



Minecraft is played by millions of children around the world, who can use their imagination to build three-dimensional worlds with virtual building blocks in a digital, pixelated landscape. It is classed as a 'sandbox game' which means players have the freedom to build their own creations with 'blocks' they collect and also have the opportunity to explore other people's creations with their characters. Players can choose from thousands of different 'servers' to join, which are created by other players, making every experience of Minecraft unique.

Minecraft has approximately **74m** users each month

AGE RESTRICTION **10+**

What parents need to know about **MINECRAFT**



GROOMING

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 even been more serious cases in which children have been persuaded to meet these people in real life.

CYBERBULLYING & GRIEFING

In multiplayer mode, there is a live chat feature which allows players to talk to other players through text. The chat functionality includes basic filtering to block out external links and offensive language being shared, but this varies between each server. Griefing is when someone purposely upsets another player during the game. This can be done by ruining somebody's creation or generally doing something to spoil gameplay for another. Essentially, 'Griefing' is a form of cyberbullying and can be extremely frustrating for players.

COMMUNICATING WITH STRANGERS

There are thousands of servers to choose from in Minecraft which are a single world or place created by the public, allowing users to play the game online or via a local area network with others. No two servers are the same and each server has its own individual plug-ins which are controlled by the creator. This means that some servers will allow communication with strangers.

VIRUSES & MALWARE FROM MODS

There are several websites that offer downloadable 'mods' which modify gameplay in a number of different ways. Most of the mods will be safe to use, but as they have been created by the public, they will often contain viruses that can infect your child's device and potentially try and find personal information from you or your child.

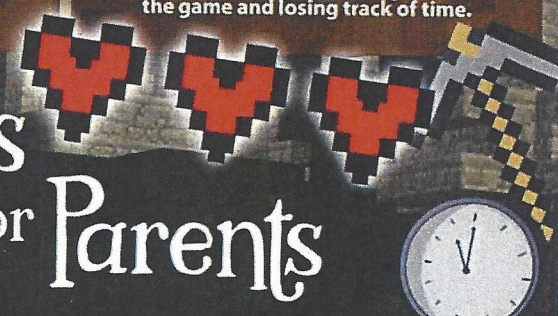


AGE RESTRICTION & 'FANTASY VIOLENCE'

According to the ESRB 'Entertaining Software Rating Board', Minecraft is suitable for users aged 10+. Due to its 'Fantasy Violence', the ESRB states that the rating has been given as 'players can engage in violent acts such as lighting animals on fire and harming animals with weapons. Mild explosions are occasionally heard as players use dynamite to fend off creatures and mine the environment.'

CHILDREN MAY BECOME ADDICTED

As with other games, Minecraft is a game where players can keep returning, with constant challenges and personal goals to achieve. Children may find it difficult to know when to stop playing, becoming absorbed in the game and losing track of time.



National Online Safety Top Tips for Parents

DISABLE OR MODERATE CHAT

To avoid potentially inappropriate comments in a live chat, you can follow these steps to turn live chat off: 1. Select 'Options' 2. Toggle the Chat button to 'Hidden' or 'Commands Only'. Bear in mind that the chat feature is also where your child can enter commands during the game, so this may limit their game play.

MONITOR YOUTUBE TUTORIALS

Many Minecraft users turn to YouTube for video tips on improving their gameplay and discovering new techniques. Although many videos are age-appropriate, some include sexual references and bad language. We suggest watching Minecraft tutorial videos together with your child. If your child is under the age of 13, we suggest installing 'YouTube Kids' which provides a safer platform for children to find the content they want, safely.



SCAN 'MODS' FOR MALWARE

Minecraft 'mods' add content to games to give more options to interact and change the way the game looks and feels. But while 'mods' can bring fun for a child, it's important to consider that downloading and installing 'mods' could potentially infect their device with a virus or malware. In 2017, security company Symantec said that between 600,000 and 2.5 million Minecraft players had installed dodgy apps, which hijacked player's devices and used them to power an advertising botnet. Install a malware scanner on every device that your child plays Minecraft on, and make sure it's up-to-date.

PLAY IN 'CREATIVE' OR 'PEACEFUL' MODE

Even though the age limit is 10+, Minecraft can be quite overwhelming at times, especially for younger players or SEND children. We suggest limiting your child to play in 'creative mode' or 'peaceful mode' which takes away the survival element and removes the 'scarier' monster/zombie characters.

SET TIME LIMITS

With 'Gaming Disorder' becoming an official health condition, we suggest setting a reasonable time limit when playing Minecraft. Parents can use parental controls on devices to limit the time a child is playing games. It is worth having a conversation with your child to understand what 'mode' they are playing on the game. This may help you decide on how much time you would like them to spend playing on it. For example, a mini game will have an 'end', but this will depend on how long the game creator has made the game last. In 'survival mode', the game has no end as there is no goal to be achieved other than the child's own e.g. after they have built something.

CHOOSE SERVERS CAREFULLY

Advise your child to only enter servers with people they know and trust to protect them from engaging in conversation with strangers. Your child can also create their own multi-player server and share this with their friends to join in which is safer and more controlled than joining a stranger's server.

Sources:
<https://minecraft.net/en-us/article/minecraft-multiplayer-server-safety>
<http://parentinfo.org/article/staying-safe-on-minecraft>
<https://www.bbc.co.uk/news/uk-wales-38284216>
<https://support.xbox.com/en-GB/xbox-one/security/cannot-change-my-privacy-settings-1>
<https://lifehacker.com/a-parent-s-guide-to-playing-minecraft-with-your-kids-1788022798>

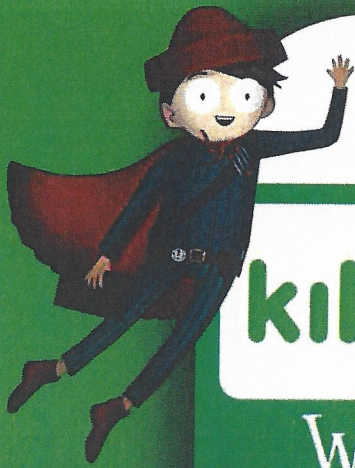
<https://www.mirror.co.uk/tech/new-minecraft-game-needs-caution-11251242>
<https://www.mirror.co.uk/news/uk-news/ paedophiles-using-online-computer-games-1023355>
<https://leahnieman.com/4-fabulous-family-friendly-minecraft-servers/>
<https://www.howtogeek.com/289985/how-to-set-up-minecraft-so-your-kids-can-play-online-with-friends/http://minemum.com/chat-setting>

THIS IS AN INDEPENDENT ONLINE SAFETY GUIDE AND IS NOT AN OFFICIAL MINECRAFT PRODUCT. THIS GUIDE HAS NOT BEEN APPROVED BY NOR IS IT ASSOCIATED WITH MOJANG

© National Online Safety Ltd

This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

www.nationalonlinesafety.com



kik

Kik (or Kik Messenger) is a free messaging app used by 300 million people worldwide that lets users exchange messages, photos, videos, GIFs and webpages via a Wi-Fi connection or data plan. Kik is unusual in that your child can sign up without a phone number and then find and message other people via just their username. Kik is aimed at anyone aged 13 years and older – the app says teens between 13 and 18 years old will need parental permission but it does not verify ages.

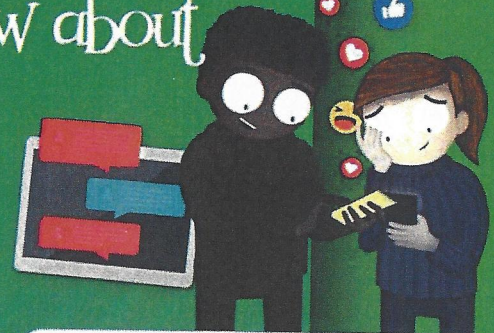


AGE RESTRICTION
13+

1 new message

What parents need to know about

Kik



CHILD SEXUAL EXPLOITATION & GROOMING

Police in the UK have warned that Kik has featured in more than 1,100 child sexual abuse cases in the last five 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 sex 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.

FAKE OR ANONYMOUS PROFILES

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 Wi-Fi instead. By using a username, your child can avoid sharing personal information with others on Kik, but on the flipside, this makes it far easier for people to remain anonymous or to create a fake persona.

SEXUAL PREDATORS

Some people may use Kik with the intention of targeting children. Typically, this is a subtle and a potentially dangerous individual who will initially portray themselves as a friend who 'understands' a child. They may also lie about their age and it's possible that your child could be manipulated by a stranger into doing regrettable or illegal activities, and maybe even meeting them in real life.

JOINING PUBLIC GROUPS

As soon as Kik is downloaded, your child can join public groups to chat with up to 49 others about anything from music to sports to travel by searching for topics they are interested in. However, groups can include inappropriate names and content. There are also private groups on Kik that can be joined by scanning a group Kik code or if they're added by someone on their contact list.



SEXTING

Due to the general ease of sharing photos and videos, sexting has been reported on the app. These messages can be screen-captured or copied at the press of a button, which could lead to further dangers, such as blackmail and cyberbullying. It is illegal to make, possess, download, store and share sexual images, photos and videos of a person under the age of 18. This also includes any sexual images, photos and videos that a child may have taken of themselves.

KIK 'BOTS'

Users can add 'bots' to their friends list and communicate with them on the app. 'Bots' are automated software programs built into the app that mimic conversation – developers, brands and Kik can create 'bots' to communicate with any Kik user who has opted to start a conversation with them. Kik has been associated with 'pornbots' and 'spambots', which try to lure users into clicking on links or porn websites by using suggestive and often personalised messages.

VIDEO CHAT

Your child can take part in a live video chat with their friends in a one-to-one chat, or with up to six friends at a time in a private group chat. There is the danger that conversations can be recorded and shared without their knowledge, and with live video conversations, your child is at risk of seeing or hearing content that is inappropriate, sexual or violent.

PERSONAL OR COMPROMISING USERNAMES

As Kik works with usernames and not phone numbers, some people may search for clues as to who someone is in real life, based on their name. For example, if your child uses their real name or something similar, strangers could potentially find out their identity and even start looking for them on other social media platforms.



Top Tips for Parents

1 new message

CHOOSING A USERNAME

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 or last name. Get them to choose a username that is hard to guess, using a combination of letters and numbers.

SHARING USERNAMES

Explain to your child that sharing usernames on social media channels, such as Twitter, Instagram or Facebook, will make it visible to people they might not know – and they'll be able to message your child. If your child joins a group, anyone within that group will be able to see their username. Your teen will have a Kik Code that's unique to them and lets your child connect with anyone that scans the unique code. Encourage your child not to share their Kik Code with anyone they don't trust.

DEACTIVATING ACCOUNTS

If your child is under 13, you can submit a deactivation request to Kik by emailing support@kik.com. Use the subject line 'Parent Inquiry' and include your child's Kik username and age in your message. If your child is over 13 and you want to close their account, you will need access to the email address registered to their account before you visit <https://ws.kik.com/deactivate>.

FIND GENUINE FRIENDS

The Kik app includes an optional feature that your child can turn on to help find real friends on Kik. The feature works by checking for accounts in Kik that match an email address or phone number stored in contacts (on a smartphone). If the app finds a match, it will notify both your child and their friend with a Kik message.

SHOW HOW TO BLOCK & REPORT

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've been blocked. The blocked user's name will no longer appear in contacts in Kik. Your child can also report a group if they think it's 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 spam bots have been created 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 the chat from the conversation list. If conversations are saved, Kik will automatically block the spam account but save the chat history.

DON'T TALK TO STRANGERS

If your child knows not to talk to anyone they don't know in real life, the risks of using Kik are drastically lowered. Alternatively, if any stranger happens to send your child a message, teach them to ignore it.

COMMUNICATION IS KEY

If your child sees something disturbing, pornographic, deviant or otherwise troubling, they may be left confused and in need of somebody to explain it to them. As such, tell your child that you are always there to help them if they need it, and if they start acting differently to normal, calmly ask them why.

AVOIDING UNEXPECTED IMAGES

Kik censors images from strangers to limit lewd content being shared by surprise. The app will blur all photos in messages when users who have never interacted before contact each other for the first time. Users can only share unblurred images after they have both approved each other.

USING A VALID EMAIL

According to Kik, it is really important for users to provide a valid and accessible email address when registering their account. This will help to make sure your child is able to receive important emails from the service, such as a link to reset their password, when they need them.

MUTING OR LEAVING A CHAT

If someone has said something inappropriate to your child through Video Chat, they can mute the user or leave the Video Chat. Tap on the person's Video Chat bubble and a mute icon will appear. When a child mutes themselves, their microphone will be disabled and nobody else in the chat will be able to hear them.

1 new message

SOURCES:
<https://www.teensafe.com/blog/everything-a-parent-needs-to-know-about-kik>
<https://help.kik.com/en-us/articles/11500689388-Keep-your-Kik-account-private>
<https://www.bbc.co.uk/news/uk-45368276>



1 new message



National
Online
Safety

A whole school community approach to online safety
www.nationalonlinesafety.com

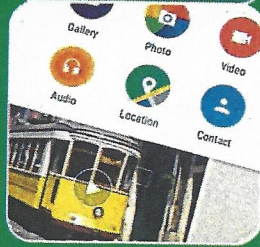
Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061



WhatsApp is one of the most popular messaging apps in the world, with more than 1.5 billion people in more than 180 countries using it to send and receive text, photos, videos and documents, as well as make voice and video calls through an Internet or Wi-Fi connection. The free app offers end-to-end encryption, which means that messages can only be read by the sender and the recipient in one-to-one chats, or all members if it is a group chat. Not even WhatsApp can read them.



AGE RESTRICTION
16+



What parents need to know about

WhatsApp



AGE LIMIT CHANGE

Since May 2018, the minimum age for using WhatsApp is 16 years old if you live in the European Union, including the UK. Prior to this, the minimum age was 13, which still applies for the rest of the world. WhatsApp has not yet stated whether it will take action against anyone aged between 13 and 16 who already hold accounts under the old terms and conditions, such as closing their account or seeking parental permission.

SCAM MESSAGES

Occasionally on WhatsApp, people receive spam messages from unauthorised third parties or from fraudsters pretending to offer prizes to 'lucky people', encouraging recipients to click on a link to win a prize. A common scam involves messages warning recipients that their WhatsApp subscription has run out with the hope that people are duped into providing their payment details. Other scam messages include instructions to forward the message in return for a reward or gift from WhatsApp or another person.

FAKE NEWS AND HOAXES

WhatsApp has been linked to enabling the spread of dangerous viral rumours. In India, for example, a number of attacks appear to have been sparked by false rumours shared on WhatsApp.

THE 'ONLY ADMIN' FEATURE AND CYBERBULLYING

Cyberbullying is the act of sending threatening or taunting text messages, voice messages, pictures and videos, with the aim to hurt and humiliate the receiver. The group chat and group video call features are great for multiple people to chat simultaneously, but there is the potential for people to hurt others with their comments or jokes. The 'only admin' feature gives the admin of a group chat greater control over who can send messages. Whilst this can be good for one-way announcements, the group admin has the power to block somebody from responding to an offensive message in a chat, which could result in a child being upset and unable to reply.

CONNECTING WITH STRANGERS

To start a chat in WhatsApp, you need to know the mobile number of the contact you want to speak to and they also need to have the app downloaded. WhatsApp can find contacts by accessing the address book of a device and recognising which of those contacts are using WhatsApp. If your child has shared their mobile number with somebody they don't know, they can use it to get in touch via WhatsApp.

LIVE LOCATION SHARING

WhatsApp's 'Live Location' feature enables users to share their current location in real time to their contacts in a chat, allowing friends to show their movements. The feature, which can be found by pressing the 'attach' button, is described by WhatsApp as a 'simple and secure way to let people know where you are'. Location-sharing is already a common feature on other social apps, including Snapchat's Snap Map and Facebook Messenger and can be a useful way for a child to let loved ones know they are safe. However, if your child is in a group chat with people they do not know, they will be exposing their location.



National Online Safety

Top Tips for Parents



CREATE A SAFE PROFILE

Even though somebody would need your child's phone number to add them as a contact, as an extra security measure we suggest altering their profile settings to control who can see their profile photo and status. The options to choose from are 'Everyone', 'My Contacts' and 'Nobody'. We suggest selecting 'My Contacts' or 'Nobody' to ensure their profile is protected.

EXPLAIN HOW TO BLOCK PEOPLE

If your child has received spam or offensive messages, calls or attachments from a contact, they should block them. Messages and status updates sent by a blocked contact will not show up on the phone and will stay undelivered. Blocking someone will not remove this contact from the contact list - they will need to be removed from the phone's address book. To block a contact, your child needs to open the person's chat stream and tap on the settings.



REPORT SCAM MESSAGES

Advise your child not to tap, share or forward any message that looks suspicious or sounds too good to be true. When your child receives a message from an unknown number for the first time, they will be given the option to report the number as spam directly inside the chat. They can also report a contact or a group as spam using the following steps: 1) Open the chat. 2) Tap on the contact or group name to open their profile information. 3) Scroll to the bottom and tap 'Report Spam'.

LEAVE A GROUP

If your child is part of a group that makes them feel uncomfortable or has been added to a group they don't want to be part of, use the group's settings to show them how to leave. If someone exits a group, the admin can add them back in once. If they leave again, they cannot be added again.

USING LIVE LOCATION SAFELY

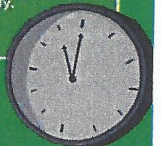
If your child needs to use the 'Live Location' feature to share with you or a friend, advise them to only share it for the amount of time they need to. WhatsApp gives the options of either 15 minutes, one hour or eight hours. However, your child can choose to stop sharing at any time.

DELETE ACCIDENTAL MESSAGES

If your child has sent a message to the wrong chat or if a message they sent has contained a mistake, they can delete it. To do this, simply tap and hold on the message, choose 'Delete' and then 'Delete for everyone'. The app allows seven minutes to delete the message after it has been sent, but it is important to remember that recipients may have seen and screenshot a message before it was deleted.

SET TIME LIMITS

A 2017 study found that by the age of 14 the average child will have sent more than 35,000 texts, 30,000 WhatsApp messages and racked up more than three solid weeks of video chat. Although it is inevitable that your child will use technology, you can still set boundaries. This is not easy, especially since teens use their devices for both schoolwork and free time, often simultaneously.



AGE RESTRICTION
13+
with parental permission

What parents need to know

Twitch

Twitch is a gaming-focussed live-streaming service, owned by Amazon, where you can watch others play games live and listen to commentary as they play. It has 15 million daily active users and more than three million people live-broadcast video game streams and other content on Twitch, with channels dedicated to just about every popular video game imaginable – both modern and retro. There are also shows that feature gaming competitions, professional tournaments, game-related chat and news. Plus, numerous non-gaming channels covering everything from cooking and music to art and travel. But Twitch is not just about watching other people's shows – anyone can broadcast their own gaming action.



Top Tips for Parents

THE RISK - IT'S LIVE & UNCENSORED
As gamers get engrossed in their games, it is very common to hear rather choice words, so the chance of your child encountering swear words and bad language is extremely high. There is not only the language of the person running the stream that you need to consider, but also the language of other Twitch users in the text-based chat that accompanies streams.

What parents can do

There's not much you can do to reduce exposure to bad language on Twitch, but if there are any troublesome users, it is possible to block them. It is a good idea to spend a little time with your child as they explore different channels on the platform, as this will give you an idea of the sort of content they are being exposed to. As Twitch does not offer any parental control options, this is the best way to police what your child is doing. If your child is overwhelmed or disturbed by comments that are being posted in the stream chat, it is possible to hide it from view by clicking the little arrow to the right of the Subscribe button.

THE RISK - VIOLENT GAMES & ADULT CONTENT
Like so many websites, Twitch does not allow children under the age of 13 to create an account, but in practice, there's nothing to stop anyone signing up by simply entering a false date of birth. In addition to swearing, commentary provided by other Twitch users may well contain adult content, and the games themselves can be rather violent. Bear in mind that many of the games on the market these days have an age rating of 18, and this is indicative of the bad language, sexual content and violence that they may contain.

What parents can do

There is nothing that can be done to prevent your child from accessing whatever channel they want – short of using your router settings or parental control software to block access to the site completely. One of the problems with Twitch is that while there is plenty of child-friendly content out there, it is not at all easy to quickly identify what might not be suitable. Spend some time working with your child to help identify channels that will be appropriate for them. While it may be hard to ensure they stick to these channels, it is useful for them to know that there is content available that is not overtly adult in nature.

THE RISK - POTENTIAL COSTS
By default, Twitch is ad-supported, but there is a monthly subscription option – called Twitch Turbo – that offers an ad-free experience. On top of this, it is possible to subscribe to individual channels, and each one is chargeable individually. There's also Twitch Prime, a premium experience included with the Amazon Prime and Prime video subscription memberships, which offers bonus games and exclusive in-game content and Twitch Merch – an online store offering merchandise, such as T-shirts and hoodies. Twitch Bits is a virtual currency that gives your child the power to encourage and show support for streamers – through 'cheers' – and get attention in chat through animated emoticons. Bits cost real money and there's one option to buy 25,000 Bits for £2.88. It's easy to see how costs could very quickly mount up the more involved your child gets into Twitch.

What parents can do

Take steps to restrict access to your credit/debit card, as well as your PayPal account, to avoid getting hit by a large bill. If you are able to access your child's Twitch account, it is possible to check their purchase history, so you can see if they are spending too much money on subscriptions or donations. Explain to your child that subscribing to channels and purchasing Bits for cheers is optional, and that they can watch and enjoy a stream without doing either.

THE RISK - UNWANTED CONTACT FROM OTHER USERS

Just like any website or platform with a social element to it, there is the risk that your child will not only come into contact with the sort of people you might rather they didn't, but also that they could be harassed, groomed or bullied online.

What parents can do

Within Twitch settings, in the Security and Privacy section, it is possible to block messages – known as 'whispers' – from strangers. It's worth noting that this option only blocks messages by those who are not your friend, someone you follow, someone you subscribe to, one of your mods, or one of your editors. Taking things further, it is possible to completely block users who become problematic. Show your child how to make use of this option by clicking on a user's name and in the little pop-up that appears, click the icon that looks like a little speech bubble to block them. If your child wishes to report the user to Twitch, click the three dots button beneath the block option and click Report.

THE RISK - WEBCAM SHARING

As well as seeing streaming footage of games, Twitch also lets users share their webcam, so people can see them. This gives yet another way for people to share inappropriate content, and it also gives another way for streamers to subject your child to advertising, sponsored content and product placement.

What parents can do

Getting involved in your child's use of Twitch is the best way to keep an eye on the sort of content they are consuming and intervene if anything inappropriate crops up. As part of your conversations with your child about what is appropriate to share online, try to educate them about careful use of their own webcams if they choose to stream their own gaming. As well as ensuring they are not encouraged into doing anything inappropriate on camera, it is also important to check that anything that can be used to identify them is not included in shot.

THE RISK - TWITCH EMOTES

Twitch's interactive chat feature is littered with emoticons or 'emotes', which for first time users will be completely bewildering. They typically feature faces of notable streamers, Twitch employees or fictional characters, such as a grey-scale photograph of a game developer known as Kappa, which is often used in Twitch chat as a symbol of sarcasm or mockery. Your child may be upset or sensitive if they are the target of negative emotes while chatting with other gamers, or they may find some emoticons offensive.

What parents can do

Chat to your child about how they use Twitch and show an interest in understanding how it works. There are lots of online guides to Twitch emotes if you really want to get clued up on what your child is talking about in chats. Twitch's Terms of Service dictate that emotes must not be used for harassment – defined by targeted insults, defamation, intimidation, and threats of any nature. If your child finds an emote that violates guidelines, they can report it via the 'User Report' tool. Channel owners can also add specific emotes to their 'Channel Banned Words' list.

SOURCES:
<https://www.twitch.tv>



National Online Safety

A whole school community approach to online safety
www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061