THINK U KNOW .org.au

Fact sheet

PARENTAL CONTROL: Apple iOS 7 Guided Access Mode

Follow us: @ThinkUKnow_Aus facebook.com/ThinkUKnowAustralia

What is Guided Access mode?

Guided access mode is seperate to restriction settings and is targeted at parents who lend their device to small children to allow them to use a specific app, such as a game.
This mode locks the device into a specific app, disabling hardware buttons, and specified software buttons. This allows the child to use the specified app without fear of them exiting the app and accessing inappropriate material on the device, or inadvertently changing settings. The app can only be exited either by entering a passcode, or by performing a forced reboot on the device.

How do I enable Guided Access mode?

1. Settings > General > Accessibility > Guided Access
2. From the devices home screen, tap the Settings icon.
3. From the settings menu, tap the General tab.
4. Tap Accessibility from within the General tab.
5. Tap Guided Access.
6. Toggle the Guided Access button to the green position.
7. Tap Set Passcode, and enable a four digit guided access mode passcode.

How do I activate Guided Access mode on an app?

1. Open the app as usual, then once the app has loaded triple press the devices home button.
2. Following the instructions on the screen, select any areas of the app which you wish to disable the functionality for.
3. Tap the Start button to activate guided access mode.

How do I exit Guided Access mode on an app?

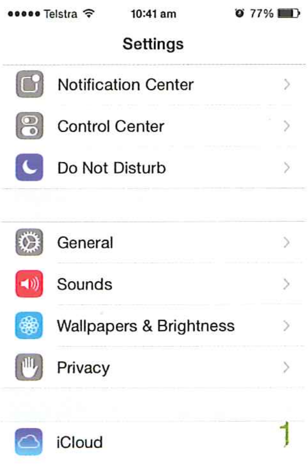
1. From within guided access mode, triple tap the home button.
2. Enter your guided access mode passcode.
3. In the guided access window that appears, select the End button.

Alternatively if you forget your passcode you can perform a forced reboot of the device by holding down the home and power buttons simultaneously for 15 seconds.

Where can I find more information about iOS parental controls?

Apple has a support page for Guided Access accessible at http://support.apple.com/kb/ht5509 , and for Restrictions accessible at https://support.apple.com/kb/ht4213.

How do I enable Guided Access mode?

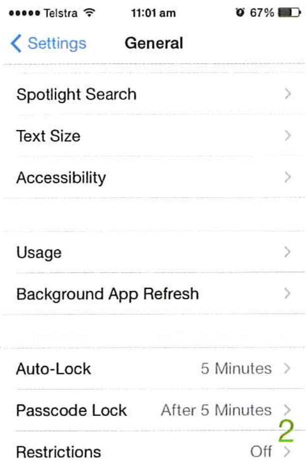


●●●●● Telstra 10:41 am 77%

Settings

- Notification Center
- Control Center
- Do Not Disturb
- General
- Sounds
- Wallpapers & Brightness
- Privacy
- iCloud

1

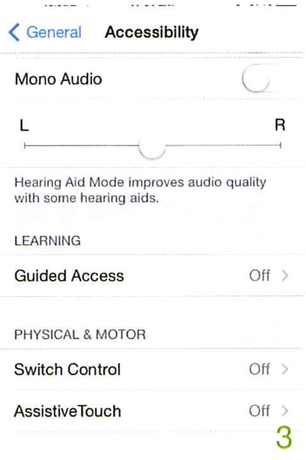


●●●●● Telstra 11:01 am 67%

< Settings General

- Spotlight Search
- Text Size
- Accessibility
- Usage
- Background App Refresh
- Auto-Lock: 5 Minutes
- Passcode Lock: After 5 Minutes
- Restrictions: Off

2



< General Accessibility

Mono Audio

L R

Hearing Aid Mode improves audio quality with some hearing aids.

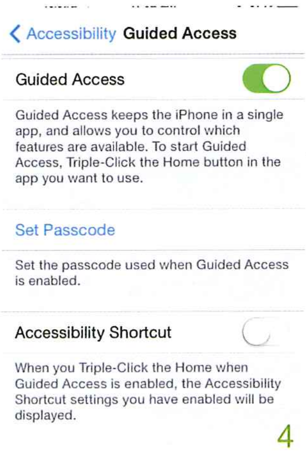
LEARNING

- Guided Access: Off

PHYSICAL & MOTOR

- Switch Control: Off
- AssistiveTouch: Off

3



< Accessibility Guided Access

Guided Access

Guided Access keeps the iPhone in a single app, and allows you to control which features are available. To start Guided Access, Triple-Click the Home button in the app you want to use.

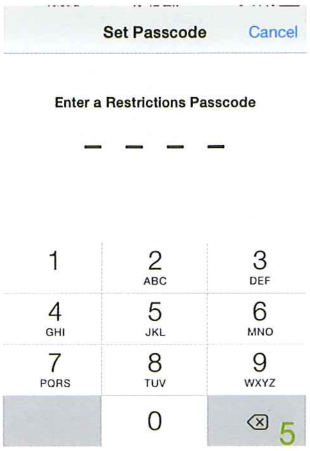
Set Passcode

Set the passcode used when Guided Access is enabled.

Accessibility Shortcut

When you Triple-Click the Home button when Guided Access is enabled, the Accessibility Shortcut settings you have enabled will be displayed.

4



Set Passcode Cancel

Enter a Restrictions Passcode

_ _ _ _

5

For more information visit www.thinkuknow.org.au

AFP3285

THINK U KNOW .org.au

Fact sheet

PARENTAL CONTROL: Apple iOS 7

Follow us: @ThinkUKnow_Aus facebook.com/ThinkUKnowAustralia

What devices are iOS parental controls available on?

Parental controls can be enabled on any device running Apple's iOS operating system. This includes iPhones, iPods, and iPads.

What controls do restrictions provide on iOS devices?

Restrictions allow you to control what content is accessible from an iOS device, prevent the removal of existing apps, and prevent the modification of existing settings. Restrictions are protected by a four digit passcode. If the passcode is not known then the only way to disable restrictions is by performing a factory restore on the device, erasing the data stored on the device. The restrictions feature is suited for devices that that are primarily used by a minor, for example a child's mobile phone. They are less suited towards shared devices, or parents devices that are only used by children occasionally. For these devices use Guided Access mode - see next page for details.

What restrictions can I place on my child's device?

Apple's iOS software allows parents great flexibility in scripting access on their child's device including restricting app downloads, limiting access to particular websites and restricting the use of some built-in apps.

To ensure that restrictions are set for the correct content make sure 'Ratings for' is set to 'Australia' (See Image B).

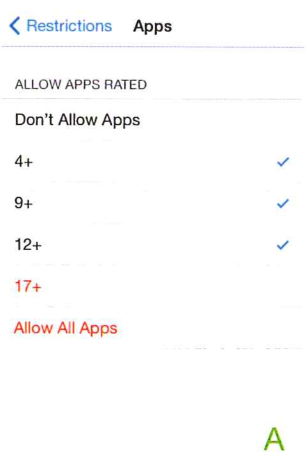
Restricting access can be extremely helpful to ensure your child is not exposed to inappropriate content, however keeping open lines of communication with your children around responsible internet usage is essential.

How do I setup parental controls on an iOS device?

1. Settings > General > Restrictions > Enable Restrictions
2. From the devices home screen, tap the Settings icon.
3. From the settings menu, tap the General tab.
4. Tap Restrictions from within the General tab.
5. Tap Enable Restrictions.

You will then be able to enable individual restrictions by toggling pre-installed app access, and by tapping various categories, and choosing the desired restriction level for that category.

iOS 7 Parental control features



‹ Restrictions Apps

ALLOW APPS RATED

Don't Allow Apps

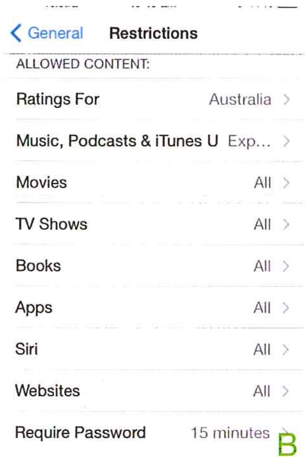
4+ ✓

9+ ✓

12+ ✓

17+

Allow All Apps

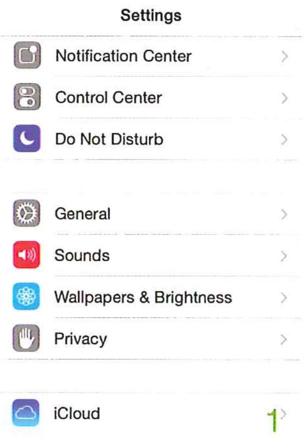


‹ General Restrictions

ALLOWED CONTENT:

Ratings For	Australia ›
Music, Podcasts & iTunes U	Exp... ›
Movies	All ›
TV Shows	All ›
Books	All ›
Apps	All ›
Siri	All ›
Websites	All ›
Require Password	15 minutes ›

How do I setup parental controls on an iOS device?



Settings

Notification Center ›

Control Center ›

Do Not Disturb ›

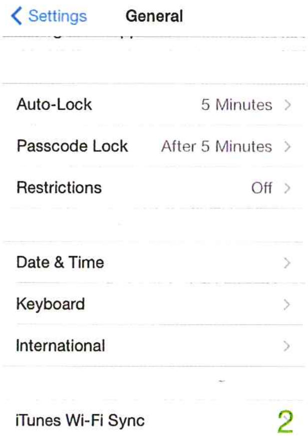
General ›

Sounds ›

Wallpapers & Brightness ›

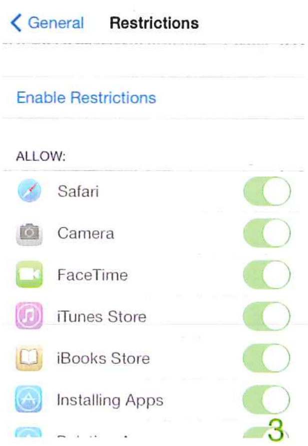
Privacy ›

iCloud ›



‹ Settings General

Auto-Lock	5 Minutes ›
Passcode Lock	After 5 Minutes ›
Restrictions	Off ›
Date & Time	›
Keyboard	›
International	›
iTunes Wi-Fi Sync	



‹ General Restrictions

Enable Restrictions

ALLOW:

Safari

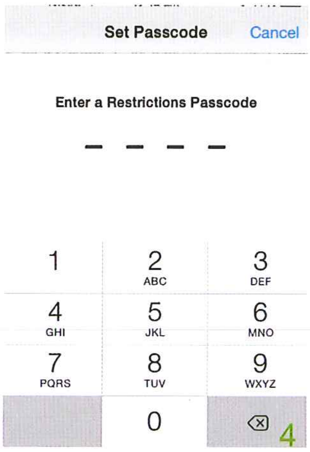
Camera

FaceTime

iTunes Store

iBooks Store

Installing Apps



Set Passcode Cancel

Enter a Restrictions Passcode

_ _ _ _

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
	0	⌫

Note: When restrictions are enabled for apps, and then subsequently disabled your apps may be placed directly onto your home screen and not into folders which you previously had them within.

THINK U KNOW .org.au

Fact sheet

MANAGING YOUR REPUTATION

Follow us: @ThinkUKnow_Aus facebook.com/ThinkUKnowAustralia

When you send something digitally, either via your mobile phone or over the internet, you lose control over who sees it and what they do with it. You may never be able to permanently delete the image or text. Before you send something, think about where it might end up.

Do you know who you are sending it to?

You might be tricked into thinking you are communicating with a friend, but can you ever be sure that it is only them holding the phone or looking at the screen?

Do you know what they will do with it?

Even if you are sure who is on the other end, can you really trust them? If your relationship turns sour, can you be sure that they won't use that text or image against you?

Do you want it to be around forever?

Once you have shared something in a digital format, it can easily be distributed to others and posted on the internet. Distribution might start with just your school, but it can quickly spread to your community and beyond. Once you put something on the internet, it can never be permanently deleted. Think about these things before you ever share something digitally.

How will it affect your future?

A future employer, university or sporting organisation might research you online and decide not to give you a position if they find inappropriate images or posts of you.

Sexualised images of you could even end up in the collection of an online sex offender. This might result in law enforcement attempting to identify the victim in this image and this could cause you and your family unnecessary stress and humiliation.

What should you do before it happens to you?

Think twice before communicating or agreeing to share this type of material with someone, especially using technology to do so.

Have you been part of the problem?

By storing or helping to distribute this type of material, you are contributing to this serious issue. Distributing these images maliciously is viewed even more seriously.

What should you do if it has already occurred?

If you have received this type of material, delete it without forwarding it. Tell the person who sent it to you that you are not interested in being a part of this. If you know who the person in the image or communication is, let them know what is going on. They wouldn't want to be the last to know.

If you have created this material, delete it and don't share it. If you have sent it to someone, ask them to delete it and make sure they do.

If someone has created this material of you without your permission, you need to tell a trusted adult and they can assist you in reporting it to law enforcement. This is a serious matter and should not be ignored.

So what does the law say?

Any images, text or representations of someone under the age of 18 in a sexual pose or engaged in a sexual act is considered child pornography.

Young people in Australia and overseas have been charged under child pornography laws for engaging in this type of behaviour.

You can NEVER consent to making child pornography.

For more information visit:
www.thinkuknow.org.au

thinkuknow.org.au

AFP AUSTRALIAN FEDERAL POLICE Microsoft DATACOM CommonwealthBank