Online Safety Booklet

Inside this booklet we will cover various social media apps, along with settings and games on your children phones.
Below is some of the things we will be covering.

Phone Settings
Facebook
Snapchat
Instagram
Kik
Tiktok
Live.Me
Youtube
Minecraft
Roblox
Fortnite
Catfishing
The App Store
Online Challenges
Online Grooming
Sexting

"It takes on average 45 minutes to groom a child online, but only 5-10 minutes to check out child's devices"

Phone Settings

On your child's phone, click onto settings and scroll down to **'Screen-time'**
'Downtime' allows you to set a schedule for time away from the screen (For example: Dinner time), during downtime, only apps that you choose to allow and phone calls will be available.
'App Limits' allows you to set daily time limits for app categories you want to manage. App limits reset every day at midnight.
'Always allowed' apps are available during downtime or if you selected the All Apps and Categories app limit.
'Content and Privacy Restrictions' allows you to block inappropriate content.
Using a screen-time password to secure the screen-time settings and to

allow more time when limits expire.
If your child is on your iCloud, you can share screen-time to any device on the cloud.

Facebook

Facebook's minimum age is **13**, although this is often and easily bypassed.
Know your child's login details; this is not to breach privacy and should never be misused, however there are many benefits to having this information.
1.) Freedom to check your children friends list's, I will explain shortly how to set their friends list to private, this will mean the only way for you to view it, will be to log in.
2.) Children tend to behave more online and avoid dangerous sites and apps if they know you can check their accounts at any time.
3.) Ability to check for any out go place messages from strangers or suspicious activity on their account.
To check your child's privacy settings on Facebook, simply press the 3 lines on the bottom right hand side of your screen and scroll down to settings and privacy, click settings, privacy settings and make sure any personal details such as phone number and home address is set to **'Only me'** and other information such as posts and photos are set to **'friends only'**.
While in this settings scroll down to **'Who can see your friends list'** and choose **'Only me'** or **'Specific friends'** and choose yourselves or trusted friends/family.
Further down in the settings part of Facebook, scroll down to **'Location settings'** and turn this off on your child's device.
Facebook has been linked to **311 Grooming cases** in a matter of **9 months** and was described by the head of Britain's top child abuse investigating agency as one of the UK's major online locations for **child sex grooming.**

Snapchat

Snapchat's minimum age is **13**.
Find snapchat settings by pressing onto the profile logo (Top Left) and then selecting the cog icon.
In settings scroll down to the **'Who can'** option and set to **'Friends only'**
Set **'View my story'** as '**Friends only'** and change **'See my location'** as **'Only me'**
As well as these settings, parents should do regular checks of their

child's friends lists for new or unknown persons.
You can check your child's snapchat friend's by clicking the small speech bubble on the camera page, then pressing the same speech bubble in the top right hand corner.
To remove anyone from your child's list, simple hold your finger in the contacts name and you will see the menu with the option to '**remove friend or block'.**
'Two factor authentication' is added security for logging in on new devices. To add this extra feature just go to your snapchat settings and click the **'Two factor authentication'** menu, this will prevent anyone else gaining access to your snapchat.
'Quick add' allows snapchat to show your profile to other users who you are currently **not connected to** and don't have on your contacts list. To turn this off, go into **snapchat settings**, scroll down to **'Who can'** and click **'See me in quick add'**
I highly recommend enabling **'Ghost mode'** on the app so that your child's location will no longer be visible to anyone on the **'Snap map'.** To enable this, go onto the **'Snap map'** and tap the cog in the top right corner. Here, change the settings to **'Ghost Mode'**
Snapchat has been linked to **176 grooming cases** in the past **9 months**. According to the **NSPCC** snapchat was linked to **14% of sexual grooming cases in 6 months in 2018.**

Instagram

Instagram's minimum age is **13.**
To make your child's Instagram account **private**, simply click on the small person at the bottom right hand side of the screen.
Click the 3 lines at the top right hand of the screen and at the bottom there should be a sign saying **'Settings'**, once you click this go down to **'privacy & security'** and set the **'account privacy'** to **'Private account'**
This prevents strangers following your children online and viewing images and videos your children upload.
Your child is in control of who can comment on their photos and videos . In the **'Comment Control'** section of the app settings, they can choose to **'Allow comments from everyone' 'people they follow'** and **'those peoples followers'**. Alternatively you can also completely **'turn off commenting'** on all posts. You can also '**turn off comments'** from **'individual persons'** on **'individual posts'** or **'all posts'.**
Your child can also add **'Manual Filter'** which means they can choose certain words that will be instantly blocked from their page, this will lower the risk of, **swearing, bullying** and any sort of **sexual comments** that

may be put on your child's posts or pictures.

KIK Messenger

Kik messenger's minimum age is **13.**
When setting up a Kik account, ensure that your child knows the importance of a **secure username** and why it shouldn't contain any clues as to who they are in real life, especially their **first** and **last names.**
Explain to your child that showing said username on social media such as Twitter and Facebook could make your username visible to many people who are unknown to them, and they will then be able to **contact your child** on Kik.
If your child is **under 13**, you can submit a **deactivation request** to Kik by emailing **Support@kik.com** using the subject line ***Parent Enquiry*** and including your child's Kik username and age in the email.
If your child is **over 13 but under 16** and you want to **close their accoun**t, you will need access to the email address registered to their account before you visit ***https://ws.kik.com/deactivate.**
Teach your child how to **block and report** users on the app. Kik's block feature lets users **block all contact** with another user without revealing to the other user that they have been blocked. Your child can also **report a group** if they think it is **offensive** or being used for **abuse**.
Some users of Kik have reported that they receive **sexually explicit automated messages** over the app, this is when automated **spambots** have been used to **distribute explicit images** and texts using the service. Your child can use the **'Report'** feature to **report spam**, once reported, there is the option to keep or remove chat from the conversation list. If conversations are saved Kik will automatically **block the spam account** but **save the chat history.**
What makes Kik **unique** to most other private messaging apps is the fact that it **doesn't require** a phone number as it works through WIFI instead. By using a username, your child can **avoid sharing** personal information with others on Kik, but on the flip-side, this makes it easier for people to r**emain anonymous** or to create a **fake persona.**
Police in the **UK** have warned that Kik has featured in more then **1,100 child sexual abuse cases** in the last **5 years**, and that **children are at risk** on the app.
Offences involving the app include, **Child Sexual Exploitation, Grooming and image violations.**
Kik has also been identified by **US police** as being used by **sexual predators**, and they say it is responsible for **several recent incidents** involving **children**, including the **murder** of a **13** year old girl by a man

she met via Kik.
Some people may use Kik with the intention of **targeting children**. Typically this is a **subtle** and a **potentially dangerous** individual who may initially portray themselves as a **friend** who understands a child. They may also **lie about their age** and its possible that your child could be **manipulated** by a stranger into doing **regrettable** or **illegal activities** and perhaps even **meeting in person**.

Tiktok

Tiktok's minimum age is **13.**
By default users accounts are **automatically** set to **public** when they first create an account.
Tiktok encourages users to **share** creative expression through their **videos**, but if posted **publicly**, anyone in the **world can see** your child's homemade content.
If your child's profile is open, **strangers** can use the app to **comment** on your child's videos. While this isn't always sinister, it gives **potential predators** the ability to **contact** your child through the platform.
Tiktok lets users lip sync their favourite songs and produce music videos. Some of the music choices contain **swear words** and **sexual themes**, so not only can children be **exposed** to potentially **inappropriate content** but they can broadcast themselves miming or singing these lyrics.
There has been reports of some users promoting **anorexia, porn, self harm and violence**.
If you or your child see something inappropriate on Tiktok, you can **flag up** an account, video, comment or chat by simply tapping **'report'** in the apps **'digital wellbeing'** feature. There is also an **'Enhanced restricted mode'** limiting appearance of videos which may be inappropriate.
Setting up a **private account** means only people who you and your child approve of can see their creations. To make an account private, tap the three dots at the top right hand of the screen to access settings. Click **'Privacy and safety'** scroll down until you find **'Private account'** and turn this seeing on.
When signing up users are prompted to input they date of birth, if the date of birth they have entered means your child is **under 13,** they app will block them. However this doesn't stop your child from **lying about their age.** The app is intended for people ages **13 and over**, so explain the rating is there for a reason; to keep them protected from **online dangers**. It is actually possible to watch Tiktok videos without creating an account, so make sure your child, if under 13, hasn't downloaded the app.

LiveMe

Live me's minimum age is **17.**
LiveMe is a **streaming video** app that lets you watch live streams and broadcast your own live videos to anyone interested.
Publishing live videos can give away clues to your **child's identity** and **location**. **Predators** will search videos to identify information in the background that gives details about your child such as, street names or school uniforms. Explain to your child that they need to think carefully about where and when they broadcast live.
As with anything that is posted and shared with other people and online, remember that once it is up, its hard to take back. Once videos are shared online, they become public. Videos can attract the attention of **sex offenders** or someone may **threaten** to share videos with others unless your child sends money or more videos.
The only way to know what your child is watching or broadcasting on LiveMe is by regularly monitoring their usage, remind your children to never share any personal information with people they do not know online.
If someone has been acting inappropriately, you are encouraged to ask for help by emailing **'LiveMe@cmcm.com'** with the subject line **'ATTENTION:INAPPROPRIATE BEHAVIOUR'** and send evidence, including a screenshot of their profile. You can also directly report inappropriate content from inside the app using the report option. However, it is worth remembering that it is not wise to screenshot and save inappropriate material.
Explain to your child that is they notice **inappropriate behaviour, bullying**, or any other **rule-breaking conduct** on LiveMe, they can **block** a user from chatting on their broadcast and profile by tapping on their name, navigating to their profile page and then choosing 'block'
Live streaming apps can potentially expose young people to **graphic** and **inappropriate content**. LiveMe says it is 'explicitly intended to be used by individuals 17 years of age or older'. Those under 18 should have their **parents permission** to download and use the app, but there are no age verification checks. As soon as you open the app or websites homepage, you are greeted with scantily clad adult broadcasters, posing suggestively with captions such as **"Join me in bed"**. There is every chance your child will watch content that is not suitable for them or be encouraged to share similar content themselves.
Law enforcement agencies have warned that LiveMe is placing children at risk from online predators. A sheriff in Texas issued a

warning that Paedophile's have a virtual open window to your child's bedroom. Live chat can be used by **online groomers** to target young people who may be manipulated into sending **sexual images** and videos. LiveMe also has a chat feature, which allows users to speak to each other in private. In 2018, a **65 year old male** in the **UK** was **jailed** for posing as a teenage boy to **groom young girls** on LiveMe, and offered virtual currency in exchange for teenagers exposing themselves.

YouTube

As youtube is the biggest video sharing website in the world, there is content available for all ages, meaning some content will **not be appropriate** for your child. If you think that content is unsuitable, there is a flagging feature to **'submit for review'** by youtube staff, but you will need to be aware that just because a video is not appropriate for a younger audience, it may not violate youtube's policies. Youtube has mechanisms in place to automatically **remove explicit** and **harmful content,** yet offensive content may still slip through.

Restricted mode is an optional setting you can use to help screen out potentially mature content you may prefer your child not to see.

Restricted mode works on the browser or device level, so must be turned on for each browser or device your child uses. To do this, follow these steps:

On a desktop:

Go to the bottom of any Youtube page and switch **'Restricted mode' to 'ON'**

To make it more difficult for this to be turned off, you will be given the option to lock restricted mode onto the browser.

On a mobile:

Tap the three vertical dots at the top-right on the screen and press **'Settings'**

Click on **'Restricted mode filtering'**

Press **'Restrict'**

Please note that you can't lock restricted mode on a phone the same way that you can on a desktop. You will to turn this on each time you child uses it.

When using Youtube, there may be instances where your child receives negative comments. If somebody's giving your child a difficult time, here's how to block them and prevent future comments and replies:

Go to their **channel/account** by clicking on their name,

Click on **'About',**

Tap the **'dropdown box'** with an image of a flag on it,

Press **'Block user'**

Tap **'Submit'.**
Youtube has launched a tool called **'Time Watched'** that allows you to see how long has been spent on the platform. Once you have discovered how much time has been spent on the app, there is the option to set a time limit. Once the limit is reached, a reminder will pop up on the screen. You can also disable sounds and vibrations to help resist the urge to check for notifications.

Minecraft

Minecraft's minimum age is **10 (No age restrictions)**
Minecraft chat automatically shows up when you join an online server and another player or character approaches yours.To **avoid potentially inappropriate comments** in live chat, you can follow these steps to turn live chat of; 1. Select **'Options'** 2. Toggle the chat button to **'Hidden'** or **'Commands only'.**
When you join the game and begin playing hit the **[ESC]** button on your PC or Laptop, if you are playing with a phone or tablet press the '**pause logo'** in the top right of your screen. You should now the see the games menu, press **'Options'** first and then press **'Multiplayer Settings'** You now need to press the chat button until it shows as hidden. Chat will now be invisible and you will see zero messages from anyone else on the game.
The majority of users who play Minecraft are children, making it an **'appealing'** gateway for groomers. It has been reported that some users have created worlds in Minecraft to **lure young people** into a conversation to ask **for explicit** photos. There have been more **serious cases** in which children have been persuaded to **meet these people** in real life.

Roblox

Roblox's minimum age is **8.**
Whilst the games in Roblox are aimed at **8-18 year olds**, there are currently no age restrictions for signing up. This means both adults and young people can play and communicate with each other and send friend requests through the platform. Once a friend request is accepted this means they can communicate with others outside of gameplay.
Make sure your child's social media accounts are not listed in the settings/account information. If they are, advise them to make them **private** or **remove** them in their account. This will ensure nobody can find and contact them on social media platforms outside of Roblox.

In the accounts settings, check that your child is not giving away any **personal information** in their bio/profile. For example, their full name, phone number or snapchat username. If you see that they have, explain why this is **potentially dangerous** and remove it immediately.
Rob lox is great for children to play together and chat to each other, however if you wanted to completely turn off chat for your child (Meaning they could not contact anyone including friends) you can do so by following these steps:
When logged in, go to the **'account settings'** page by clicking on the **'gear icon'** at the top right corner of the page, then click **'settings'**. Next clicl on the **'Privacy tab'** and under **'Who can chat with me in game'** select **'No one'** and this will disable in game chat.
Rob lox has been linked to multiple online **grooming cases** in the **US & UK** with children **as young as 5** receiving messages with very **inappropriate content and asking for meets.**

Fortnite

Fortnite's minimum age is **12.**
Signing up to the game is relatively simple. Users have the option to log in with either their Facebook or google accounts or their email address. When signing up with an email address, **no proof of age** is required. If your child is under the age of **12,** it is important to check whether your child has the game downloaded.
Interacting with other players in the game is part of the fun as players can communicate with their friends and other players in the game. Players will benefit from wearing headphones to hear footsteps from other players trying to compromise their game. Wearing headphones makes it difficult for parents to hear exactly what is being said and children may be **exposed** to **inappropriate language**, Fortnite includes really good **reporting features** for players either **cheating** or **misbehaving**, and works towards having one of the best online gaming communities.
There is an option to **turn off** the voice chat feature, which means your child wouldn't be able to talk to anyone, including friends. However they would still be able to use in 'In-app chat and hear other peoples conversations. To turn off voice chat, open the **'Settings'** menu in the top right of the main fortnight page, then click on the **'Cog icon'**. Open the audio tab at the top of the screen. From there, you can turn off voice chat.
If your child believes a player is playing or **talking inappropriately**, you should advise them to report them. To report a player, you can use the **'in-game' feedback tool** located in the main menu of the game.

Additionally, you can report a player in-game when spectating them.

Catfishing

The term '**Catfish'** was coined in a 2010 documentary about a man who developed an **online relationship** with a women, only to discover the person he thought he was communicating with was someone else. **Catfishes** make up life stories and use photographs of **unsuspecting victims** to create **fake identities**. They will share life experiences, jobs, friends and photographs to the fake accounts. The aim of the **perpetrator** may be to **lure victims** into a **sexual relationship,** but they can also be part of social engineering to trick people out of money. After building up trust and developing an online relationship, a catfishes may ask for cash for a loan, money for travel, or some other form of payment. **Cat fishing** can escalate very quickly. As someone executing a **catfishing** scam is looking to achieve a goal, - whatever that may be - they are likely to want to get things moving as quickly as possible. The victim may be encouraged to develop a relationship faster then they are comfortable with. In addition to this, people who create **fake identities** could also be taking the **victims photos** and pretending to be them. It is common for fraudsters to post pictures stolen from social media sites, including Facebook and Instagram.

Go through your **child's privacy** and security settings thoroughly to ensure that their online profiles are set to private. This means that only friends can see their profile and can contact them. It may also be a good idea to check through your child's friends list with them - do they know and trust everyone on the list? In some cases, its difficult to stop children talking to new people. In these circumstances, encourage your child to be curious and ask lots of questions rather then rely on the information given in someones online profile. Do they have any mutual friends? If not, how did that person find them and why did they reach out? Its vital that they know **never** to arrange to meet up with people they meet online, and never send money to them — either their own, or from your account.

Make sure that you and your child is aware of how to **report and block accounts** on all platforms that the child uses. You can r**eport fake accounts** and **block users** to prevent them from viewing your child's profile, as explained above with all apps.

The App Store

To download and buy apps from the app store, your child will need an apple ID. If they have used other apple services, such as iCloud, they

can sign into the app store with the same apple ID. If they are aged **13 and under**, they cannot sign up for an apple ID on their own, but an adult can create an apple ID for a child.
You can create an Apple ID for a child **under 13** and add them to your group to keep an eye on their activity.
Go to **'Settings' > [Your name] > Family sharing > Add family member > Create a child account > Next, enter your child's birthday and tap next.** Review the parent privacy disclosure and tap agree. With family sharing, you can add up to **6 family members** to share App store purchases, as well as iTunes and Apple books.
To find apps and games that are right for your children, check the age ratings. On the iPhone or iPod touch this can be found in the **'information section'** on the app's product page, and on the iPhone and desktop the age range is near the buy button. On the kid page, you can find apps for age ranges, including **5 and under, 6-8 and 9-11.**

Online Challenges

As well as having the potential to cause actual **physical harm**, some challenges can be extremely **upsetting** for children. Many are created with the sole purpose of **instilling fear** in an individual in order to coerce them into doing things that could have **long-term emotional effects** on them.
Its important to talk to your child regularly and monitor their online activities. Encouraging **honesty** and **openness**, will give you a much clearer viewpoint of how your child is interacting online and what concerns they have. Create an atmosphere of trust. Ensure they feel they can confide in you or another trusted adult regarding anything they may have seen or experienced online that upsets them.
As with all online activity, ensuring you have effective parental controls set up on all devices, will help filter and restrict the dangerous or inappropriate content you don't wish your child to have access to.
Additional measures for protecting your child include checking the **privacy settings** on your child's devices, monitoring their friends list and ensuring their personal information is safe and secure and keeping a watchful eye on the content they are sharing.

Sexting

Sexting is illegal if you share, **make, take or distribute an indecent image** or **video of a child under the age of 18**. Sexting or **'youth produced sexual imagery'** between children is still illegal, even if they are in a relationship and any images are shared consensually.

Many young people see sexting as ‘banter’ or a joke, an easy way to show someone you like ands trust them, or just a cool thing to do. But they may not realise the **consequences** of sharing personal information and how it can be **potentially harmful** to them in the future. Your child may feel **pressured** into sexting, so they don’t come across as boring, or think it's a way to show someone they care for them. They may feel under pressure to give in to repeated requests or feel obliged to share **sexual messages and imagery.** Sexting can also expose young adults to the risk of being exploited by Paedophile's or sexual predators, who then use the images to extort additional photos, sexual favours, and sometimes money from victims.

Once a photo is out there, there is no way of knowing how many people have saved it, tagged it, or shared it. Children like to show off to their peers and suddenly, an image has gone beyond its intended recipient, to classmates, friends and even strangers. Once an image or video has been shared online, theres nothing to stop it being archived and repeatedly shared.

Children and young people may not realise that what they are doing is illegal. Ensure that your child understands that when they are under the age of 18, it is **against the law** for anyone to take or have a sexual photo of them, even if it's a selfie, and even when the activity is **consensual**.

If an image has already been shared, either your child or yourself should speak to the person that the image was shared with and ask them to delete it. You can also use the **report** button on a website where the image was posted. Speak to your child’s school, as they may be able to confiscate phones if they know that they have **sexual imagery stored.** If you believe your child was **forced** into sending the image, **report this to the police.** You can also report straight to **Dewberry house.**

If your child has ever received a **sexual image,** assure your child they have done the right thing by coming to you. Ask them if they requested the image or if they received it unwillingly. If the image was send to your child by an adult and you are concerned about **sexual exploitation** please contact the **police.**

Online grooming

In April 2017, a new government law came into force in England and Wales to allow **police to charge** adults who send sexual messages to children through mobile phones and social media.In the first year since the law change, there were **3,000 police-recorded offences** of **sexual communication** with a child - a figure 50 per cent higher than experts expected in the first year.

According to a **2018 NSPCC report**, a quarter of young people have experienced an adult who they don't know in real life trying to contact them online. One in four said they had been sent messages, images, videos or other content that made them feel **sad, worried or uncomfortable**. One in 10 girls and one in 20 boys under the age of 13 said they had received **unwanted sexual messages.**

Groomers use **psychological tricks** and methods to try and isolate children from their families and friends and will often choose to target more **vulnerable children** who may be easier to manipulate. In order to seek **potential victims**, predators are likely to use apps and websites that are popular with children and young people. Groomers can use a **'Scattergun'** approach to find victims, contacting hundreds online to increase their chance of success.

Grooming is generally a slow, methodical and intentional process of manipulating a person to the point where they can be **victimised**. However, according to researchers at the university of Swansea, **online groomers** can also be very **rapid,** with analysis of chat logs revealing that it can take just **18 minutes** for some predators to arrange a meet with their victim.

The fastest predators used sophisticated, **persuasive language-based strategies** to rapidly build trust, including the use of small talk and praise which quickly escalated into requests for sexual messages.

Many people expect groomers to be adults **posing as children,** but this is not always the case. Data from the university of Swansea reveals that groomers use of identity deception (around age, location and appearance) is fairly low. This can be because they approach many children, limiting their ability to lie. The worry is that honesty can be more damaging to the victim since they are more likely to feel as if they are in a real relationship.

Talk to your child about what a **healthy relationship** looks like and how to detect someone who might not be who they claim to be. Explain that groomers will pay your child compliments and engage in conversations about personal information, such as hobbies and relationships. They may admire how well they play an online game or how they look in a photo. **Groomers** will also try and isolate a child from people close to them, such as parents and friends, in order to make their relationship feel more special and unique.

Show your child that you will support them and make sure they understand they can come to you with any concerns they may have. They need to know they can talk to you if someone does something they are uncomfortable with, whether that is **inappropriate comments, images, requests or sexual comments.**

Child safety experts have identified key grooming patters and advise for

parents to look out for:

Secretive behaviour about what they are doing online,

Internet or smartphone usage late at night,

Going to unusual places to meet up with friends you have no heard of,

They are clingy, have problems sleeping and eating or even bedwetting,

A lack of interest in extra-curricular activities,

Having new items, such as clothes or phones, which they can't explain,

They seem withdrawn, anxious, depressed or aggressive,

Having older boyfriends or girlfriends.

Of course these signs could be a warning for many other things but please be aware of what your children are doing online.

If you are worried that your child is being groomed online or sexually exploited, you can call the **police station on 01534612612,** the **NSPCC 01534760800** or **Dewberry House (SARC) (Sexual Assault Referral Centre) on 01534888222**

If you think your child is in **immediate danger** and needs safeguarding, call the police immediately on **999.**