ONLINE SAFETY

MALIN BRIDGE PRIMARY SCHOOL

ONLINE SAFETY

INTRODUCTION

Whilst the use of computers and phones to access online material can be incredibly useful and enhance a child's education, it can also cause serious damage to mental health and relationships. The issues outlined in this document also affect adults.

Monitoring how your child accesses online material can be frustrating; it takes knowledge, time and persistence.

This document provides guidance on online safety relating to how children access some of the most well-known social media platforms and browsers for searching content on the Internet.

Although it is vital to stay up to date with the latest developments and to understand the contents of this document, the most effective way of ensuring your child's safety is still to talk to them openly and honestly about their lives online, without judgement. This will allow you to help them on their journey to becoming a safe user of the internet. Just like all social interaction, children will learn from their mistakes. It is important that they are able to make those mistakes in a supportive environment, with trusted adults to help them if things every go wrong.

THE CORE MESSAGES

Understand what your child has access to when using devices and understand what they may be able to access. Put filters in place if you deem exposure to be of concern or consider restricting use completely.

Remember that even with social media accounts set to private, the main feed is likely to be visible which means that your child can see what the public uploads.

Be mindful that time restrictions can also be placed onto a device, restricting when and how long your child uses the device.

Device management is often very extensive and if you wish to do something specific the likelihood is that you can achieve it. Strive to search out methods that suit your needs (Google and YouTube are excellent resources for this).

Establishing trust and being able to talk to your child about the Internet and social platforms (and for them to be able to talk to you) is possibly the most effective approach anybody could take.

Because technology is constantly being updated, the specific references in this document may be outdated. You are advised to check the functionality of the software you are using at the time to determine if it can achieve what you need it to.

THE INTERNET AND CHILDREN

The Internet is a place of opportunity, inclusion and diversity, the benefits of which outweigh the drawbacks.

Some of the risks are outlined in this document, some severe, but unlikely; others are mildly damaging and frequent.

It is the behaviour of individuals, combined with the vulnerability of children, that causes issues such as sexual exploitation; the technology only makes it easier to spot.

Likewise, the Internet exposes us. It does not change us. Somebody writing negative comments on Facebook, for example, exposes themselves; it is not the technology changing our behaviour.

INAPPROPRIATE CONTENT

The level of graphic sex and violence that is easily accessible in both video format and still images online should never be underestimated. Cameras now record in ultra-high definition, and audio quality is also crystal clear; nothing is left to the imagination.

11-16-year-olds are one of the largest audiences for pornography websites. Extreme material can be accessed anywhere and at any time, and this can have severe consequences on a child's mental health, including warping their perception of how relationships function. This can have life-altering consequences.

Graphic violence, including torture and executions, is also readily available. Again, the adverse effects on a child's mental health can be severe.

Inappropriate content can be searched for but a child may simply stumble upon it accidentally, or it may be shared directly with them by somebody else.

Inappropriate content can come in many other forms, such as through negative comments on social media platforms, chain mail in WhatsApp conversations friend requests from strangers.

How children interact with online content should also be given equal consideration. For example, a completely private TikTok account could still make a child feel insecure about their own appearance through the use of the beautification filters generated as part of the app. Another example is a child misinterpreting a comment, or writing a comment that is read by the recipient in a way that was not intentional.

EXAMPLES OF AREAS FOR CONCERN

- Access to inappropriate content such as violence and pornography
- Negative comments made on social media platforms such as Facebook, including apps such as TikTok and WhatsApp
- The way beautification photography filters warp the way children see themselves
- Overuse of mobile phones which breeds laziness, a detachment from reality and dependency
- Fear and anxiety generated through pressure to engage with chain mail, as often seen on apps such as WhatsApp (i.e. 'send this to X number of friends or something bad will happen')
- Grooming by paedophiles posing as children on social media platforms
- Websites and chat rooms that encourage self-harm and suicide
- Seeking validation through likes, followers and comments on social media (it is interesting to note that, as a pilot, Instagram recently removed all likes from its platform in Australia in an attempt to improve the mental health of users, and this may be rolled out across the platform)

How can I ensure that my child is protected?

Please note that the instructional examples below given relate to iPhone for mobile devices. The guidance may be the same/similar on Android and desktop versions.

Examples are given for some of the most common platforms but not every platform is mentioned in this document. All principles apply across all platforms.

Accept that your child (every child) is at risk and understand the risks.

Establishing trust and being able to talk to your child about the Internet and social platforms (and for them to be able to talk to you) is possibly the most effective approach anybody could take.

As humans, we are naturally curious. Do not let your expectations of your child block the likelihood that at some point they may want to access inappropriate material simply out of curiosity, as may their friends.

Do not underestimate the volume and extremity of inappropriate content available online.

It is vital that you acknowledge your child is at risk, however small the risk may be, even if they do not have access to a mobile phone or computer, simply because of the prevalence of both the Internet and electronic devices. Ignoring the issues or treating them as trivial could result in your child being exposed to something that causes them significant distress.

Managing expectations

- Children will probably find ways around your controls if they want to, so building trust is highly important.
- Threatening to remove devices from children is unlikely to build trust and encourage children to share negative experiences.
- No matter what safety measures you put in place, children will inevitably encounter adult/inappropriate content as they get older. What will they do when this happens? Will they come and talk to you? Will they be too embarrassed/scared?
- When talking to children, it is important to show a real interest, and not to dismiss online activities as less valid/important.
- Discuss screen time in a nuanced and positive way (instead of "children spend too much time looking at screens", try "some online activities are more beneficial than others"). There is no evidence that screen time itself is a problem, but that repetitive and negative activities, combined with lack of sleep and time to be mindful have an impact. A useful reference point is https://www.childrenscommissioner.gov.uk/our-work/digital/5-a-day/). And consider what they would be doing instead.
- Remember that messaging on social media apps is a part of how young people socialise and is not separate from it. It is important that parents understand this and approach the subject without too much judgement: children will open up and share if they feel able to. Chatting in 'real life' is not intrinsically more valid than communicating online.

Treat computers and mobile devices differently

The way mobile devices are used is very different to the way a computer is used (such as desktop PC or laptop). This is because a mobile device is completely portable and treated as a highly personal possession - particularly a mobile phone. As such, it is often used in a completely different way. A child is more likely to exercise their curiosity on a mobile device and do this in the privacy of their own bedroom, for example. A child will also engage with many more platforms that are only available on mobile devices.

If your child has access to a mobile device and a computer, consider how they use each one and why.

A home computer is more likely to be used as a family computer and based in a static location, in which case a child is more likely to be more reserved in their use of it. The browser (such as Chrome, Firefox or Internet Explorer) may be used as an educational tool and little else (searching for homework-related topics, playing games etc.).

A mobile phone, for example, is much more likely to be used to access social apps, such as WhatsApp, TikTok, Facebook and Snapchat.

HOW TO SEE WHAT YOUR CHILD HAS BEEN LOOKING AT USING A BROWSER

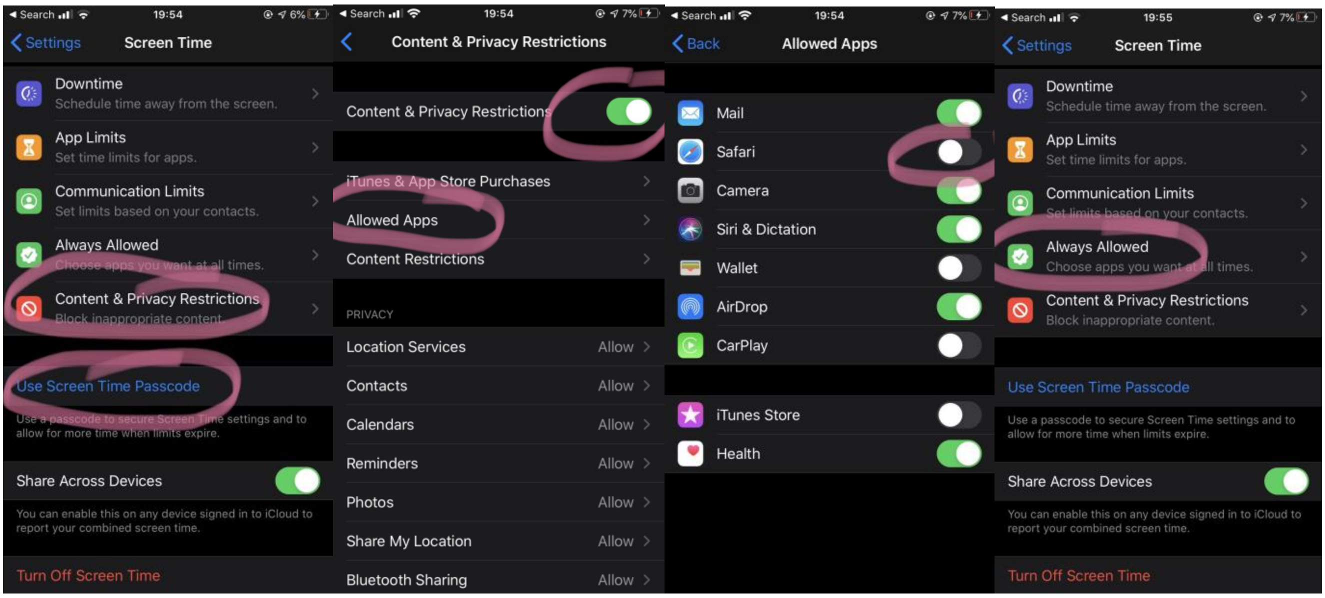
Each time you search for something online (using a browser such as Internet Explorer, Chrome, Firefox or Safari, for) information relating to what you searched for and any websites you visited is stored in the browser's history. This applies to any device. Your child is unlikely to know how to clear the history of a browser.

- Your browser may show 'History' as a tab. Or it may be hidden in a menu (for example, accessible by clicking 3 small dots at the top far right of the screen in some browsers). Access the history to view activity. If you are logged into Google when the browser is being used (Google Chrome), the history will also be stored in your Google account and therefore accessible to you from your Google account and not tied to that specific device.

It is possible that your child does know how to clear history, so an absence of reference to anything significant does not necessarily mean that they have not seen something inappropriate.

HOW TO REMOVE ACCESS TO MOBILE DEVICE BROWSERS (SUCH AS SAFARI) AND APPS (SUCH AS YOUTUBE AND TIKTOK)

Presuming that removing access to a home computer browser is not practical, removing access to the browser on a mobile device (such as Safari and Chrome, for) could be useful, especially if your child does not need it. This will result in your child being unable to search for anything on the Internet and so drastically cuts down on the risk of them being exposed to inappropriate content. You can remove access to browsers and apps on Apple devices through **Screen Time** as follows (if you do not use Apple, your device may have something very similar so be sure to check):



Settings — Screen Time

Downtime — Schedule time away from the screen.

App Limits — Set time limits for apps.

Communication Limits — Set limits based on your contacts.

Always Allowed — Choose apps you want at all times.

Content & Privacy Restrictions — Block inappropriate content.

Use Screen Time Passcode — Use a passcode to secure Screen Time settings and to allow for more time when limits expire.

Share Across Devices: On — You can enable this on any device signed in to iCloud to report your combined screen time.

Turn Off Screen Time

Content & Privacy Restrictions

Content & Privacy Restrictions: On

iTunes & App Store Purchases

Allowed Apps

Content Restrictions

PRIVACY

Location Services	Allow
Contacts	Allow
Calendars	Allow
Reminders	Allow
Photos	Allow
Share My Location	Allow
Bluetooth Sharing	Allow

Back — Allowed Apps

Mail	On
Safari	Off
Camera	On
Siri & Dictation	On
Wallet	Off
AirDrop	On
CarPlay	Off
iTunes Store	Off
Health	On

Settings — Screen Time

Downtime — Schedule time away from the screen.

App Limits — Set time limits for apps.

Communication Limits — Set limits based on your contacts.

Always Allowed — Choose apps you want at all times.

Content & Privacy Restrictions — Block inappropriate content.

Use Screen Time Passcode — Use a passcode to secure Screen Time settings and to allow for more time when limits expire.

Share Across Devices: On — You can enable this on any device signed in to iCloud to report your combined screen time.

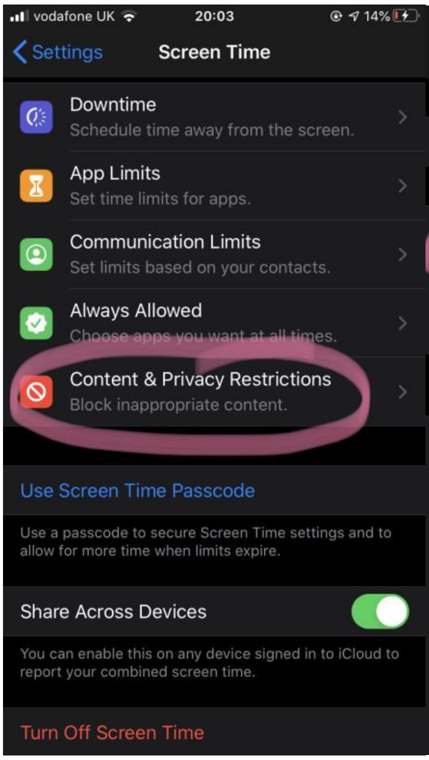
Turn Off Screen Time

BE SURE TO SET A PASSWORD THAT YOUR CHILD CANNOT ACCESS!

IMPORTANT NOTE

As your child gets older, it would be appropriate to allow more apps on your child's device. However, this must be accompanied by mutual trust - you should feel confident that they will tell you if anything bothers them, and they must trust that you will react in a reasonable and balanced way. For example, if your response to them showing you something inappropriate on their device is shock, outrage or punishment, they are unlikely to make further disclosures.

You can prevent apps (and purchases) being downloaded in the first instance by:



vodafone UK 20:03 14%

Settings Screen Time

Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

Communication Limits
Set limits based on your contacts.

Always Allowed
Choose apps you want at all times.

Content & Privacy Restrictions
Block inappropriate content.

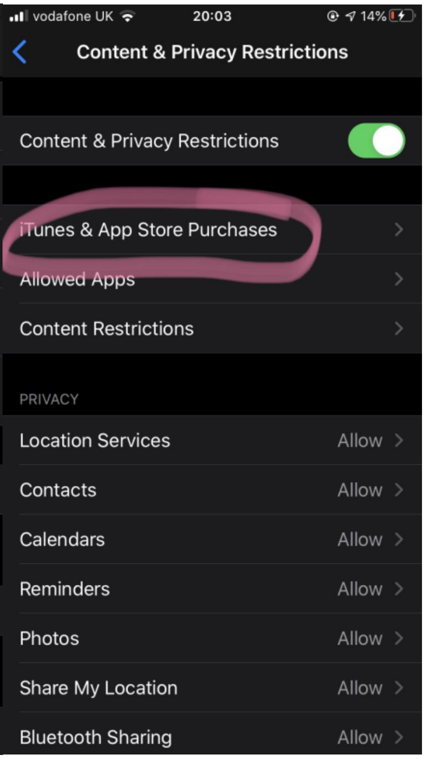
Use Screen Time Passcode

Use a passcode to secure Screen Time settings and to allow for more time when limits expire.

Share Across Devices

You can enable this on any device signed in to iCloud to report your combined screen time.

Turn Off Screen Time



vodafone UK 20:03 14%

Content & Privacy Restrictions

Content & Privacy Restrictions

iTunes & App Store Purchases

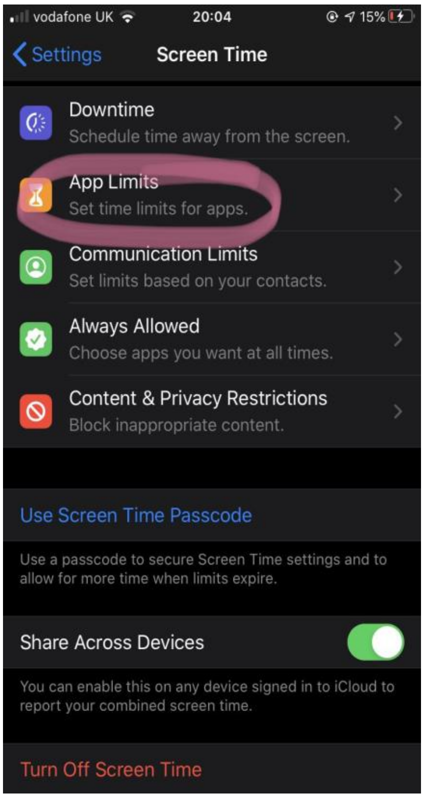
Allowed Apps

Content Restrictions

PRIVACY

Location Services	Allow
Contacts	Allow
Calendars	Allow
Reminders	Allow
Photos	Allow
Share My Location	Allow
Bluetooth Sharing	Allow

ADD A TIME LIMIT TO APPS ON IPHONE



vodafone UK 20:04 15%

Settings Screen Time

Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

Communication Limits
Set limits based on your contacts.

Always Allowed
Choose apps you want at all times.

Content & Privacy Restrictions
Block inappropriate content.

Use Screen Time Passcode

Use a passcode to secure Screen Time settings and to allow for more time when limits expire.

Share Across Devices

You can enable this on any device signed in to iCloud to report your combined screen time.

Turn Off Screen Time

Activate Parental Controls on your Home Internet Connection (also known as Parental Filters)

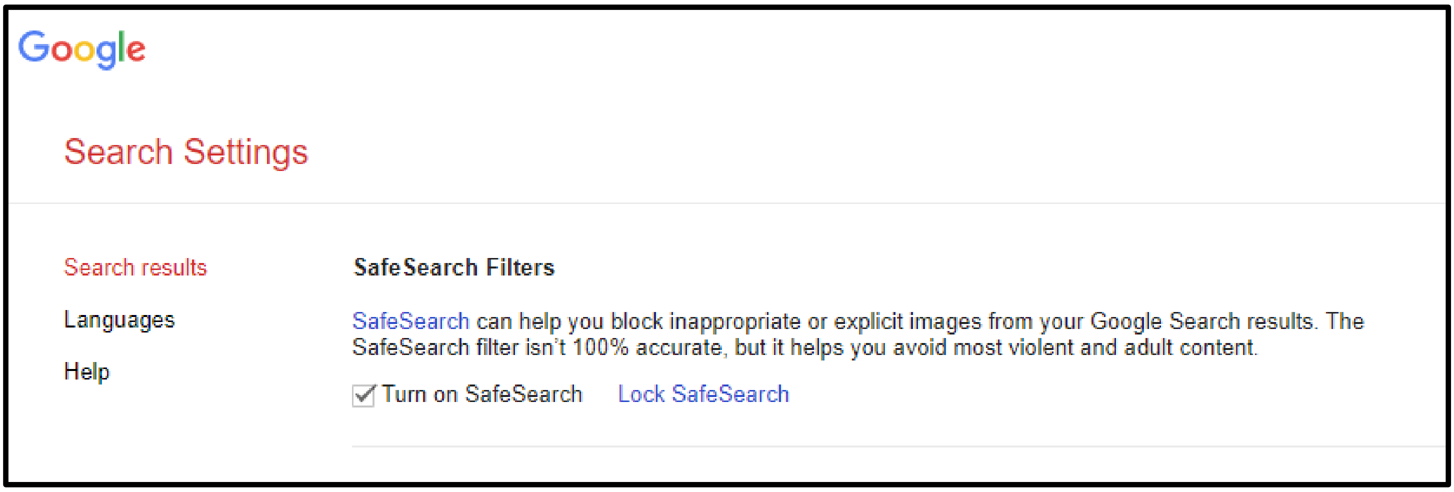
Place parental controls on all devices that access the Internet using your home Internet connection. Parental controls allow filters to be activated which will prevent certain websites from being accessible, based on the restrictions settings that you choose. It may be that links to inappropriate websites are still visible in search results, and the description of the website.

FILTERS DO NOT BLOCK INAPPROPRIATE IMAGES. If a child uses a search term for inappropriate content in an image search, the relevant images will appear. To block such images, you will need to restrict your actual website browser - please see '*How to filter inappropriate images*' below. Inappropriate images are much harder to block because it may not be clear that the images are associated with an inappropriate source (this is further highlighted by the use of images on social media which are linked only to a person's profile and so not flagged as inappropriate).

How to Filter Inappropriate Images

This may not be effective on all devices.

1. Create a Google account (use Google to search for ‘create a Google account’).
2. Visit https://support.google.com/websearch/answer/510 and follow the instructions.
3. Visit https://www.google.com/preferences
4. Turn on SafeSearch (you can also lock this using your google password


Google

Search Settings

SafeSearch Filters

SafeSearch can help you block inappropriate or explicit images from your Google Search results. The SafeSearch filter isn't 100% accurate, but it helps you avoid most violent and adult content.

☑ Turn on SafeSearch

This example is from a Windows desktop

Note that you must stay logged in to Google for SafeSearch to work.

How to Filter Inappropriate Websites

Start with your ISP (Internet Service Provider - such as Virgin Media, Sky and BT). Every ISP has a customer account login function. Once logged in to your account, navigate to Parental Controls and activate them. This will either prevent or restrict inappropriate content from being accessible. This is not completely effective so you cannot set it and forget it.

If you cannot access your account, simply contact your internet provider.

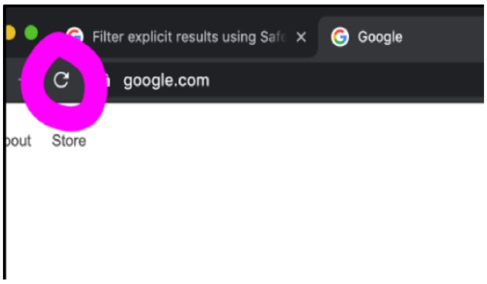
It may not be something that you feel comfortable doing, but test that the controls work by visiting a website that you consider to hold inappropriate content. You can do this by searching for an inappropriate topic in a web browser and clicking on links in the search results.

Virgin Media, for example, often does not always turn the child filters on successfully the first time.

ALWAYS REFRESH YOUR BROWSER AFTER YOU HAVE ACTIVATED FILTERS TO CHECK THAT THEY ARE ACTIVE.

HOW TO REFRESH YOUR BROWSER

This example is from a Windows desktop but the principal is the same across devices



ACTIVATE PARENTAL CONTROLS ON A DEVICE THAT IS USED OUTSIDE OF THE HOME

If your child has access to mobile data and can therefore access the Internet when not connected your home Internet, ensure that the company providing the data (such as Vodafone, O2, EE) has parental filters activated and that the apps used on the phone have filters set.

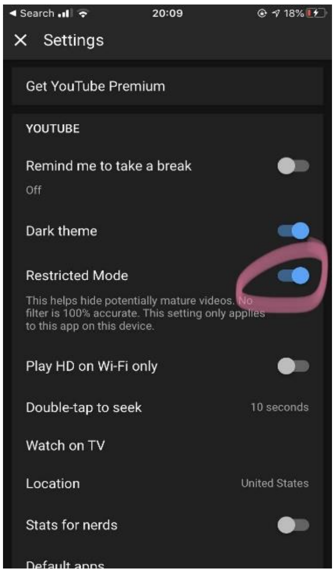
Your child may connect to a WiFi network outside of home, such as at a friend's house. If you are concerned about your child seeing inappropriate content, speak openly with the parents/guardians of the friend they are visiting to ensure that measures are put in place to prevent this. If you feel that this is ineffective the most effective solution would be to prevent your child from visiting the household.

USEFUL RESTRICTIONS WHEN USING YOUTUBE

This example is from an iPhone

YouTube also has a child-only version:

YOUTUBE KIDS



◂ Search 20:09 18%

× Settings

Get YouTube Premium

YOUTUBE

Remind me to take a break ○
Off

Dark theme ●

Restricted Mode ●
This helps hide potentially mature videos. No filter is 100% accurate. This setting only applies to this app on this device.

Play HD on Wi-Fi only ○

Double-tap to seek — 10 seconds

Watch on TV

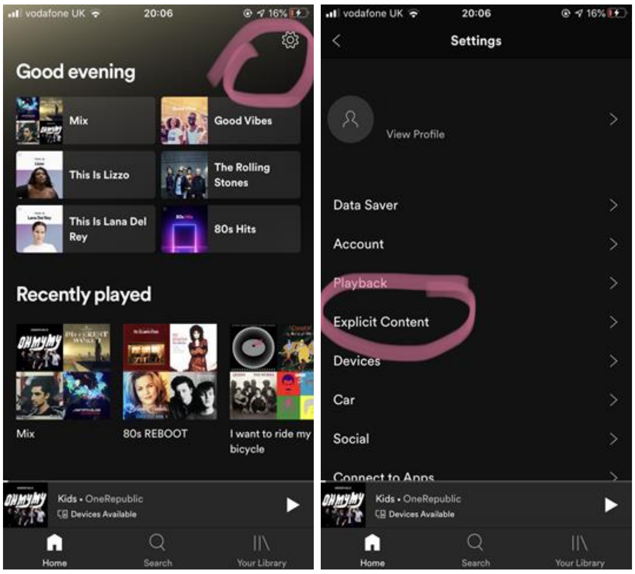
Location — United States

Stats for nerds ○

Default apps

FILTER EXPLICIT LYRICS ON SPOTIFY

This example is from an iPhone



vodafone UK 20:06 16%

Settings

View Profile

Data Saver

Account

Playback

Explicit Content

Devices

Car

Social

Connect to Apps

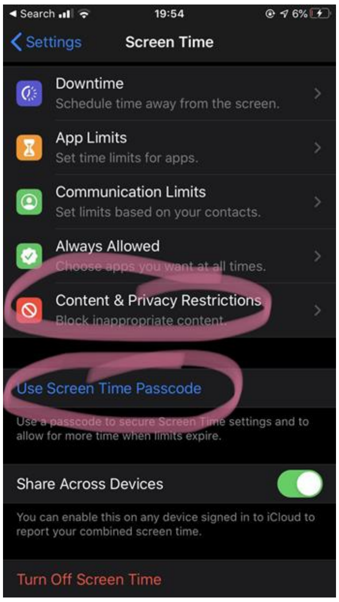
PREVENT STRANGERS TALKING TO YOUR CHILD ON FORTNITE

Instructions can be found here:

https://www.internetmatters.org/parental-controls/gaming-consoles/fortnite-chapter-2-battle-royale-parental-controls-guide/

BE AWARE THAT BY DEFAULT, ANYBODY CAN JOIN A GAME AND TALK FREELY.

USEFUL RESTRICTIONS FOR TIKTOK



Downtime
Schedule time away from the screen.

App Limits
Set time limits for apps.

Communication Limits
Set limits based on your contacts.

Always Allowed
Choose apps you want at all times.

Content & Privacy Restrictions
Block inappropriate content.

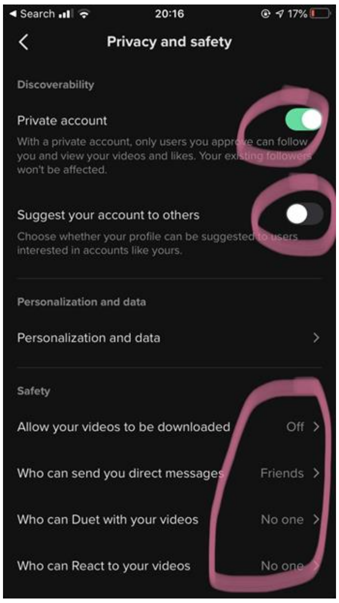
Use Screen Time Passcode

Use a passcode to secure Screen Time settings and to allow for more time when limits expire.

Share Across Devices ●

You can enable this on any device signed in to iCloud to report your combined screen time.

Turn Off Screen Time



Discoverability

Private account ●

With a private account, only users you approve can follow you and view your videos and likes. Your existing followers won't be affected.

Suggest your account to others ○

Choose whether your profile can be suggested to users interested in accounts like yours.

Personalization and data

Personalization and data

Safety

Allow your videos to be downloaded — Off

Who can send you direct messages — Friends

Who can Duet with your videos — No one

Who can React to your videos — No one

PREVENT A FACEBOOK PROFILE BEING VISIBLE TO THE PUBLIC

Go to **Settings**

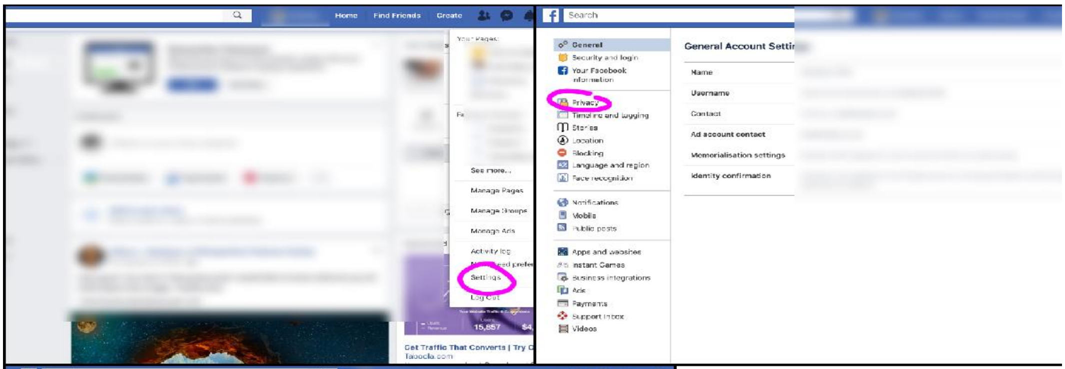
Go to **Privacy**

Make sure it just your **friends** who can see your future posts.

Limit past posts.

Limit who can send friend requests by selecting **friends of friends.**

Limit who can look you up by your phone number and email address to **friends.**



General Account Settings

Name

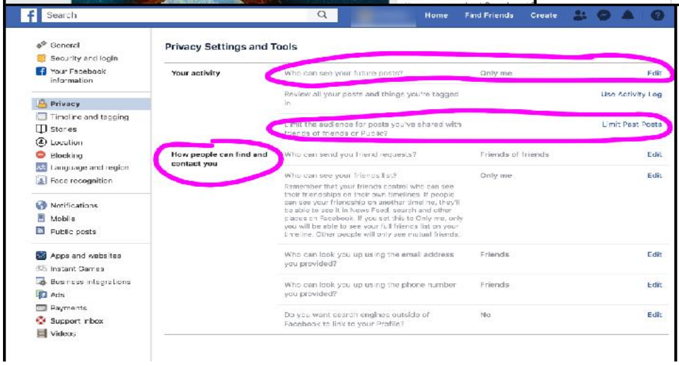
Username

Contact

Ad account contact

Memorialisation settings

Identity confirmation



Privacy Settings and Tools

Your activity	Who can see your future posts?	Only me	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How people can find and contact you	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list? Remember that your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will only see mutual friends.	Only me	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your Profile?	No	Edit

WhatsApp Chain Mail

Chain mail is a highly passive-aggressive form of communication that serves no purpose but can cause fear and anxiety. In order to identify this, you may need to access your child's phone.

Chain mail essentially asks the recipient to forward the message to more people and threatens that if this is not done then bad things will happen.

Information we post can be damaging

Any information that is communicated via a social media platform can be visible to members of the public unless you ensure the relevant privacy settings are in place.

For example, if you have a Facebook account, is your profile public? Many profiles are public without the account holder being aware, and posts and images are available for anybody to look at.

(see *Prevent a Facebook profile being visible to the public* above).

Information that is sent privately could also be brought into the public domain simply because the information can be copied (such as images captured as a screenshot) and posted elsewhere by the recipient.

It is worth nothing that aside from safeguarding concerns, employers now use searches to look for information relating to candidates.

Information posted online can remain online forever.

Summary

This applies to any platform that is being used online and on any device:

Top tips

Do not assume that the default settings of a particular device/service are suitable for your child. It may be that you need to change them.

- Consider who could find your child online and how they could communicate with them.
- Consider what information is being engaged with and shared by your child.
- Consider if the platform is appropriate or not.
- Consider the possible harmful effects of platforms that beautify your child.
- Set parental filters.
- Set privacy settings.
- Turn off commenting (could be restricted to friends only).
- Explain how comments work and how comments online are different from face-to-face comments.
- Turn off friend requests (could be invite only).
- Do not engage with chain mail.
- Do not focus on getting likes and followers.
- Be mindful of the amount of time being spent online and the purpose it is serving.
- Be open with your child and have regular conversations about online activity.
- Check your child's online activity regularly, including browser history and chat messages.

STAY INFORMED

THE INTERNET IS CONSTANTLY EVOLVING. The guidance outlined in this document may therefore become obsolete over time. It is advised that you keep yourself informed of changes and improvements in technology.

SOME USEFUL WEBSITES

Parentzone (digital family advice)
https://parentzone.org.uk/home

Childnet (keeping children safe online)
https://www.childnet.com

NSPCC (preventing abuse)
https://www.nspcc.org.uk/keeping-children-safe/online-safety/?ac=140903#guides

Netaware (specific advice about apps and websites)
https://www.net-aware.org.uk/

ThinkUKnow (online education programme, aimed at teachers)
https://www.thinkuknow.co.uk/parents/

Fight The New Drug (how porn kills love)
https://fightthenewdrug.org/how-porn-kills-love/

QUESTIONS?

If you have any questions please do not hesitate to contact:

Mr Winterbotham at TWinterbotham@chorustrust.org

ACKNOWLEDGEMENT

Many thanks to Graeme Tidd for taking the time to produce this document. It involved a huge amount of expertise and hard work and Malin Bridge School appreciate his efforts to keep our children safer online.