won't appear on your Home Screen until you turn it back on.

To change your Allowed Apps:

1. Go to Settings > *Screen Time*.
2. Tap *Content & Privacy Restrictions*.
3. Enter your Screen Time passcode.
4. Tap *Allowed Apps*.
5. Select the apps that you want to allow.

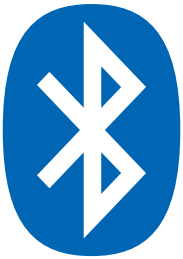


DID YOU KNOW?

"When we asked children the question about when they had last spoken to a parent or care-giver about online safety, we found that almost a third of children had rarely or never spoken to them?"

Cybersafety Ireland (2017 statistics)

BLUETOOTH



Bluetooth is a simple way for smartphones, printers, PCs, digital cameras, and other gadgets to link together over relatively shortdistances using wireless (radio wave) technology.

On Android

All Android devices feature a Bluetooth toggle switch in the Settings menu. To access the option, go to the Home screen, tap the “Apps” button” and open the “Settings” app. The Settings app will display a “Bluetooth” toggle button under the “Wireless and networks” subheading that you can to enable and disable Bluetooth.

Some Android devices like the Samsung Galaxy S series, Google Nexus series, Motorola Moto X and HTC One include a shortcut on the Status bar drop-down menu that when tapped enables or disables Bluetooth for the device.

People who find themselves frequently toggling Bluetooth power can make the process faster by installing a Bluetooth toggle widget on the Home screen. The toggle widget does the same thing as the toggle options in the Settings menu, but is easily accessible.

Apps like the Bluetooth Toggle Widget, Bluetooth Switch and Bluetooth Settings launcher enable the toggle button on the home screen.

To add widgets, press and hold an empty space on the home screen, select “Widgets,” press the widget and drag it to the home screen. If this doesn’t work, see if there’s a Widgets tab in the Apps drawer and add it from there.

BLUETOOTH SAFETY

How to turn on/ turn off bluetooth on iPhone

1. Go to Settings on your iOS device home screen.

2. Tap on Bluetooth.

3. Now turn toggle Bluetooth On.

If you ever want to turn off Bluetooth, then just follow above steps and turn Bluetooth to off.

DID YOU KNOW?

27% of teenagers aged 13-18 feel the need to hide what they view online from parents.

Digital families 2015 Survey:

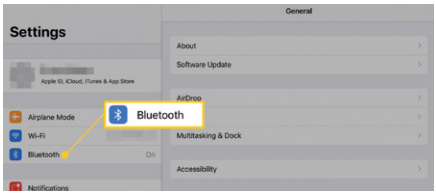
SETUP OPTIONS

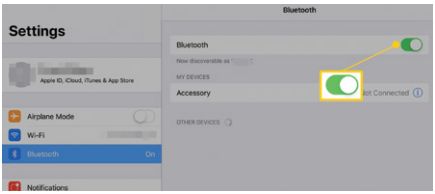
1. Turn on, or enable, Bluetooth.

2. Ensure your device is 'visible' and not 'hidden', so other nearby devices can pick up the signal.

3. Give your device a name to identify it when connecting to other compatible equipment.

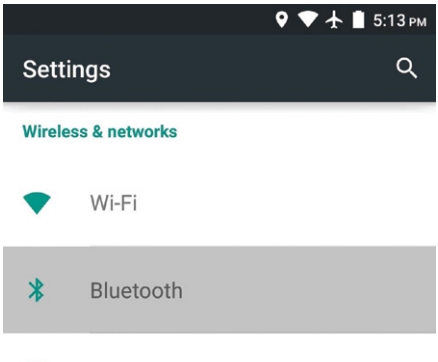
IOS SYSTEM

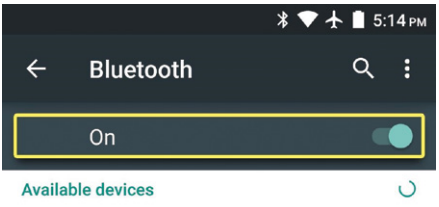




WINDOWS SYSTEM

ANDROID SYSTEM





For a more indepth step by step tutorial on setting up bluetooth on your device please go to: www.wikihow.com/Set-up-Bluetooth

FACEBOOK PRIVACY

DANGERS ON FACEBOOK

Facebook is the most popular social media app to date; in 2018 the app exceeded 2 billion daily users who chose the platform as their primary source of communication especially through Messenger, which can also double up as a live video chat.

Many young people are not using appropriate privacy features; some have not been honest about their age when gaining access to Facebook (who do make a huge effort to ensure appropriate use).

By using Facebook as an adult date of birth, many other apps intended for adults can be accessed which can expose young people indirectly to adult content and possibly strangers.

Facebook claims it has over 400 million users. Facebook came under fire in 2010, when 15 privacy and consumer protection organisations filed a complaint with the Federal Trade Commission, charging that the site, among other things, manipulates privacy settings to make users' personal information available for commercial use. Also, some Facebook users found that their private chats were accessible to everyone on their contact list in a major security breach that's left a lot of people wondering just how secure the site is.

There are 5 things you should be wary of when it comes to facebook. These are:

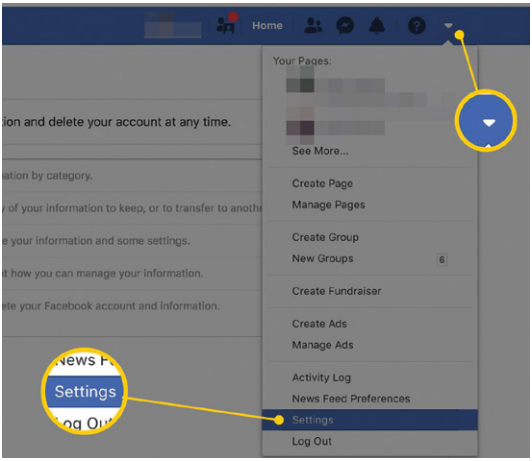
- Your information is being shared with third parties
- Privacy settings revert to a less safe default mode after each redesign
- Facebook ads may contain malware
- Your real friends unknowingly make you vulnerable
- Scammers are creating fake profiles.

Source: https://www.cbsnews.com/news/five-hidden-dangers-of-facebook/

FACEBOOK PRIVACY SETTINGS ON PC

Facebook offers privacy settings to hide content or posts from strangers. It also allows you to change who you can accept friend requests for, such as only allowing friend requests from people who have mutual friends.
The following steps are for facebook 2018 version on desktop.

1. In the top right hand corner of the window, click on the arrow. Then select 'Settings'

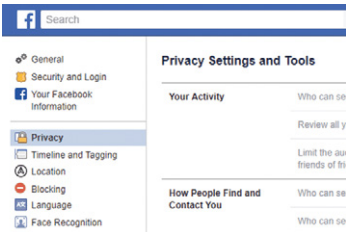


DID YOU KNOW?

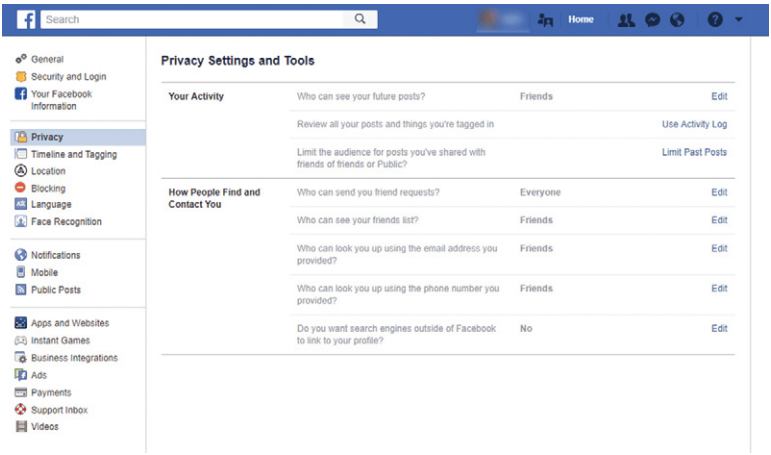
"22% of the children surveyed were in online contact with strangers. Most of these (14%) reported that they were in contact at least once a week and 6% of this number every day".

Cybersafety Ireland (2017 statistics)

2. On the left hand side of the page, select ‘Privacy’.

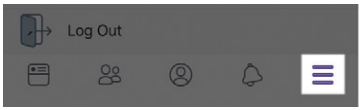


3. You will be able to set the limits to your childs account here. Such as who can send friend requests, and who can view their posts. Click on the ‘EDIT’ to change the settings on each option.

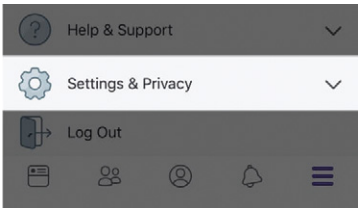


FACEBOOK PRIVACY SETTINGS ON MOBILE

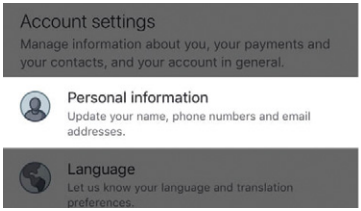
1. On mobile tap on the menu icon on the top right hand side. The menu icon is indicated as 3 horizontal lines.



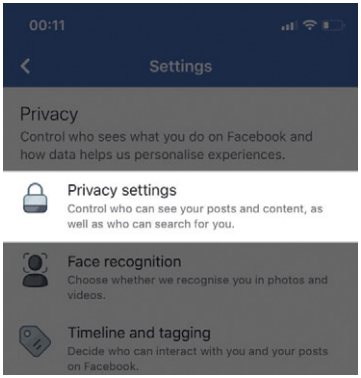
2. Scroll down until you reach 'Settings & Privacy". Tap on it once and select 'Settings'.



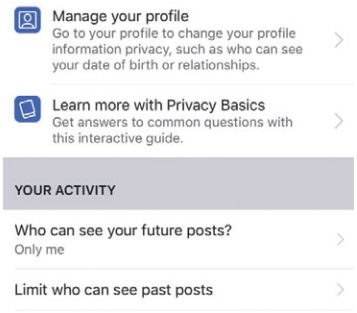
3. To add restrictions on your account, tap 'Personal Information'. If you wish to change the password, you can scroll down to security options and change it from here. You can also change many other settings here, but to add restrictions to your childs account, tap on Personal infomation.



4. Here you can manage a range of options, such as if you want facebook to recognise you in photos or videos, tags appearing on your timeline, your public posts (visible to people who are not your friend on facebook), and see the people who you have blocked. For the interest of this guide, we will be tapping on *Privacy Settings*.



5. From the Privacy Settings you can change your facebook profiles privacy settings.
You can also learn more about the Privacy basics and review who can see your profiles information and posts to find how to better protect both your private details and your childs.



If you have anymore questions, you can visit: www.facebook.com/help/445588775451827

EMAILS

EMAIL DANGERS

1. Malware

To protect against viruses that were spread via email in the early days, anti-spam solutions would block any executable files that were included as attachments. Others go with the strategy of not opening any attachments unless they were scanned by email anti-virus software first. Most companies still employ these security features; however they are not enough. Some Cyber criminals have learned that they can continue to spread malware via email using:

- Links to malicious websites
- Masquerading the file extension
- Creating malware and viruses that automatically launch when the email is opened.

Not only have these cyber attacks grown in their level of sophistication, but the level of damage that they can do has grown substantially over the years.

2. Phishing

Phishing first came to popularity when people used it to steal AOL account information via instant messaging in the earlier days of the internet. Scammers send emails that are identical to those sent by a bank, for ex. links embedded in emails direct those who click on them to websites that are almost exact counterfeitsmaking it almost impossible for the unsuspecting user to know that they are being scammed. Without the advanced technologies that can identify possible phishing scams, without preventing legitimate emails from being delivered, corporate email users can easily find confidentiality of their user credentials at risk.

3. Spam

Spam levels have fluctuated over the past few years, but more than 75% of email is considered to be spam in one form or another.

Spam is still a headache for businesses because it: impacts on storage resources, means time wasted sifting through emails.

Source: http://www.gju.edu.jo/sites/default/files/Information%20Systems%20and%20Technology%20Center/3_email_security_dangers_you_need_to_look_out_for.pdf

SETTING UP AN EMAIL

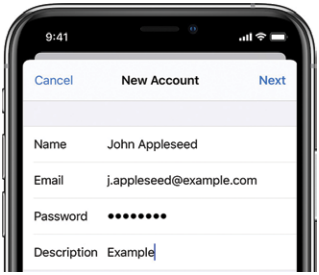
Short for electronic mail, email is an Internet service that allows people who have an e-mail address (accounts) to send and receive electronic letters.

Add an email account to your Apple device

1. Tap on the Mail Icon ( ) on the home screen. To access the home screen press the home button on the front of the Ipad.

2. Tap on type of account you would like to use, such as: Microsoft Exchange, MobileMe, Gmail, Yahoo! Mail, AOL, or Other.

3. Enter your Email account information. Then tap *Next*, Mail will will try to find the email settings and finish your account setup. If Mail finds your email settings, tap *Done* to complete your account setup.



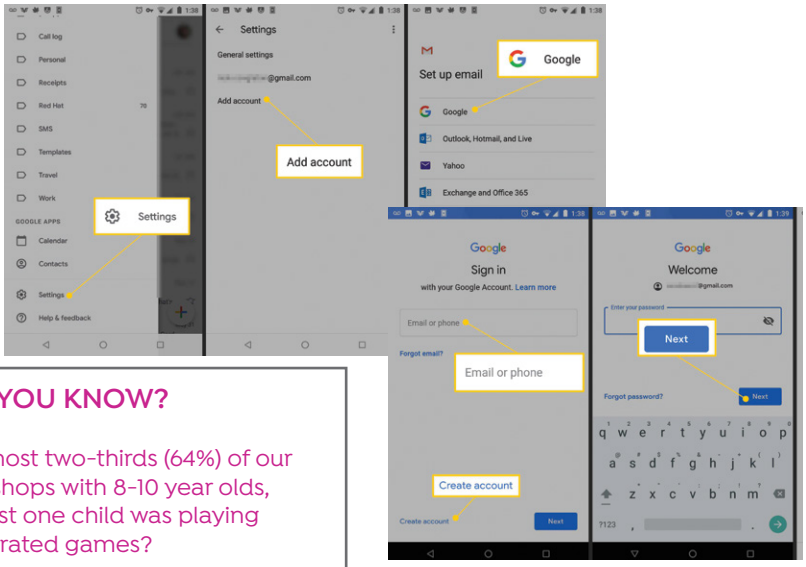
Add an email account on your Android device

1. Make sure you have Gmail installed on your device. Go to Settings > Accounts & Sync. Then tap *Add Account* and choose Google. Now tap "New" on the page to add a Google Account.

2. Type the name and tap "Next". Input email and user name, which then becomes your Gmail address. Tap "Next" and your phone will connect to the network to see if the e-mail address is OK.

3. Tap the password field and enter a password for the account. Re-enter the password for confirmation. Tap "Next" and input a recovery email for this Gmail account.

4. Tap "Next" where you can Join Google+ or touch "Not now". Then agree to Google Terms of service. Now you have a Gmail account.



DID YOU KNOW?

In almost two-thirds (64%) of our workshops with 8-10 year olds, at least one child was playing adult rated games?

Source: https://www.androidphonesoft.com/resources/set-up-gmail-on-android.html

EMAIL SCAMS - HOW TO SPOT A SCAM!

1. The email has improper spelling or grammar

This is one of the most common signs that an email isn't legitimate. Sometimes, the mistake is easy to spot, such as 'Dear eBay Costumer' instead of 'Dear eBay Customer.' Others might be more difficult to spot, so make sure to look at the email in closer detail. Legitimate organisations would have editors who review their marketing emails carefully before sending it out. So when in doubt, check the email closely for misspellings and improper grammar.

2. The hyperlinked URL is different from the one shown

The hypertext link in a phishing email may include, say, the name of a legitimate bank. But when you hover the mouse over the link (without clicking it), you may discover in a small pop-up window that the actual URL differs from the one displayed and doesn't

contain the bank's name. Similarly, you can hover your mouse over the address in the 'from' field to see if the website domain matches that of the organisation the email is supposed to have been sent from.

3. The email urges you to take immediate action

Often, a phishing email tries to trick you into clicking a link by claiming that your account has been closed or put on hold, or that there's been fraudulent activity requiring your immediate attention. It is possible you may receive a legitimate message informing you to take action on your account. To be safe

For more information visit:
www.zonealarm.com/blog/2014/07/7-ways-to-spot-phishing-scam/

though, don't click the link in the email no matter how authentic it appears to be. Instead, log into the account in question directly by visiting the appropriate website, then check your account status.

4. The email requests for personal information

Reputable organisations don't ask their customers for personal information via email. If you have a checking account, your bank already knows your account number.

5. The email says you've won a contest you haven't entered

A common phishing scam is to send an email informing recipients they've won a lottery or some other prize. All they have to do is click the link and enter their personal information online. Chances are, if you've never bought a lottery ticket or entered to win a prize, the email is a scam.

6. The email asks you to make a donation

As unbelievable as it may seem, scam artists often send out phishing emails inviting recipients to donate to a worthy cause after a natural or other tragedy. For example, after Hurricane Katrina, the American Red Cross reported more than 15 fraudulent websites were designed to look like legitimate Red Cross appeals for relief efforts. Potential victims received phishing emails asking them to donate to the Red Cross, with links to malicious sites that stole their credit card numbers. If you'd like to make a donation to a charity, do so by visiting their website directly.

7. The email includes suspicious attachments

It would be highly unusual for a legitimate organisation to send you an email with an attachment, unless it's a document you've requested. As always, if you receive an email that looks in any way suspicious, never click to download the attachment, as it could be malware.

For more information visit:
www.wikihow.com/Spot-an-Email-Hoax-or-Phishing-Scam

YOUTUBE SAFETY

YOUTUBE SAFE SEARCH

YouTube is a platform that allows people to create any content they like, some of which is questionable material regardless of filtering. There are however some ways of making it a little safer using YouTube's Restricted Mode (formally called Safety Mode).

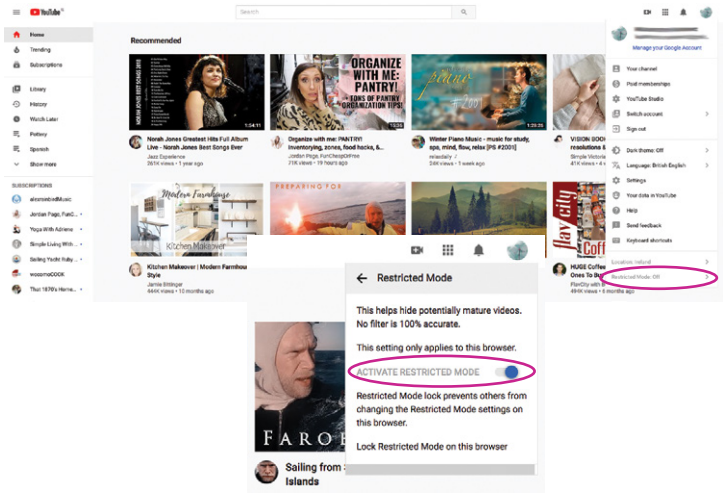
How to Activate Parental Controls When Searching Directly on YouTube.com

1. To implement the *Restricted Mode* for YouTube, go to YouTube.com and click on your Account picture, situated on the top, right menu.

2. You will see a reference to *Restricted Mode*: Off.

3. Click the arrow and details about '*Restricted Mode*' will appear.

4. Clicking *On* beside '*Activate Restricted Mode*'.

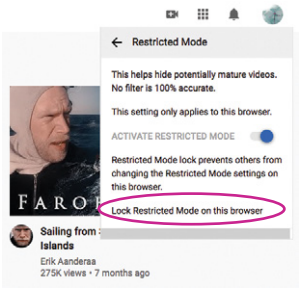


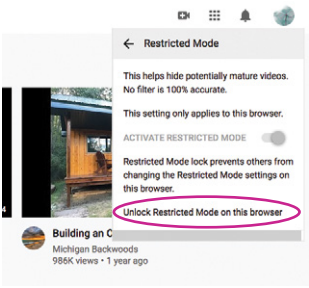
Locking YouTube Safe Search

You will need a Google account to use YouTube. If you have a Gmail account you will already have a google account and can log in to YouTube with your Gmail account login information. See the previous section to see how to create a Gmail account.

Now while logged in, return to YouTube and click on your Account picture and scroll down to the to the *Restricted Mode* link. Click the 'Lock Restricted Mode on this browser' to lock the safe search on YouTube. The page will reload and the YouTube parental control for the video search results are turned on for the system. Restricted Mode is now activated you can now log out of your account. Unlocking restricted mode on YouTube will require you to log into your account. This guarantees that no one else can deactivate the safety setting.

Important: If you have more than one browser on your computer, you will need to follow these steps for each browser.

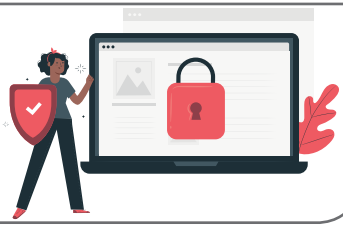




DID YOU KNOW?

28% of children aged 11-12 had looked at pornography online.

CyberSafeIreland Annual Report 2017



Source: https://mashtips.com/set-safe-search-youtube/

VIDEO GAME CONSOLES

XBOX ONE
XBOX ONE S, XBOX ONE X MODELS

Online safety and privacy settings for parents and children

Xbox One has age-appropriate controls and settings that you can adjust to suit your family's needs. Access these settings from either Xbox.com or an Xbox One console though you can only change content and app settings from the console.

From Xbox.com

1. Change privacy and safety settings for you or a child.
2. Sign in to the adult's Microsoft account at Xbox.com. If you've forgotten your account email address or password, see the *Lost Account Solution* or the *Lost Password Solution*.
3. Under My Xbox, select *Profile*.
4. Select *Privacy Settings* or *Online safety* on Xbox One. Due to the secure nature of these settings, you may be asked to enter a security code that we'll send to the alternate phone number or email address previously saved to your account.
5. Select the account you want to look at.
6. Review the settings currently in place and update those you want to change.
7. Save your changes on each tab before moving on to the next.

From your Xbox One console

Change privacy and safety settings for you or a child:

1. Sign in to your Xbox. (If you're changing the settings for a child, sign in using an adult's account.)

2. Scroll left on the *Home* screen to open the guide. Select *Settings* > *All Settings*.

For your account:

1. Under *Privacy & online safety*, select *Xbox Live privacy*.

2. Choose a default, or customise your settings by selecting *View details & customise*.

For a child's account:

1. Under *Account*, select *Family*.

2. Enter your password or passkey, and then select the account you want to update.

3. Select *Privacy & online safety*, and then choose the default settings, or customise by selecting *View details & customise*.

When you download apps from Microsoft Store, each app requires permission to access data from your console.

1. On your Xbox One console, select *Settings* > *Privacy & online safety* > *App privacy*.

2. Choose from the list what you'd like to give permission for by selecting the check boxes.

If you're signed in with a child account, you'll need your parent to sign in and give permission for apps to access your data.

1. Sign in with an adult's account.

2. Go to *Settings* > *Family*.

3. Select the child account you'd like to manage, and go to *Privacy & online safety* > *App privacy* to give permission.

Please Note

If multiple gamers are signed in, apps can only access data everyone has given permission for. When you give apps permission on a console, it's only saved on that console. If you use multiple consoles, make sure you give your apps permission on all your consoles.

DID YOU KNOW?

In almost two-thirds (64%) of our workshops with 8-10 year olds, at least one child was playing adult rated games.

Cybersafety Ireland (2017 statistics)

For more information visit: privacy.microsoft.com

MANAGE APP PRIVACY SETTINGS

Xbox One safety features enable you to control what kinds of content each of your family members can access on Xbox One. To set content restrictions, see how *"Online safety and privacy settings for parents and children"* on page 33. For help changing these features, see Troubleshoot changing online safety or privacy settings on Xbox One.

Access to content

Once on your xbox one console you can set the content restrictions based on the content's recommended age, which Xbox One uses to control the child's access to specifically rated games, movies, TV shows, and music.

By default, if the child is under 8 years of age, Access to content is set to "Off."
To change the default setting for your child:

1. Press the Xbox button to open the guide.
2. Select *Settings*.
3. Select *All Settings*.
4. Under Account, select *Family*.
5. Select the child account you want to update.
6. Select *Access* to content.
7. The content limits are unrestricted for all users over the age of 8. You can select preset age-appropriate limits by choosing your child's age from the list. We'll show you what the presets are for that age. You're not restricted by date of birth you decide which maturity level is appropriate.

Web filtering

Web filtering allows parents to determine what kinds of websites their children can view in the Microsoft Edge app. These are the default settings by age group:

Young children: General interest

Child and teen accounts: Online communication.

To change the default setting for your child:

1. Press the Xbox button to open the guide.
2. Select *Settings*.
3. Select *All Settings*.
4. Under Account, select *Family*.
5. Select the account for the family member whose settings you want to change, and then select *Web filtering*. Choose the appropriate setting.

Note: Web filtering settings on the Xbox One console are not transferable to other Microsoft services such as Windows 10. Settings for your Windows PC can be managed through the Microsoft Safety & Security Center.

Purchase choices

Xbox One enables the parent to control what kinds of apps each child may download from Microsoft Store. The setting options are:

Blocked (none)

Free apps only

Free or paid apps

To change the default setting for your child:

1. Press the Xbox button to open the guide.
2. Select *Settings*.
3. Under Account, select *Family*, select the account for the family member whose settings you want to change, and then select *Access* to content.
4. Change the *Buy* and *Download* setting.

If you are interested in learning more about privacy settings and safety settings to best protect your child you can visit *support.xbox.com* for more information on how to access settings to best protect your child.

LOCATION SERVICE AND PRIVACY

Some apps and services need to know your specific location to work correctly to provide maps to help you on your way. The Xbox location service tells your apps and services where you are, so you can discover new places and get where you want to go.

How location settings work

To play on your PS4, you'll need to have a PlayStation Network account. The first time an app that uses the location service needs your device location, it requests your permission. If you give an app permission but change your mind later, follow the steps below to change what apps can access your location info.

Note: For exceptions to location settings, please read all app privacy policies to learn more about how those apps and services use your Xbox's location.

How to control location history and settings

To turn location service on or off:

1. On your Xbox, double-tap the Xbox button to open the guide, then select *Settings* > *All settings* > *Account* > *Privacy & online safety* > *App privacy* > *Location*.

2. Select or clear Location on to turn it on or off.

To change whether a specific app can have access to your location:

1. On your Xbox, open the guide, and select *Settings* > *All settings* > *Account* > *Privacy & online safety* > *App privacy* > *Location*.

2. Turn each app on or off where it appears under Choose which apps can use your location. If *Location* is turned off for your user account, you won't be able to turn on location settings for individual apps.

ONLINE ABUSE

We don't know how many children and young people are affected by online abuse. Children often:

- don't tell anyone because they feel ashamed or guilty
- may not know who to tell
- may not realise they are being abused.

DID YOU KNOW?

1 in 3 internet users are children.

•

1 in 4 children have experienced something upsetting on a social networking site.

•

Around 1 in 8 young people have been bullied on social media.

•

3 in 4 parents have looked for or received information or advice about how to help their child manage online risk.

•

There were over 2,200 counselling sessions with young people who talked in Childline about online sexual abuse online in 2017/18.

For more information and facts please visit: www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/facts-statistics/

PLAYSTATION 4
PLAYSTATION4, SLIM AND PRO MODELS

What is the Playstation Network (PSN)?

When you receive your PlayStation 4, you get far more than a gaming console. You also get access to the PlayStation Network,an entertainment service that offers movie streaming, music, TV programming, and of course, online gaming. If you're new to the PS4 and everything that goes with it, check out this handy overview of the PlayStation Network.

Account Creation

To play on your PS4, you'll need to have a PlayStation Network account. You can create an account in mere minutes by entering a few basic pieces of information, such as your name, date of birth, state, and language. You'll need to come up with a password as well. Make it a strong one, over 8 characters, with a couple of numbers and special characters thrown in to stall potential hackers. You can also sign in with your Facebook account if you don't want to go through the entire account creation process.

MORE INFORMATION ON THE PSN

User Profile Setup

Next, you set up your user profile, including your online ID or username, the name everyone will see when you're on your PlayStation Network account. Think about this username carefully, because once you choose it, you can't change it. Choose a profile picture or an avatar to go with your username. You can also customise your profile with information about yourself.

Automatic Updates

PSN allows automatic updates to your PS4 console. You can disable this in the settings if you do not want them.

Live Broadcasting and Social Media

With the growing increase in game streaming, the PS4 offers a selection of live streaming broadcasting stations. Streaming games live means that anyone can watch your child playing a game, and if they have a headset or camera, mean that they can both hear and see your child. Make sure to have the conversation with them about the dangers of strangers on the internet.

Other Benefits

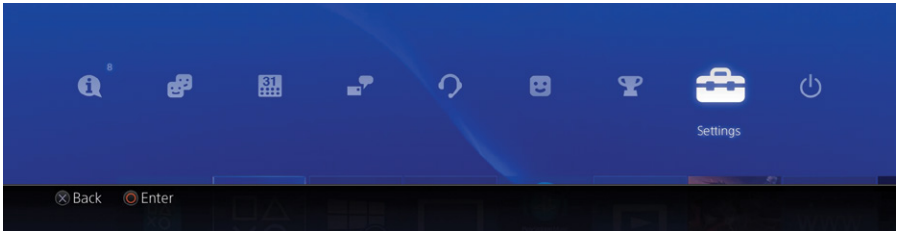
With your free PSN account, you get voice messaging, voice chat, limited online multiplayer gaming, and access to PlayStation Music, PlayStation Memories, PlayStation Now, PlayStation Video, and PlayStation Vue. If you have subscriptions to streaming services such as Hulu, Netflix, Spotify, or Amazon Instant Video, you can access all of that content through your PS4 as well, using the PlayStation Network.

Source: www.ps4home.com/a-beginners-guide-to-the-playstation-network/

The steps here can help you keep your parental control settings secure, and prevent children from attempting to override or change the settings without the family manager's permission.

1. To get started, power on your PlayStation 4, sign in with a user account, and access the home screen. You can press the "PlayStation" button in the center of the controller to access the home screen if you're on another screen.

Press the "Up" button on the controller to access the row of icons on the top of the screen, select the *Settings* icon on the right, and press the *X* button.

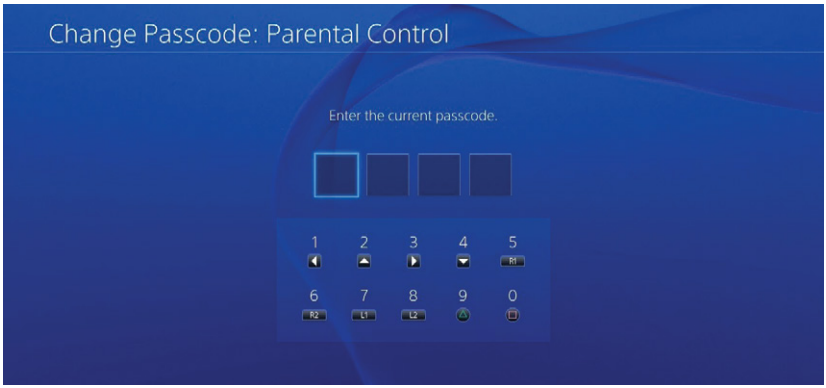


2. Select the *Parental Controls/Family Management* option in the list and press *X*.

PSN PARENTAL CONTROLS CONTINUED

3. Select *PS4 System Restrictions* here.

4. You'll be prompted to enter the parental controls passcode. If you haven't set a custom PIN yet, enter the default code, which is 0000. Press the "Square" button four times to enter 0000.



The System Restrictions give you a few options. By default, *New User and Guest Login* is allowed. You can disable this feature to ensure guests or new users can't sign in, which would prevent child users from bypassing any restrictions on their individual accounts.

For more information visit:
https://www.playstation.com/en-gb/get-help/help-library/my-account/parental-controls/

GENERAL PSN PRIVACY SETTINGS

Account holders can limit how visible they are to other users on PlayStation Network using Privacy Settings. You can customise the following features:

- Messages
- Friend requests
- Voice and video chat invitations
- Invitations to play online
- Trophies

How to change Privacy Settings on PSN

Please select your PlayStation system from the list below:

PS4 Privacy Settings

There are a few extra ways to communicate and share your information on PlayStation 4, so make sure you check all three options in the Privacy Settings menu.

1. Go to *Settings* > *Account Management* > *Privacy Settings* and enter your password.

2. Select the feature you would like to change Privacy Settings for.

3. Choose who you want to allow from the drop-down menu: *Friends*, *Friends of Friends* or *No One* and select *Confirm*.

NINTENDO SWITCH

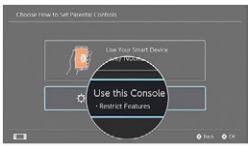
How to enable parental controls

1. Launch *System Settings* from the Home screen on your Nintendo Switch.

2. Scroll down and select *Parental Controls*.

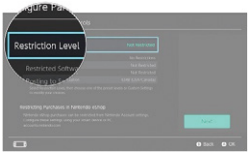
3. Select Parental *Controls Settings* on the right side of the screen.

4. Select *Use this console*.



5. Select *Restriction Level*.

6. Select *Teen*, *Pre-Teen*, or *Child* to create a pre-made setting.



DID YOU KNOW?

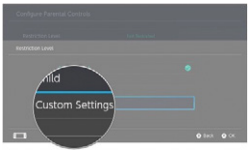
When we asked children the question about when they had last spoken to a parent or care-giver about online safety, we found that almost a third of children had rarely or never spoken to them.

Cybersafety Ireland (2017 statistics)

How to manually configure parental control settings

1. Follow the steps above and select *Custom Settings*.

2. Select *Restrict Software* to manually select the software rating restrictions. You can select from games rated ages for 3+ up to games rated for ages 18+.



3. Select *Software Rating Organisation* to change the region for your ratings regulations.

4. Select *Post to Social Media* to restrict or unrestricted the ability to post screenshots to your social media accounts.

   Note:
   Nintendo account users under 13 years old can't post to social media.

5. Select *Communicating* with others to restrict whether or not you can send and receive messages and chats, get user profile information, and view and share images. Some software will allow you to enable some communications restrictions individually.

When you are done manually configuring parental controls, hit *Next* to save your settings.

You will then be asked to enter a four to eight digit PIN, which you will use every time you access Parental Controls in the future.

HOW TO DELETE PARENTAL CONTROLS

If you decide that you don't want any restrictions on your Switch, you can delete the Parental Controls settings very easily.

1. Launch *System Settings* from the Home screen on your Nintendo Switch.
2. Scroll down and select *Parental Controls*.
3. Select *Parental Controls Settings* on the right side of the screen.
4. Enter your PIN.
5. Hit *Delete Settings* on the screen or the *X* button on your controller.

Nintendo Switch has parental controls: https://www.nintendo.com/switch/parental-controls/

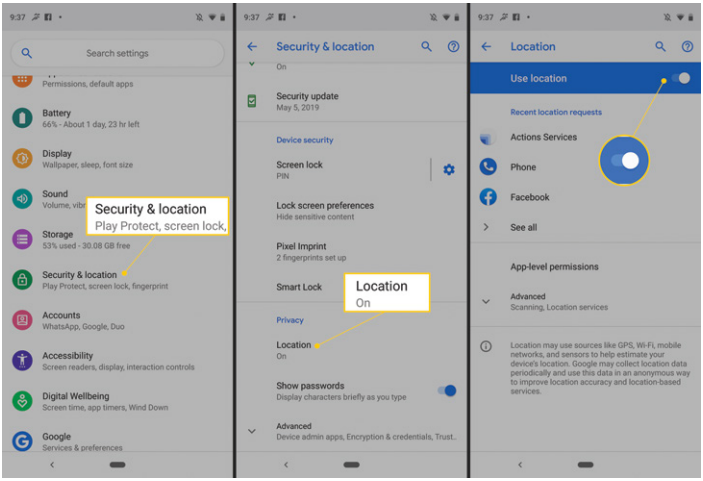
For more information on Parental Controls, see Nintendo's offical video on Parental Controls at: https://www.youtube.com/watch?v=03bAayBtcb0

LOCATION

LOCATION SETTINGS ON ANDROID

When you set up your Android device, you'll be asked if you want to share your location data. If you say yes, then google automatically adds your movements to your location history. The following steps will show you how to opt out of this option.

1. Open *Settings*.
2. Scroll down to *Security & Location*, then hit *Location*.
3. You'll see an on/off switch in the top right. Use this to turn location.
4. Services on or off altogether.
5. Tap on *Location* > *Google Location History*.
6. Once again there's a button in the top right that lets you turn your location history on or off.



LOCATION SETTINGS ON APPLE DEVICES

What is location tracking?

A lot of apps and iOS system services require location tracking in order to help customise the user's experience and provide the most helpful information possible. All of these apps and system services ask permission before they start to track an iPhone or iPad, but some apps won't function if you disable location tracking. You can tell if location services are active if a black or white arrow icon appears in the status bar at the top of the device.

Disable Location for iOS System Services

1. Click *Settings* > *Privacy* > *Location Services*.
2. Scroll to the bottom and select *System Services*.

We recommend not disabling location services on all system services on your iOS devices. While a lot of services can be utilized without tracking your location, it's best to go through the list individually.

DID YOU KNOW?

Only 65% of Irish parents are worried about their child revealing personal information online.

irishtimes article 2015

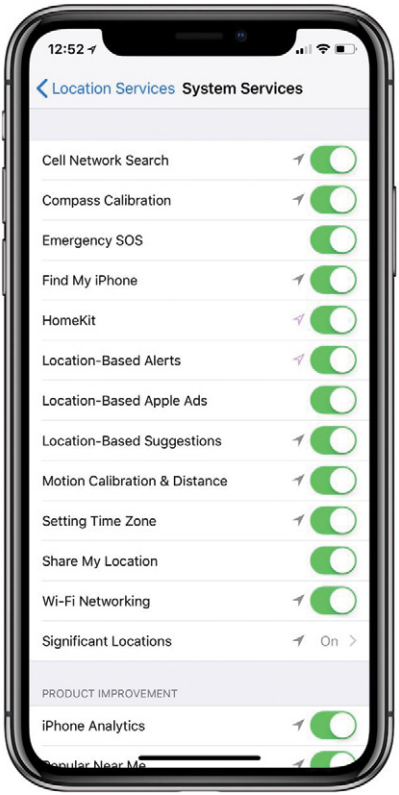
HERE'S HOW SYSTEM SERVICES USE LOCATION TRACKING:

1. Cell Network Search tracks cell tower usage and sends data to Apple.

2. Compass Calibration uses location tracking to help calibrate the electronic compass.

3. Emergency SOS is a newer feature that allows users to discreetly call 911 and uses location data to help assist in the event of an emergency.

4. Find My iPhone is a service provided by Apple that will enable you to track an iOS device remotely.



For more information on each system service illustrated to the right, please visit: https://uk.pcmag.com/howto/116364/how-to-turn-off-location-services-on-ios-devices

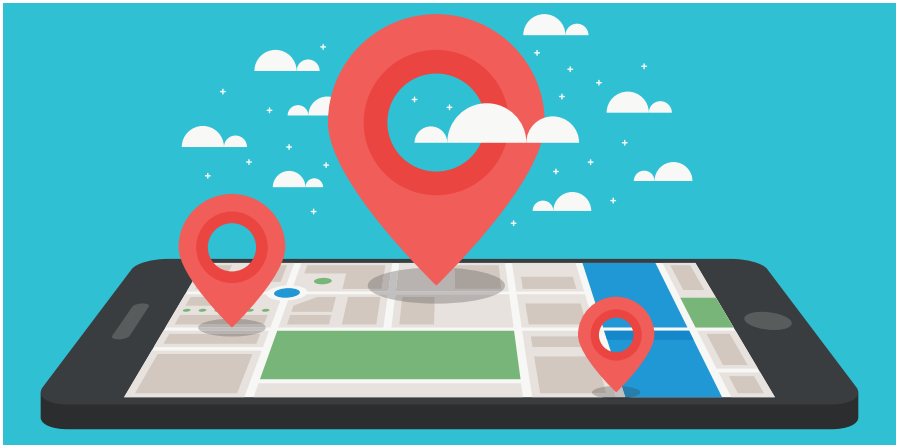
HOW TO DELETE YOUR LOCATION HISTORY ON ANDROID

You can restrict the use of built-in apps or features. If you turn off an app or feature, it won't delete it, it's just temporarily hidden from your Home screen. For example, if you turn off Mail, the Mail app won't appear on your Home Screen until you turn it back on. To change your Allowed Apps:

1. If you also want to delete your location history, you can do that here too: under *Location History* tap the three dots in the top right, then hit *View/Manage*.

2. Hit the three dots once more, then *Settings*.

3. You should now be in a section headed Personal content From here you can Delete all Location History or select Delete Location History range to delete just a part of it. Once deleted this information can't be recovered.



HOW TO DISABLE LOCATION FOR APPS

Click *Settings* > *Privacy* > *Location Services.*

It's good to look over this page often, mainly if you have downloaded apps recently, to make sure the location settings are set to what you're comfortable with. Luckily, Apple makes it very simple to adjust location permissions to individual apps on all iOS devices. There are typically three options for location services for apps:

1. *NEVER* – This option ensures that location services will never be tracked while using the app.

2. *WHILE USING* – The app only utilises location tracking while actively using the app. This includes if the app is not completely closed; completely close an app by double-clicking on the home button, finding the app that needs to be closed, and swiping it up and away (it's slightly different on iPhone X).

3. *ALWAYS* – The app can always track an iOS device's location.

Usually there's an app explanation when choosing what location access you want to allow. That explanation will help you decide if you should disable location services because it informs you how that specific app uses location tracking. It's a safe bet to set location tracking to the "*while using*" option to avoid background tracking without your knowledge.

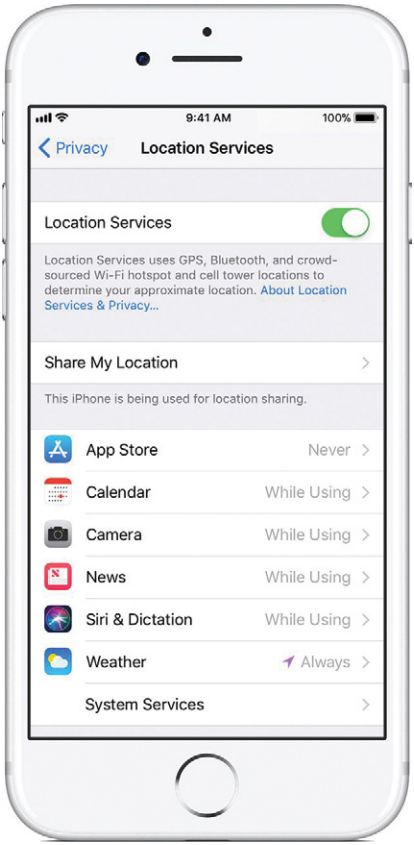
DISABLE LOCATION SERVICES COMPLETELY

Tap *Settings* > *Privacy* > *Location Services* and toggle the location services button at the top to the left or off position.

Be careful about doing this. That location services toggle is kind of the master switch to all location permissions. If an iOS user decides to turn off location services completely, a lot of the features that users use every day will no longer work.

For example, photos won't attach a location when you take them, mapping applications won't be able to direct you anywhere, and other third-party apps will be unusable.

Disabling location services may help you preserve your device's battery life and maintain the highest level of smart device privacy, but it will diminish your overall experience.



The purpose of the Children and Young People's Services Committees [CYPSCs] is to secure better developmental outcomes for children through more effective integration of existing services and interventions at local level. The work of all CYPSCs is underpinned by the national policy framework for children and young people 2014-2020, 'Better Outcomes, Brighter Futures' which sets out a vision for 'Ireland to be one of the best small countries in the world in which to grow up and raise a family, and where the rights of all children and young people are respected, protected and fulfilled; where their voices are heard and where they are supported to realise their maximum potential now and in the future'.

For more information on Co. Wicklow CYPSC please contact:

Fionnuala Curry, Co-ordinator
087 6043511
fionnuala.curry@tusla.ie or visit www.cypsc.ie
Tusla, Wicklow Primary Healthcare Centre,
Knockrobin, Rathnew, Co. Wicklow

CYPSC
CHILDREN & YOUNG PEOPLE'S SERVICES COMMITTEES
Wicklow

An Roinn Leanaí
agus Gnóthaí Óige
Department of Children
and Youth Affairs