Marino College
Second Level

# Internet safety Guide for Parents/ Guardians

# TABLE OF CONTENTS

# INTERNET SAFETY TIPS

## No.1

### Discover the internet together

Be the one to introduce your child to the internet. For both parent and child it is an advantage to discover the internet together. Try to find websites that are exciting and fun so that together you achieve a positive attitude to internet exploration. This could make it easier to share both positive and negative experiences in the future.

## No.2

### Agree with your child rules for internet use in your home

Try to reach an agreement with your child on the guidelines which apply to internet use in your home. Here are some tips to get started:

→ Discuss when and for how long it is

acceptable for your child to use the internet

→ Agree how to treat personal information (name, address, telephone, email)

→ Discuss how to behave towards others

→ Agree what type of sites and activities are OK or not OK

→ Follow the rules yourself! Or at least explain why the rules are different for adults.

## No.3

### Encourage your child to be careful when disclosing personal information

A simple rule for younger children should be that the child should not give out their name, phone number or photo without your approval. Older children using social networking sites like Facebook should be encouraged to be selective about what personal information

and photos they post to online spaces. Regardless of privacy settings, once material is online you can no longer control who sees it or how it is used.

## No.4

### Talk about the risks associated with meeting online 'friends' in person

Adults should understand that the internet can be a positive meeting place for children, where they can get to know other young people and make new friends. However,

for safety and to avoid unpleasant experiences, it is important that children do not meet strangers they have met online without being accompanied by an adult you trust. In any case, the child should always have their parents' approval first. In addition, it is also a good idea to have a fail-safe plan in place such as calling them shortly after the meeting begins so that they can bail out if they feel uncomfortable.

## No.5

### Teach your child about evaluating information and being critically aware of information they find online.

Most children use the internet to improve and develop their knowledge in relation to schoolwork and personal interests. Children should be aware that not all information found online is correct, accurate or relevant. Show your child how to check information they find by comparing it to alternative sources on the same topic. Show them trusted sites they can use to compare information.

# HOW WE MONITOR YOUR CHILDS IPAD IN SCHOOL

In Marino College we use Mobile Device Management (MDM) to effectively manage and monitor student devices.

***Jamf School*** is a purpose-built mobile device management solution (MDM) for schools. Jamf has a web-based interface — deploying apps, managing and securing student devices.
Jamf keeps track of managed devices, users and apps. It allows the administrator to view the status of devices quickly and easily, and identify issues for remediation.

Jamf School Student gives students restricted permissions over their own devices, allowing them to focus on their education without being distracted by unauthorised apps.

With the Jamf School Student app, students can manage their own iPad devices. They can install apps approved by the school and use documents stored in their personal iCloud drive.

# HOW TO MONITOR YOUR CHILDS IPAD AT HOME

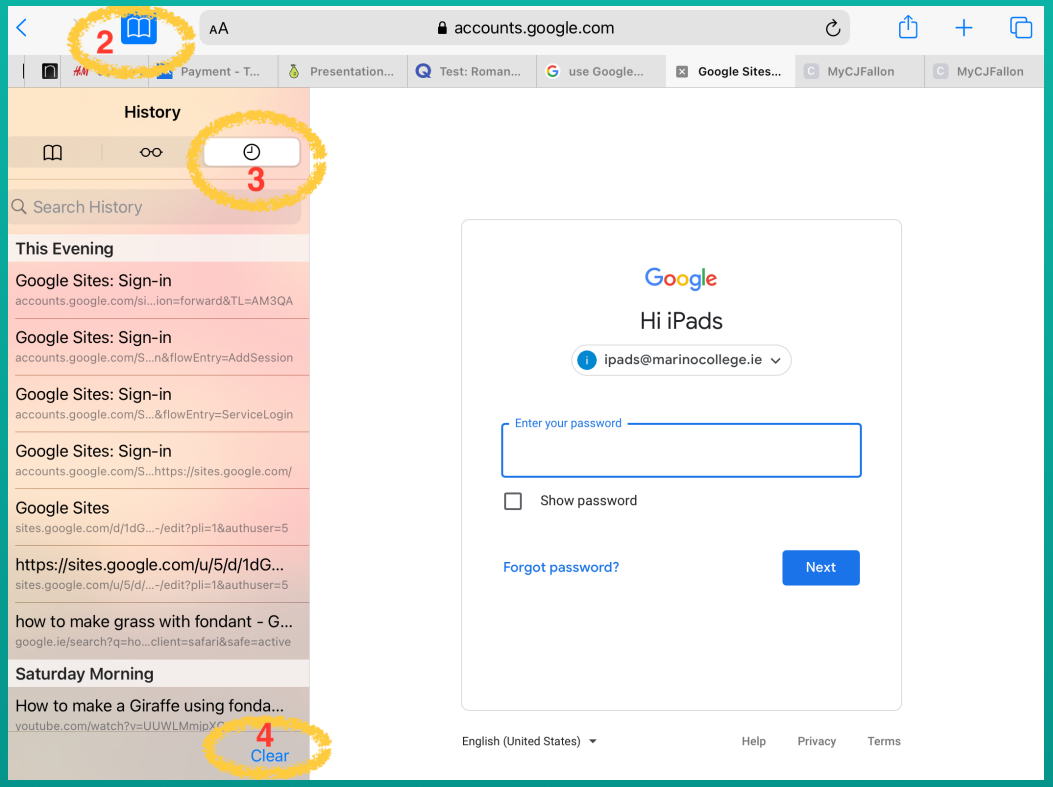
MDM installed by the school does not allow your son/daughter to download any apps all educational apps are installed prior to students receiving their device. When students are using the school wifi certain websites are restricted for their protection. It is very important to monitor what your son/daughter searches and accesses while using internet/wifi outside of school.

You can manually view internet history of their iPads and keep a strict check on the kinds of websites they visit.

**Step1**

Open Safari on your Childs iPad

**Step 2** Click on the book icon




**Step 3:**

Click on the clock symbol- this will provide you with the days and dates sites were accessed.

Safari's browsing history should now be displayed on your iPad screen. Notice in the example that sites visited earlier today, such as About Computing & Technology, are displayed individually. Sites that were visited on previous days are separated into sub-menus. To view a particular day's browsing history, simply select the appropriate date from the menu.When a specific entry in the iPad's browsing history is selected, the Safari browser immediately takes you to that particular Web page.

**Step 4:**

Click the clear button on the bottom of this drop down menu to clear the internet search history

# HOW TO PUT RESTRICTIONS ON YOUR CHILDS IPAD

iPads have a function to enable the school and/or parents to place individual restrictions on their son/daughters device. This can be done by utilising Screen time. Screen Time enables you as a parent/guardian to set restrictions on content and time limits on general use and specific apps.

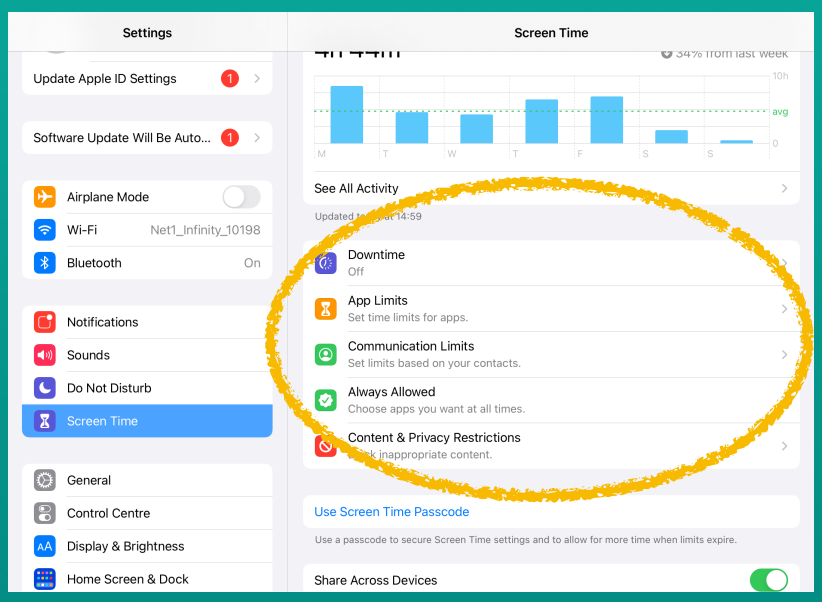
Here's why you might want to enable screen time:

- Lets you block websites/chatrooms and enforce screen time limits for apps.
- Lets you control your son/daughters contacts.
- Gives you an idea of how your son/daughters is using the iPad on open wifi.
- Stops them from making changes to the settings.

## HOW TO SET UP SCREEN TIME :

1. Tap settings
2. Tap Screen Time.
3. Tap "This is My Child's iPad."
4. Follow the prompts and then create a pass code.
   - This code is different from the one you use to unlock your iPad. Instead, it's a code you set so your son/daughter can't change the settings. You will be asked to enter an apple id to help you to reset your screen time passcode. You do not have to enter an apple id however, if you don not and forgets your passcode there is no way to reset it.If you choose this option please write down the passcode and keep it in a safe place. Remember don't share it with your son/daughter.

Inside screen time you can now manage your son/daughters **down time, app limits, communication limits, apps that are always allowed and content and privacy restrictions**



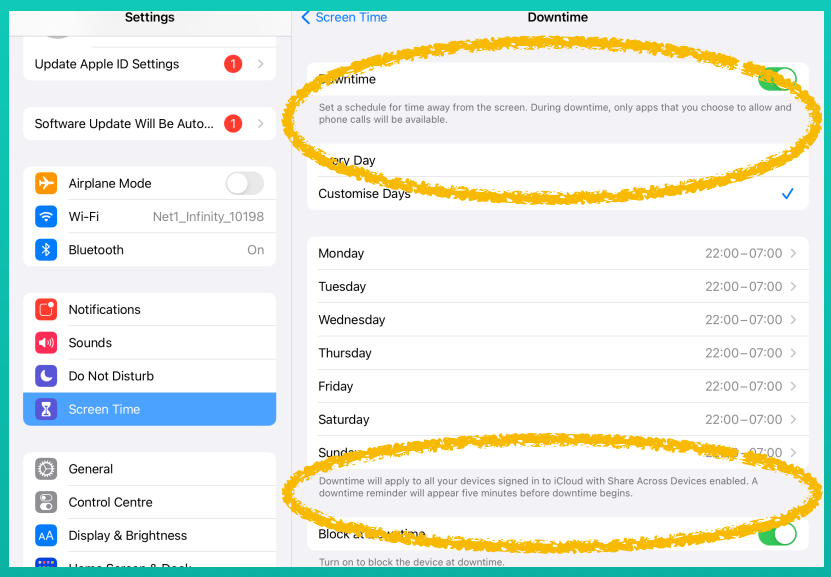
## Downtime

**How do I limit the times of day my son/daughter can use his/her iPad,  for example at bedtime?**

Set up Downtime. Down time enables you as a parent to stop device use during a set block of time.Downtime is best used for a regular span of time, but you can adjust that chunk of time on various days. It's probably most easily applied to bedtime.

### HOW TO SET UP DOWN TIME :

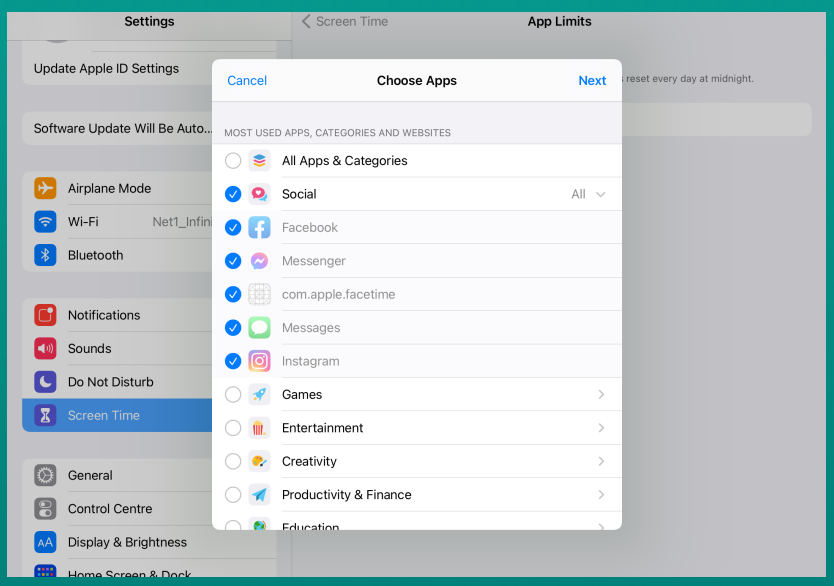
1. Tap Downtime.
2. Set a start and end time. Your son/ daughter will get a reminder five minute before Downtime starts.
3. Toggle on Block at Downtime.

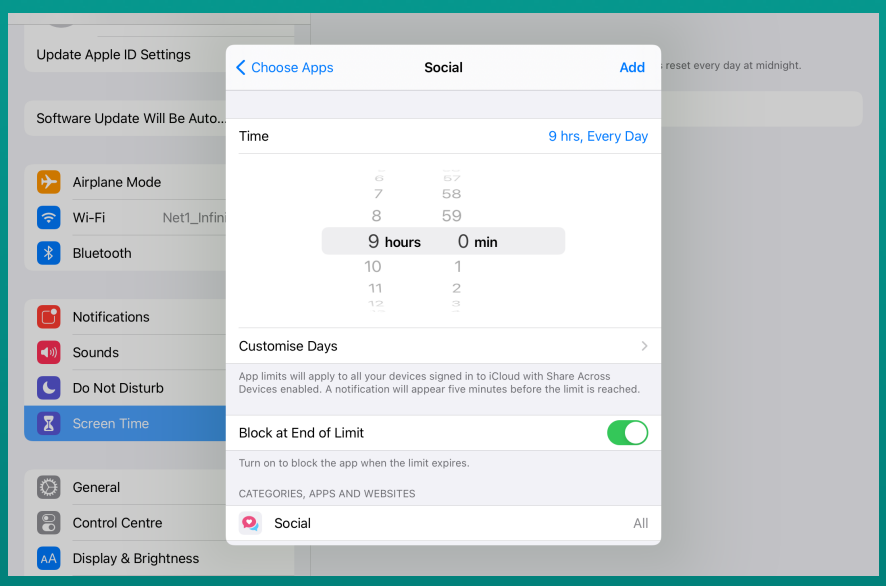



## App Limits

You can set daily limits for app categories with App Limits.

How to set up App Limits
1.Tap app Limits
2.Tap add limit
3.Select what apps you want to put a time limit on
4. Input the amount of time and the days you want an app limit to be in place and tap Add.
5. To change or delete an app limit simply tap on the limit.



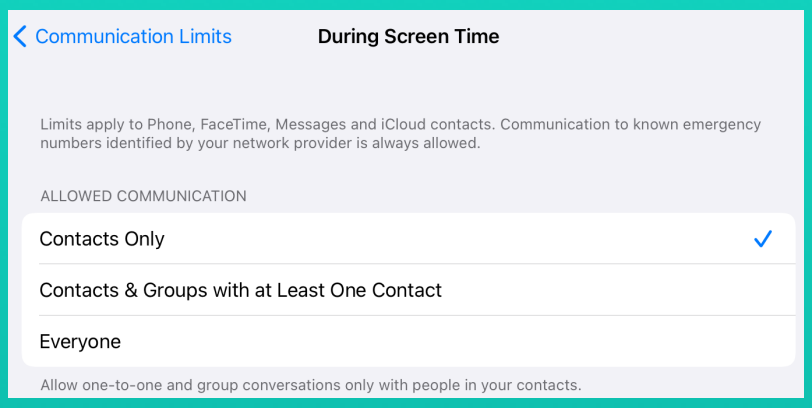



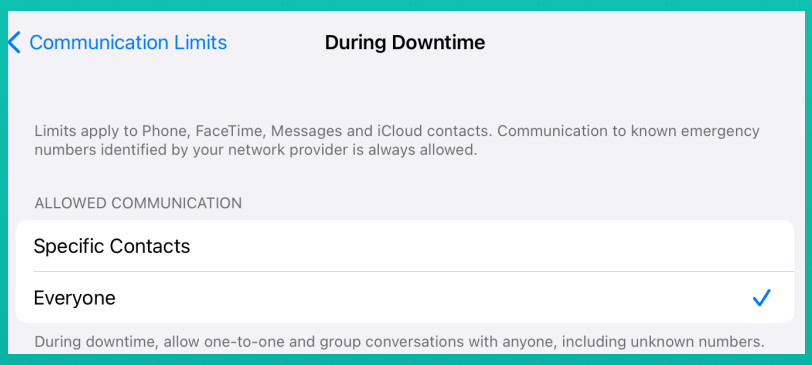
## Communication Limits

Control who your son/daughter can communicate with — throughout the day and during downtime. These limits apply to Phone, FaceTime, Messages, and iCloud contacts.

How to set up App Limits

1. Tap Communication Limits
2. Select ‘During Screen time’ or ‘ During Downtime’ this will allow you to restrict and specify contacts



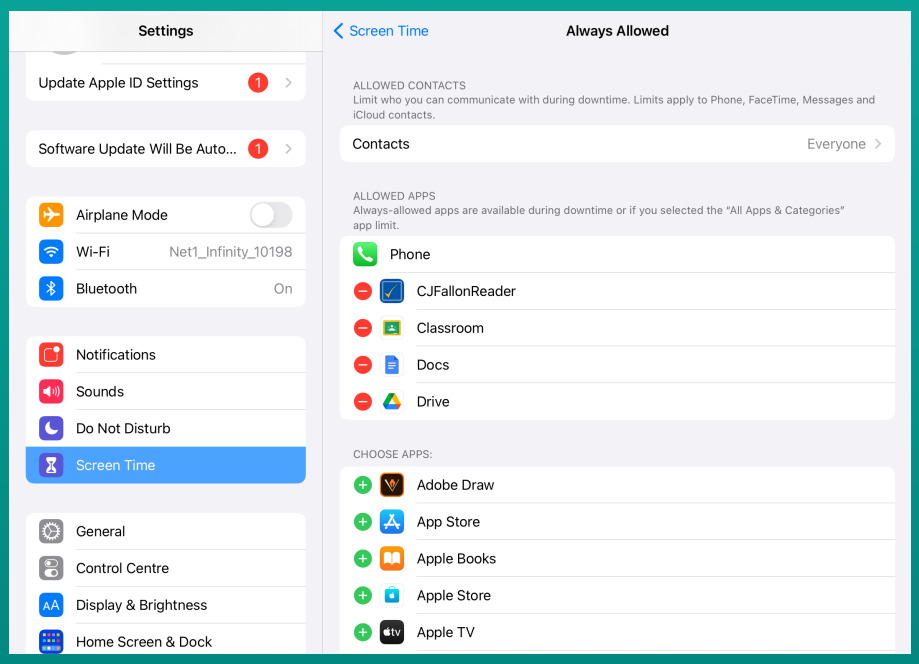




## Always Allowed

You might want to access certain apps, even if it's downtime or if you set the All Apps & Categories app limit. Phone, Messages, FaceTime, and Maps are always allowed by default, but you can remove them if you want

How to set up ‘Always allowed’

1. Tap ‘Always Allowed’
2. Select apps to be ‘ Always allowed’ by tapping the green icon and remove apps from the selection by clicking the red icon.

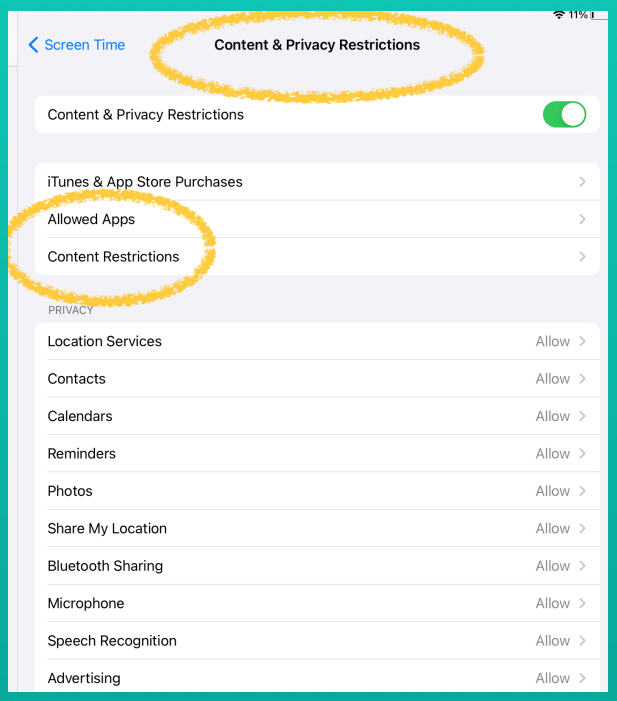


## How do I limit access to certain types of apps, like games, or specific apps, like Instagram?

The MDM installed and monitored by the school does not allow students to download social media or gaming apps. *The only way your son/daughter can access social media or gaming apps is via Safari using an unrestricted wifi connection.*

### Content & Privacy Restrictions

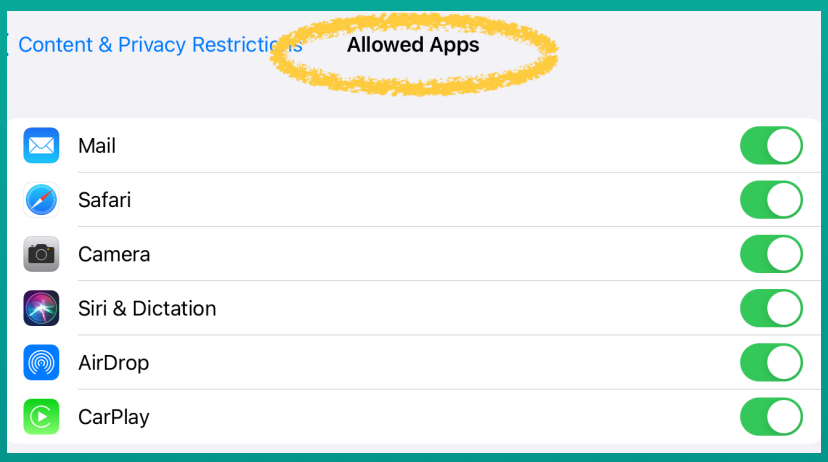
You decide the type of content that appears on your device. Block inappropriate content, purchases, and downloads, and set your privacy settings with Content & Privacy settings.




There are many restrictions that can be utilised in this section in particular ‘Allowed Apps’ and ‘Content Restrictions’.

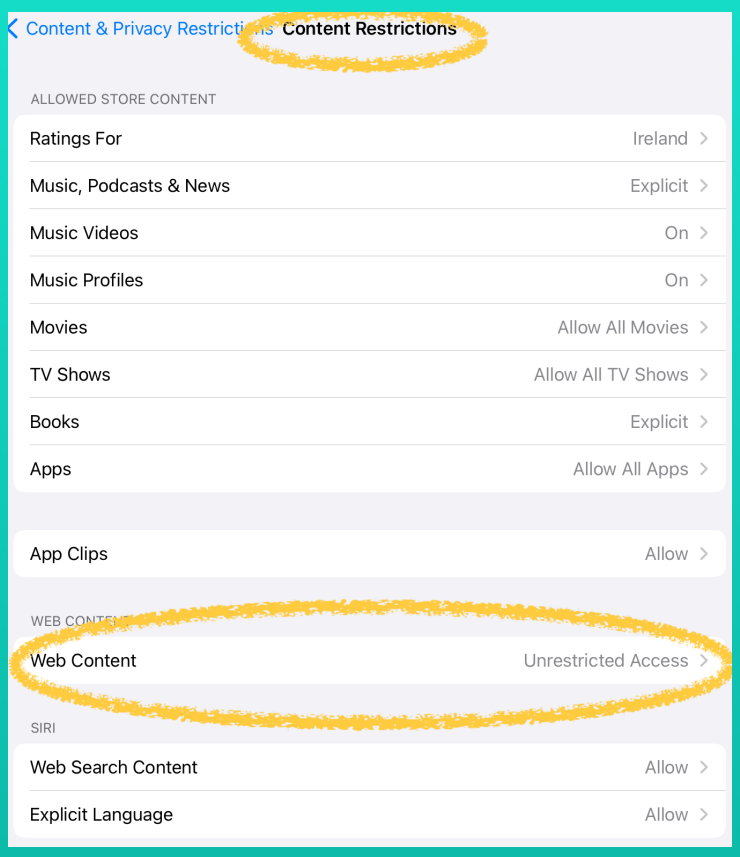
### ALLOWED APPS

These are built in apps. In turning off any of these the application automatically stops working until a time when the restriction is lifted.



## CONTENT RESTRICTIONS

In this section you can prevent any changes to the iPad, censor web content, prevent the playback of music with explicit content and movies or TV shows with specific ratings. Apps also have age ratings that can be changed using content restrictions.

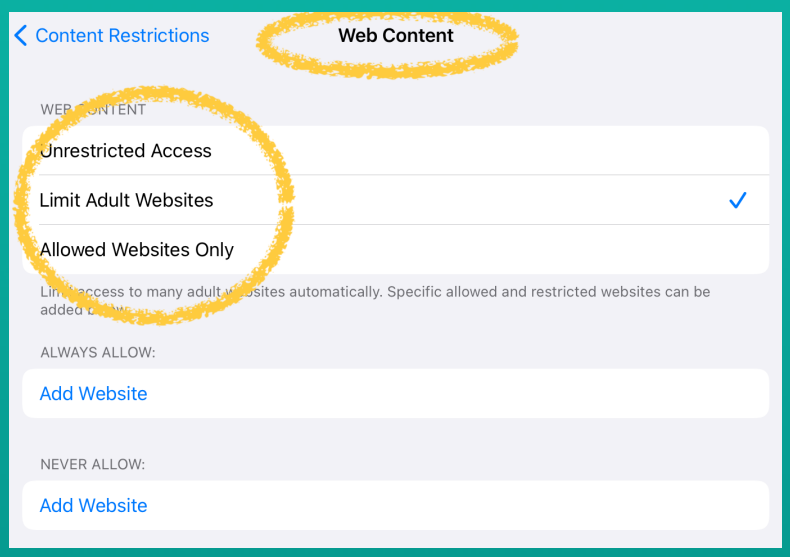



## RESTRICTING WEB CONTENT

iOS can automatically filter website content and limit access to adult content on the Internet and apps on your device. You can also add specific websites to an approved or blocked list, or you can limit access to only approved websites.

How to restrict web content:

1. Go to Settings > Screen Time.
2. Tap Content & Privacy Restrictions
3. Tap Content Restrictions, then tap WebContent.
4. Choose Unrestricted Access, Limit Adult Websites, or Allowed Websites Only.



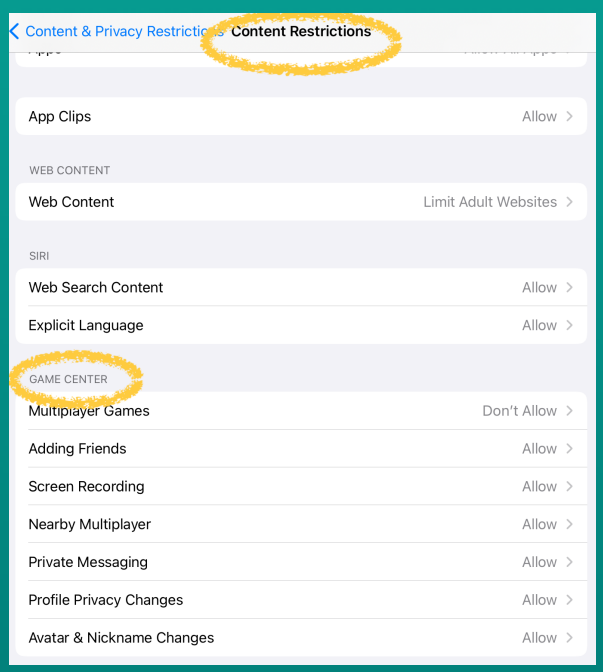

*Depending on the access you allow, you might need to add information, like the website that you want to restrict.

## RESTRICT GAME CENTRE

This allows you to restrict who your son/daughter interacts with when playing online games.

**To restrict Game Center features:**

1. Go to Settings and tap Screen Time.
2. Tap Content & Privacy Restrictions, then tap Content Restrictions.
3. Scroll down to Game Centre, then choose your settings.



# CHILDREN & SOCIAL MEDIA

### What is the right age to start?

Deciding at what age to allow your son/daughter to start using social media is often a dilemma for parents.

Age restrictions vary across social media platforms; in Ireland the Digital Age of Consent is now set at 16 years old.  It is very easy to sign up to social media platform with a false date of birth so it is important to monitor your son/daughters online activity.

## WHAT ARE IMPORTANT THINGS TO THINK ABOUT?

We know that some parents give permission to their underage sons/daughters to set up accounts on social networking sites . As a parent/guardian you need to decide id your son/ daughter is equipped to manage social pressures that can arise from social networking. The pressure to 'fit in' and/or 'be popular' can be intense. Romance, group chats and bullying can create tricky situations that even parents/guardians might find difficult.

## SOCIAL NETWORKING TIPS

### No.1

Ask your son/ daughter about what social networking services they use. Ask if you can see their profile. Don't be surprised if your child is reluctant to show you – children can see social networking as a parent- free zone where they communicate with friends.

### No.2

Sometimes a teenager won't tell a parent about a bad experience they have had online because they fear that you might deal with the problem by keeping them off their favourite social networking services. However, if they feel they can talk about their online habits with you, without judgement, or the threat of being disconnected, it will lead to more honesty in the long run.

### No.3

Ask your son/ daughter what privacy settings they have set up on their profiles. Encourage them if they are 'public', to amend the setting to 'private' so that only friends can see what they post

### No.4

It's a good idea too to talk about your child's friends list. 'Friends' is the catch all term for any contacts on social networking sites. Sometimes, in their desire for popularity, teenagers become too relaxed about who they'll accept as 'friends'. Teenagers should review their list of online 'friends' regularly, so they are sharing their information only with people they trust.

### No.5

Be sure to put emphasis on the fact that they should NOT reply to any unwanted or unsolicited messages. Scam artists or predators use messages to draw responses from young people and then target them.

### No.5

Ask your child about what they think is okay to post/share online. It's a good idea to give some guidelines about what to avoid discussing or sharing online. Some children may not understand how quickly content can be shared online, it may be helpful to explain that even by deleting a post or photo it may still be too late, and the content may have already been shared.

# CYBERBULLYING

## WHAT IS CYBERBULLYING ?

Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted.
Examples include:

- spreading lies about or posting embarrassing photos of someone on social media
- sending hurtful messages or threats via messaging platforms
- impersonating someone and sending mean messages to others on their behalf.

### The most common places where cyberbullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Online forums, chat rooms, and message boards, such as Reddit
- Online gaming communities

Face-to-face bullying and cyberbullying can often happen alongside each other. However, cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.

**Be clear on what constitutes online bullying. The procedures recently published by the Department of Education and Skills say "placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour"**

## WHAT IF MY CHILD IS BEING BULLIED ONLINE?

### STEP 1

Praise your child for coming to speak to you about the problem. Sometimes that first step of asking for help is a difficult one. Try to stay calm and not overreact. The first thing to do is to listen. Listen supportively, try not to interrogate your child. If they come to you looking for help, they have demonstrated trust in you.

### STEP 2

Be careful not to damage that by losing your cool or taking action that they are uncomfortable with. At the same time you should make it clear that in order to help them you may have to talk with their teachers and the parents of other children involved.

### STEP 3

Once you have established that bullying is taking place, you should get in touch with your child's school or youth organisation. If the cyberbullying is very serious, or potentially criminal, you could contact your local Gardaí.

### STEP 4

Schools have a particular responsibility to address bullying. Talk with your child's teacher if the bullying is school related. A pupil or parent may bring a bullying concern to any teacher in the school. The school will take appropriate measures regarding reports of bullying behaviour in accordance with the school's anti-bullying policy. All schools have an 'Anti-Bullying' policy. You should familiarise yourself with Marino Colleges policy, so you know the steps to be taken if required.

## WHAT ADVICE SHOULD I GIVE MY CHILD?

### Don't Reply:

Young people should never reply to messages that harass or annoy them. The bully wants to know they have upset their target. If they get a response it feeds into the problem and makes things worse.

### Keep the Messages:

By keeping nasty messages your child will be able to produce a record of the bullying, the dates and the times. This will be useful for any subsequent school or Garda investigation.

### Block the Sender:

No one needs to put up with someone harassing them. Whether it's messaging apps, social networking or playing games, children can use the technology block anyone who is bothering them.

### Report Problems:

Ensure your child reports any instances of cyberbullying to websites, apps, or other service providers using their reporting tools. By using these, your child will be passing important information to people who can help.

## THINK BEFORE POSTING

Once we post something, it can be difficult to control where it goes. The best advice parents/guardians can offer their son/daughter is to **THINK** before they post. Encourage your son/daughter to: Ask themselves...

*Is it **T**rue?*

*Is it **H**elpful?*

*Is it **I**llegal?*

*Is it **N**ecessary?*

*Is it **K**ind?*

# ONLINE CHILD PORNOGRAPHY

While the internet undoubtedly presents fantastic opportunities for children, it is equally clear that there is a real opportunity for children to be put at risk by their exposure to material and/or individuals which may be harmful. With the rapid evolution of internet technology, through internet on mobile phones and camera phones, parents need to understand that access to the internet is becoming increasingly diverse and therefore increasingly difficult to supervise.

## It's important to make your child aware of the risks of sharing online and how to protect them from these risks.

## Here are a few important talking points for parents:

- Help your child to understand the consequences they could face for sending or forwarding nudes. Make sure they understand that taking, possessing or sending sexting images can be a criminal offence. It can also result in sanctions at school.
- Talk to your child about what to do if they are asked to send images of themselves.
- Remind your child that once an image is sent, they have no control over what happens the image.
- Discuss the importance of being respectful to others online and how harmful sharing intimate images of others can be. Explain that it is a violation of trust and can result in serious harm to the person in the picture.
- Peer pressure can play a big part in why teens act and behave in certain ways. You can rehearse different scenarios with them to help them be comfortable with saying no.

# What to do if Intimate Images of your Child are Shared Online?

Firstly, reassure and support your child, this can be a very distressing time for them. It's also important to try and get all the facts before taking action. If images have been shared online without their permission there are a number of steps to consider taking:

## STEP 1

Do you or your child know who has shared the image?
If so contact them and ask them to remove and delete the image(s). You should also check if they have shared the image(s) with anyone else or on any other sites/services.

## STEP 2

Sharing sexting images or videos of children under the age of 18, could be considered as child pornography and may be illegal. If your child is under 18 and a nude image has been shared online, it is a potentially criminal activity and should be reported to the Gardaí.

If possible, keep any evidence of where the image has been shared and who has shared it.

## STEP 3

Regardless of age, most social networks also have a policy against revenge porn and will remove intimate images if they have been shared without permission. Reporting can normally be done within the network/app settings although it varies across social networks and apps.

## STEP 4

You might also consider contacting a legal professional if you are having difficulty removing images or contacting the website host.

## STEP 5

Not sure where the image may have ended up? Enter your child's name into a search engine, this may help find where the image has been shared.

This can be a stressful, upsetting time; it may be helpful for your child to talk to a professional or school guidance counsellor about what has happened.

# WHERE TO FIND HELP

# INTERNET SAFETY

## HOTLINE.IE

The hotline.ie service provides an anonymous facility for the public to report suspected illegal content encountered on the internet.

Get in touch: hotline.ie — 1890

## Webwise.IE

Department of Education and Skills and the European Union's Connecting Europe Facility.

Get in touch: webwise.ie

## Be Safe Online

A single online access point has been established as part of the gov.ie portal which provides pathways to information on online safety.

Get in touch: gov.ie/en/campaigns/be-safe-online