**natterhub**
preparing children to thrive online

# Complete Online Safety Guide for Key Stage2

## Contents

# Introduction

Whether we like it or not, screens are integral part of everyone's daily lives - including those of our children.

Some of the statistics can seem worrying. According to research carried out by Ofcom in 2019, 9 out of 10 primary school aged children regularly use a device to go online. A quarter of children have at least one social media profile by the age of 10, with the most popular apps including WhatsApp, Facebook, Snapchat and Instagram. These sites can also bring with them the risk of pressure from social peers, or the possibility of being contacted by strangers, though virtual bullying is not as prevalent for many as face-to-face incidents.

It's no wonder that only 55% of parents who were asked said that the benefits of being online outweighed the risks. But we at Natterhub want to change that!

## What is Natterhub?

Natterhub is a safe social media platform that teachers can use to teach children how to thrive online. It features easy-to-follow, age-appropriate lessons, and high-quality resources like online activities, news reports and even fitness videos - all designed to align with the updated compulsory PSHE and RSE National Curriculum.

Natterhub is a gated and transparent community. There are no private chats, so everyone can see what's happening at all times, and teachers access tools to make sure that children can't access the platform without supervision.

However, we also know that children are exposed to screens and the digital world outside of the classroom, and that every day is a learning experience. That's why we've put together this handy guide!

In these pages you'll find easy-to-follow explanations of the tools and platforms that children use every single day, as well as tips for dealing with some of the most common problems that they pose.

# Screen Time

**How much is 'too much' screen time?**

Screens offer children a wealth of information and opportunities for creativity. But like anything else, too much screen time can have a negative effect on their physical and mental health.

We know that watching too much TV doesn't actually make your eyes go square, but the debate of 'how much screen time is too much' has raged on for years. In truth, there's no such thing as a healthy amount of screen use - what's important is the way that you're using screens.

## 'Active' and 'passive' screen time

The most helpful way to think about your screen time is to split it between **active** and **passive** screen time. But what's the difference?

**Active screen time** is anything that engages your brain while you're looking at a screen. Doing school work, playing certain video games (especially games like Minecraft that inspire creativity) and reading books on an e-reader are all good examples of active screen time.

**Passive screen time**, on the other hand, is the kind of activity that involves shutting your brain off. This includes playing mobile games like *Candy Crush* that are designed to be addictive, scrolling through your social media feeds for what feels like hours, or watching TV.

Passive screen time is not inherently evil - there's nothing wrong with children watching educational TV shows, or even cartoons, every now and again. You just need to strike the ideal balance between active and passive screen time, making sure they get more of the former and less of the latter.

## Screens and sleep

Electronic devices can seriously throw off your body's **circadian rhythm**, the natural process by which your body decides when it's time to fall asleep and when to wake up. This is because smartphones, tablets and TVs emit **blue light**, which tells your body to stop producing **melatonin** - the chemical that makes you start to feel sleepy when the sun goes down.

Many devices now feature a **'Night Mode'** that can be set to turn on automatically at a certain time of day. This shifts the screen to emit a warmer red light that's less disruptive to your body's natural rhythms. However, the best way to get ready for bed is still to stop using your devices altogether. Make sure you turn them off at least an hour before you want to go to sleep, and keep them out of the bedroom if you can avoid it - that way, you won't be tempted to pick up your phone and start scrolling in the middle of the night!

## How to achieve the right balance

As children move into Key Stage 2, they will start to use screens more actively to help them with school work, as well as seeking out more passive screen time for relaxation. It's important at this stage to get them thinking about balancing their screen use effectively:

- Sit down with your children to discuss the impact of screens on their health, and agree on limits for passive screen time throughout the day.

- Take an active interest in the ways that your children use screens. Healthy discussions of the games they play and websites they use will help prepare them to deal with risks they may face online (see the **Common Issues** section for more detailed information.

- Encourage children to prioritise time spent with family or on creative pursuits, and emphasise the importance of turning screens off at the end of the day to get a good night's sleep.

- Work with your children to set parental controls on devices and social networks that they regularly use (see the **Know Your Stuff** section for

instructions on different devices and platforms).

- Set a good example! Children will mimic your behaviour when it comes to screens, so be aware of your own bad habits.

# Know Your Stuff

The best thing that you can do to make sure your children stay safe online is to familiarise yourself with the apps, social media platforms and devices that they use on a regular basis. That way you can have productive discussions with your children and, better still, make sure they aren't accessing anything that they shouldn't.

But don't worry if you don't know your Instagram from your elbow or think a Wii is something polite people don't discuss in public. We've put together a quick and easy guide to help you get to grips with everything!

## Social Networks

### Facebook

Facebook has over 2 billion users across the globe, and is available on all devices from your desktop and laptop to smartphones and tablets. Users can add photos and videos, update their status, interact with others and catch up with the latest news. Facebook requires users to be 13 and up, but there are no age verification measures and children can easily create an account.

Facebook can be highly addictive, giving users a Fear of Missing Out (FOMO) that encourages them to use it regularly. Its private messaging functions can lead to instances of **cyberbullying** or even **grooming** from anonymous users, and there are lots of opportunities for targeted advertising that could be seen by impressionable children.

Facebook features a handy 'Privacy Check-up', which allows you to decide who can see your child's personal information, including their email address and phone number.

1. Go to the **Settings** menu and select **Privacy Shortcuts**.
2. Click on the padlock symbol that says 'Review a few important publicity settings'.

3. Follow the step-by-step instructions for four different topics.

**Twitter**

Twitter users can publicly post tweets - short messages of up to 280 characters - as well as photos and videos. They can also share tweets written by others to their followers, and send direct messages to other users.

Twitter is great for keeping up with current trends and what's happening in the news, but it also contains a lot of content that might be inappropriate for your children. Tweets are added very quickly, which makes it easy for fake news to spread, and also allows more extremist views to be aired publicly.

Here's how you can protect a Twitter profile and make it more secure:

1. Click on your profile picture to open the menu.
2. Go to **Settings and privacy.**
3. Tap **Privacy and safety.**
4. Make sure **Protect your Tweets** is enabled to make sure only approved users can see what you tweet.
5. Untick **Receive message requests** to avoid getting direct messages from strangers.

**WhatsApp**

WhatsApp is one of the most popular messaging apps in the world. Users with a WiFi or mobile data connection can send and receive text, photos, videos and documents, as well as make voice and video calls. The app also offers end-to-end encryption, which means that messages can only be read by people included in a chat. Not even WhatsApp can read them. ~

You need to know a user's phone number in order to connect with them on WhatsApp, but it is still possible to receive spam messages from third parties. The app also includes a 'Live Location' feature, which allows users to share their geographical location in real time.

Here's how you can protect a WhatsApp profile and make it more secure:

1. Go to **Settings** in the top-right corner of the app.
2. Tap **Account** > **Privacy**
3. Make sure your **Live Location** is turned off.
4. Go to **Blocked Contacts** and tap the + icon to block unwanted contacts.

## Snapchat

Snapchat is a photo sharing app for mobile phones and tablets. The app allows users to share images for a limited number of seconds, chat with users before messages disappear, and share images with their friends list through a 'story'.

Snapchat also features a number of 'filters' which can create amusing images and videos. On the other hand, some 'beauty filters' can also lead to low body image and feelings of inadequacy among children.

The app also shares users' geographical information, and the fact that images disappear after a time limit means that many children can use it to send sexually explicit images. However, these images can still be screenshotted or recorded.

Here's how you can protect a Snapchat profile and make it more secure:

1. Tap the gear icon on the right side of your profile screen.
2. Go to the **Who Can...** section to change privacy settings.
3. Make sure the **Contact Me** and **View My Stories** options are set to **'My Friends'**.
4. Enable **'Ghost Mode'** to make sure nobody can view your location.
5. Untick 'Let other people find me' to protect your profile from strangers.

## Telegram

Telegram has no privacy controls. It is designed to allow users to connect easily with strangers, and send hidden messages (including images) that can be deleted from devices using a **self-destruct** timer. However, messages can still be forwarded to other users, and users can also share offensive or inappropriate material. .

Facebook requires users to be 13 and up, but there are no age verification measures and children can easily create an account. Because of this, we recommend making sure that your children do not have access to Telegram.

**Instagram**

Instagram is a photo sharing app that allows users to share images and video. It includes a live streaming feature, and add-ons such as 'Boomerang', 'Hyperlapse' and 'Layout', which can be used to enhance their feed. Users can choose to add filters and make adjustments to their photos, and include hashtags in their uploads to make them easier to find.

While Instagram is great for sharing amazing photos, there are some issues to consider. As with Snapchat, the use of filters can create feelings of low self-esteem and inadequacy in some children, while the addictive nature of scrolling can get children hooked on the app. Users can send direct messages (DMs) to anybody, even if that person isn't in their friends list, and posts can include details of a user's geographical location. It's also worth noting that Instagram features a lot of advertising, particularly from 'influencers' who can be paid large sums of money to promote goods and services on the platform.

Here's how you can protect an Instagram profile and make it more secure:

1. Go to **Settings** > **Privacy** > **Account Privacy** and set the switch to on. This means that only people who follow you can see your photos and videos, and anyone who wants to follow you must get your approval first.
2. Make sure Instagram's anti-bullying filter is active, to hide any comments relating to a person's appearance or threats against another user (this should be turned on by default).
3. Turn off sharing so that other users can't spread your posts without permission, and make sure that Instagram isn't connected to other social networks your child uses.

**TikTok**

TikTok lets users create, share, and view user-created videos. Users can record and upload bite-sized looping videos of themselves lip-syncing and dancing to popular music or soundbites, often for comedic effect, which can then be further enhanced with filters, emojis and stickers.

TikTok has been designed with young users in mind, but it's also likely that children scrolling through the app will come across videos with inappropriate music, or suggestive or sexual behaviour. It's easy to connect with other users on TikTok, which also makes it a popular site for predators. Additionally, the app also features a currency called 'TikTok coins', which are used to buy new emojis and can be purchased for real money.

If you set your TikTok account to private, users won't be able to see your videos unless you give them permission to follow you.

1. Go to the menu in the top-right corner of your profile page and select **Privacy and Settings**.
2. Select **Privacy and Safety** and make sure that **Private Account** is set to 'on'.

You can also use the app's **Digital Wellbeing** settings to block inappropriate content with **Restricted Mode**, as well as setting a limit on the amount of time children can use the app in a day and disabling the option to buy TikTok coins.

**Houseparty**

Houseparty is a live streaming app described as a face-to-face social network where people 'drop in' on each other to video chat, leave messages and hang out in groups. Children under the age of 13 must have a parent's permission to access the services, but no proof of age is required to create an account.

While Houseparty is great for helping children stay in touch with their friends, particularly during the current COVID-19 epidemic, it could be used to bully some vulnerable children by excluding them from hangouts. It also creates opportunities for children to come into contact with strangers - by default, Houseparty allows anybody to enter any conversation that they want, which can also leave the door open for sharing inappropriate content.

However, there are two easy ways to prevent this from happening:

1. Once you're in a 'room', you can tap the **Lock** icon at the bottom of the screen to secure that room.
2. Go to **Settings** (the cog icon at the top left), then tap **Private Mode** to make sure every room you enter is locked by default.

You can also disable location sharing in the **Options** menu - this allows you to find people on the app that are close to your geographical location.

**Zoom**

Zoom is a video conferencing service that has quickly gained popularity in the wake of the COVID-19 epidemic. Users can start their own meetings, or they can join meetings set up by others provided they have a link or meeting ID. It can be downloaded as an app for iOS and Android, or accessed via the web browser of any computer or tablet.

Because anyone can join a Zoom chat as long as they have the link for it, there's been a rise in cases of 'Zoom bombing' - users dropping into other people's conversations. While this can be harmless, there have also been reports of people shouting abusive language or sharing inappropriate images.

There are also some privacy concerns surrounding Zoom: hosts can record meetings, meaning images or videos of your child may be shared without permission, and the app can also store user information like names, phone numbers or geographical location.

Here are some easy methods for making Zoom more secure:

1. Generate random IDs for each Zoom meeting to make them more secure.
2. Go to **Account Management** > **Account Settings** and click **Waiting Room** - this means that you can see new people trying to join a meeting and decide whether to let them in.
3. Click the **Participants** button in your Zoom window and select **Lock Meeting** to prevent people from joining, even if they have the link.

**Skype**

Skype is a video service owned by Microsoft which allows users to take part in video chats or stay in touch via instant messaging.
You can only start chatting with a user once they've accepted your invitation to chat, but users can in theory send requests to anybody as long as they search for the right name. Be sure to talk to your child about not accepting requests or talking online to strangers.

Skype uses a series of features to protect children who use the platform*. You can only find a child's profile if you search for their exact Skype name or email address. Information like their age or date of birth is hidden from view, and only people in their contact list can get in touch with them via messages or video chats.

*Please note: Microsoft accounts automatically remove all restrictions if the user is 18 years old. Make sure your children are using an age-appropriate account for parental controls to apply.*

## Smartphones & Tablets

### iOS (iPhone/iPad)

1. Go to **Settings** and tap **Screen Time**.
2. Tap Continue, then choose '**This is My [device]'** or **'This is My Child's [device]'**.
3. If you're the parent or guardian on your device and want to prevent another family member from changing your settings, tap **Use Screen Time Passcode** to create a passcode, then re-enter the passcode to confirm.
4. If you're setting up Screen Time on your child's device, follow the prompts until you get to **Parent Passcode** and enter a passcode. Re-enter the passcode to confirm. In iOS 13.4 and later, after you confirm your passcode, you'll be asked to enter your Apple ID and password. This can be used to reset your Screen Time passcode if you forget it.
5. Tap **Content & Privacy Restrictions**. If asked, enter your passcode, then turn on **Content & Privacy**.

6. Make sure you choose a passcode that's different from the passcode you use to unlock your device. To change or turn off the passcode on your child's device, tap **Settings** > **Screen Time** > **[your child's name]**. Then tap **Change Screen Time Passcode** or **Turn Off Screen Time Passcode** and authenticate the change with Face ID, Touch ID or your device passcode.

Once you've done this, you can restrict access to certain apps and functions on your device, as well as setting limits on data usage, online payments and screen time.

**Android**

1. On the device on which you want parental controls, open the **Play Store** app.
2. In the top-left corner, tap **Menu** > **Settings** > **Parental Controls**.
3. Turn on **Parental Controls**.
4. Create a PIN. This prevents people who don't know the PIN from changing your parental control settings. If you're setting up parental controls on your child's device, choose a PIN that they don't already know.
5. Tap the type of content that you want to filter.
6. Choose how to filter or restrict access.
7. Once you set up parental controls, you can turn them on or off. When you turn them back on and create a new PIN, your old settings will come back. This helps you share a device with people who don't need parental controls.

## Games Consoles/Platforms

**Sony (PS4, PS3, PlayStation Network)**

1. Go to **Settings** > **Parental Controls/Family Management.**
2. Select **System Restrictions**. You will be prompted to enter the default passcode before changing to a new one.
3. Select the child user you want to apply Parental Controls to.

Once you've done this, you can filter content via age, restrict access to the PlayStation's browser, set spending limits for the account and more.

**Microsoft (PC, Xbox)**

1. Go to **Settings** > **Family** and select your child's account in order to manage it*.
2. Go to **Privacy & Online Safety**, **Access to Content**, or **Web Filtering** in order to view different options.
3. Alternatively, you can choose either **Child Defaults**, **Teen Defaults**, or **Adult Defaults** to

*Please note: Microsoft accounts automatically remove all restrictions if the user is 18 years old. Make sure your children are using an age-appropriate account for parental controls to apply.*

**Nintendo**

**3DS / Wii / Wii U:** Select Parental Controls from the Settings menu, enter a four-digit PIN, and then choose your restrictions for the Internet browser, age ratings on games, or purchases on the Nintendo eShop.

**Switch:** Download the free **Nintendo Switch Parental Controls app** for iOS or Android. You can use this to restrict access to games based on their age rating, set time limits for play and even put the console into sleep mode remotely at a certain time of day. You can also find these settings in the **System Settings** menu on the console itself.

**Steam**

1. Login to Steam with the account your child will use.
2. Click the **Steam Menu** in the top, and open **Settings**.
3. Go to the **Family** tab that opens on the left side of the window.
4. Click **Family View** to start the wizard.
5. Follow the on-screen instructions through each step of the wizard. This allows you to choose the content and features you want the child to be able to access with their account.
6. Select and confirm your new PIN.

## Streaming Services

### Netflix

1. Log in, click on your profile icon, then click **Account**.
2. Scroll down to **Settings**.
3. Click on **Parental Controls**.
4. Enter your Netflix password.
5. Create a PIN.
6. Scroll to **Restrict by Maturity Level** and click on the bubble above your kid's age group: Little Kids (6 and Under), Older Kids (12 and Under), Teens (14 and Under), or Adults (15+).
7. You can also restrict all content so nothing will play without you entering a PIN. To do this, click the bubble above **Little Kids**.
8. If you want to restrict specific titles, regardless of their maturity rating, type them into the box under **Restrict Specific Titles**.

### Amazon Prime

- On a PC or Mac, go to **Prime Video Settings** > **Parental Controls**.
- On the Prime Video app for iOS or Android, select **My Stuff** from the bottom menu, then select the **Settings** icon. From there, select **Parental Controls**, then **Viewing Restrictions**.
- Select an age restriction and the Devices you want them to apply to, then click Save.

  *Note: Restrictions only apply to the device they were set up for.*

### Disney+

1. When logged into your Disney+ account from any device, tap on the current profile name.
2. Select **Edit Profiles**.
3. Choose **Add Profile**.
4. Next, select an image for the new profile.
5. Type in a Profile Name.
6. Toggle **Kids Profile** to **On** (this disallows PG and 12A content for the profile).

## Twitch

1. Log in to your Twitch account using your email address and password. If you haven't got an account click the **Sign Up** button.
2. Choose a PIN code to ensure that your child cannot change your chosen settings. You will be asked to enter the PIN twice to confirm.
3. Once logged in, select the drop-down menu at the top right corner of the browser and select 'settings'
4. Use the **Security & Privacy** tab to block messages from strangers.
5. Use the **Channel & Videos** tab to moderate content that appears in the chat.

## BBC iPlayer (CBBC)

BBC iPlayer uses **Guidance Labels** to warn users of any inappropriate content. You can set up a **Parental Guidance Lock** to require a PIN number whenever children try to watch something with a Guidance Label. Simply go to Settings > Parental Guidance on your phone or TV app, and choose your PIN.

## Now TV

1. Go to the **Settings & PINs** area of **My Account** on the Now TV website.
2. Select **Set Up Parental PIN**.
3. Enter your PIN, confirm your password and click **Save PIN.**
4. All certificates will be selected as your default age rating. To choose a different rating, just select **Change Settings**.

## YouTube

Go to Settings and click **Enable Restricted Mode** to filter out videos that have been flagged as having inappropriate content and disable comments on videos.

## YouTube Kids

1. Tap the **Lock** icon in the bottom corner of any page in the app.

2. Complete the multiplication problem or read and enter the numbers that appear. Or, enter your custom passcode.
3. Select **Settings**.

Here you can block or approve content for your child to watch, or choose from age-appropriate filters to sort content automatically. You can also disable the search option.

## Search Engines

Both **Google** and **Bing** feature SafeSearch options. Simply go to the **Settings** option on your preferred search engine to turn it on and filter out inappropriate search results. Bing also gives you the option to use either a **Moderate** filter (which only applies to images and videos) or a **Strict** filter (for images, videos and text).

## Internet Browsers

### Chrome

The best way to make sure your children are safe while browsing Chrome is to download the **Family Link** app. This will allow you to keep tabs on the websites they visit, approve the apps that they use, and set limits on the amount of time that they use devices. See above for information on Google's **SearchSafe** settings.

### Internet Explorer

1. Open a new Internet Explorer window.
2. Click **Tools** from the dropdown menu bar at the top of the page.
3. Click **Internet Options**, then select the **Content** tab.
4. Look for the heading marked **"Content Advisor"** and click the **'Enable'** button.
5. Use the adjustable 'ratings' sliders to select what types of content are viewable.

**Microsoft Edge**

In order to apply parental controls in Microsoft Edge you need to create a child account. You can do this by following these steps:

1. Open **Windows Settings** and select **Accounts**.
2. Select **Family & Other People** from the left-hand menu.
3. Click on **Add a Family Member.**
4. Select **Add a Child**.

*\*Please note: Microsoft accounts automatically remove all restrictions if the user is 18 years old. Make sure your children are using an age-appropriate account for parental controls to apply.*

**Firefox**

Firefox doesn't feature built-in parental controls. However, if you go to the official Mozilla website and look for Firefox Add-Ons, you'll find a list of parental control add-ons.

**Safari**

*In order to use parental controls on Safari, you need to set up a child account for your children:*

1. Log in to your administrator account on the device.
2. Click **System Preferences**.
3. Click **Users and Groups**.
4. Click the lock icon in order to begin making changes. Enter your password when prompted.
5. Click the + button below the list of users to add a new user.
6. In the New Account drop-down menu, choose **Managed with Parental Control**.
7. Choose the Age:
   - 4+
   - 9+
   - 12+
   - 17+

8. Add the full name of your child.
9. Next, enter an account name.
10. Enter a password.
11. Create a password hint in case your child forgets the password. (If it is forgotten, you can log in to your administrator account and reset the password).
12. Click **Create User**.
13. When finished, click the lock icon again to prevent further changes.

*Once you've done this, you can set parental controls.*

1. Click **System Preferences**.
2. Click **Parental Controls**.
3. Click the lock icon to make changes. Enter your password when prompted.
4. Select the user account whose parental controls you want to manage.
5. Click **Enable Parental Controls**.
6. Choose one of the following options:
   - Allow unrestricted access to websites
   - Try to limit access to adult websites. You can click the Customize button to add a list of sites to always allow, and a list of sites to never allow.
   - Allow access only to these websites. There are a number of websites in this list, including Bing, Google, Facebook, Twitter, and others. Click the + to add another site to the list. Click a site in the list and then the - button to remove a site from the list.
7. When finished, click the lock icon to prevent additional changes.

**Opera**

Opera doesn't feature built-in parental controls. However, you can download an add-on called **Disconnect**, which allows you to block websites and stop third parties from tracking your child's online activities.

# Common Issues

There are so many benefits to the online world, from having a treasure trove of information at your fingertips to forming relationships with people all over the world, but being an active digital citizen comes with some unavoidable risks. Here are some of the most common issues your children may face online, how you can spot them, and what you can do to prevent them.

## Cyberbullying and Trolling

Like regular bullying, cyberbullying and trolling can take many forms. It can include:
- **Threats of violence**
- **Rejection or exclusion from events, games, etc**
- **Impersonation or mimicry**
- **Public embarrassment**

As a parent, try to look out for signs that your child is being bullied online:
- Are they spending less time on the sites and platforms they usually visit?
- Have you noticed any sudden changes in behaviour?
- Do they seem angry or low?
- Are they reluctant to go to school or take part in usual social activities?

At Key Stage 2, your child is developing more complex relationships both on and offline. If you suspect bullying might be occurring:
- **Talk to your child.** Keep calm, and ask open questions to encourage them to open up, even if the incident in question is a mild one. If you respond to the smaller things, they'll come to you with bigger problems.
- If they show you evidence of bullying make sure you **keep a record** in case you need to get the school or other authorities involved.
- Show your child how to **block** or **report** the person doing the bullying.
- Remember that people behave very differently online to the way they behave in real life. If the bullying involves someone that your child knows, it may be possible for them to discuss the behaviour and how it made them feel.

Most importantly, be sure to ask about how your child is doing even **after** the bullying has stopped! They need to feel like they can come back to you if problems arise again.

## Identity Theft

Even though your child doesn't have a bank account, the information that they share online can still be used to steal their identity.

This can take the form of unexplained letters, emails or bills addressed to your child. In the worst cases, this can even affect their credit rating. Because of their age, it can often go unnoticed for many years.

If you're worried your child might be the victim of identity theft:
- Talk to them about the information they share online. **They should not share their full name, date of birth, address or phone number with anybody that they don't know.**
- Make sure your child's devices are all password protected.
- Consider using **ad blockers** to get rid of tempting pop-ups that might be designed to steal information.

Report any suspected identity theft to **ActionFraud**, the UK's national reporting centre for fraud and cybercrime.

## Inappropriate Content

Inappropriate content can take many different forms. It can involve images of a violent or sexual nature, websites that encourage offensive or discriminatory behaviour, or it can be as simple as an advert in a free game that encourages players to spend their own money.

As children in Key Stage 2 take more confident steps online and try to establish their independence, it's more likely that they'll come across inappropriate content. There are a number of ways you can protect your child:
- **Check age ratings!** Video games, apps and even social media sites all have age ratings (usually around 13+). Make sure your child is only looking at

age-appropriate content, and that they don't use social networks without your permission.

- **Talk to your child.** Set ground rules for which sites and platforms are appropriate for your child, and which are off limits.
- **Use parental controls and privacy settings.** Look at the 'Know Your Stuff' section of this guide to make sure that your devices and websites are properly protected.
- **Be honest about what's out there.** You can't protect your child from everything, and sooner or later they'll stumble upon something inappropriate. Discuss openly with children - let them know what to expect, and what they should do when they come across it.
- **Be positive!** This information might sound scary, but don't lose sight of all of the good aspects of being online.

## Sexting & Grooming

**Sexting** refers to the sending and receiving of sexually explicit messages, photos or videos. It's far less common behaviour at a primary level, but it can be part of the process of **grooming** - the term for when people befriend children in order to take advantage of them.

There are many warning signs that many indicate a child is being groomed:
- Spending increasing amounts of time online.
- Being secretive about their online activities.
- Possessing items (like phones or other electronics) you haven't given them.
- Using sexual or explicit language.

Children at Key Stage 2 are often eager to expand their social circle and increase their online following, and will also be more aware of sexual behaviour. Here are some of the things you can do to safeguard your child against grooming:
- **Warn them about the seriousness of sexting.** Sexting is illegal when it involves children under the age of 18. It's extremely unlikely that a child involved would be arrested, but the police will probably want to speak to them.
- **Recognise the role that pressure can play.** Children who are groomed can often feel like they're being pushed into doing something they don't feel comfortable with. Explain to them that despite the pressure, the consequences of sexting can be far worse.

- **Use parental controls and privacy settings.** Look at the 'Know Your Stuff' section of this guide to make sure that your devices and websites are properly protected.
- **Be sensible when it comes to meeting people.** Never allow your child to meet online friends in real life without a parent present.
- **Keep conversation going.** Groomers work by warning children not to tell their parents about their activity, often implying that children may 'get in trouble' if they reveal anything. By maintaining a non-judgemental dialogue, you can encourage your child to be open about their concerns.

If you suspect a child you know is being groomed or abused in any way, you should contact the Child Exploitation and Online Protection Centre (CEOP) and provide detailed information. If you think someone might be in immediate danger, **call the police at once.**

## Radicalisation

Radicalisation is the process by which a person starts to believe in more and more extreme points of view. It can happen online through exposure to extreme propaganda, and if left unchecked it can lead to the radicalised person committing acts of violence in the future. Social networks can allow children to come into contact with extremists and sow the seeds of radical behaviour.

Here are some of the signs you should look out for in your children:

- Being secretive about their online activities.
- Suddenly expressing more extreme views
- Believing that their religion, culture or beliefs are under threat.
- Deciding that violence is the answer to solving problems.
- Searching for a sense of acceptance or belonging.
- Being intolerant towards people of other races, religions or political beliefs.

Children at Key Stage 2, especially those preparing to leave primary school, are likely to be exposed to new ideologies both online and offline. If you suspect your child is being radicalised, consider this advice:

- **Speak _calmly_ with your child.** Becoming angry, confrontational or judgemental will shut down conversation before it can start.
- **Recognise the role that pressure can play.** Children who are radicalised can often feel like they're being pushed into doing something they don't feel comfortable with. Explain to them that despite the pressure, the consequences of following extremists can be far worse.
- **Develop strong counter-arguments.** If you can point out flaws in the logic used by extremist groups, then you can delegitimise their beliefs.
- **Use parental controls and privacy settings.** Look at the **Know Your Stuff** section of this guide to make sure that your devices and websites are properly protected.

## Self-Harm

Self-harm is rarer among primary-age children than teenagers, but it does occur. When most people think of self-harm they think of physical acts, but emotional self-harm is increasingly common. This involves deliberately seeking out online abuse, or even posting negative information about themselves.

Be sure to look for signs of self-harm at home. These include:
- Wearing long-sleeved clothing to hide cuts and bruises.
- Depression, low motivation or low self-esteem.
- Changes in eating habits, as well as sudden changes in weight.

It can be upsetting if you suspect a child is self-harming, which is why it's important to bear these things in mind:
- **Talk _calmly_ to them.** Becoming angry or emotional could simply drive the problem underground. Be open and calm, and encourage your child to talk when they feel comfortable.
- **Try not to be too controlling.** It may be tempting to start issuing rules and ultimatums to your child, but self-harming behaviour is often a method of

exerting control when someone feels powerless. You need to strike a balance between being aware of their issues and giving them space.

- **Use parental controls and privacy settings to try and keep them away from distressing content online.** Look at the **Know Your Stuff** section of this guide to make sure that your devices and websites are properly protected. Bear in mind that these settings won't be 100% effective, but they will help.

If you are worried your child is putting their life at risk by self-harming **call 999**, or take them to A&E if you can.

## Where Can I Get Help?

Some of the issues we've raised in this guide are scary, but you don't need to tackle them alone. There are all sorts of places that can give you help and guidance.

- **Mind** is a mental health charity which includes advice and support for both parents and children.

- **ThinkUKnow** is a website run by the **Child Exploitation and Online Protection Centre (CEOP)**, with detailed advice and resources for parents and children to better understand sexual exploitation and abuse.

- The **NSPCC** website contains helpful guides and advice to deal with a wide range of issues, from abuse and self-harm to general online safety.

- If you're worried about something that's happening at school, speak to your child's teachers.

- If you think that something serious or illegal is happening, don't be afraid to contact the police.

# Gaming

There are lots of benefits to playing video games online. They're a great way for children to spend time with their friends, get lost in a compelling story, or unleash their creativity! But there are also plenty of unique issues linked to online gaming that are worth watching out for. Here are a few tips on how to make sure your kids stay safe and get the most out of their games.

## Popular Games

### Fortnite
Fortnite is a massively popular 'battle royale' game, in which 100 players are dropped into a map and the last one standing is the winner! Though there is violence, it's fairly cartoonish - there is no blood or gore, and players who 'die' simply vanish from the map. We recommend you use your best judgement in deciding if this is suitable for your child.

While Fortnite is free to download and play, it features cosmetic items which are bought using a virtual currency called V-Bucks, although this can be bought using real money (see the **Loot Boxes** section below for more information).

### Apex Legends
Similarly to Fortnite, Apex legends is a 'battle royale' shooter, though players compete in teams of three instead of individually. It also contains items in **loot boxes**, which can be bought using either a virtual currency or with real-world money. However, it's a more violent game than Fortnite, with realistic weapons and blood effects when a player is hit. As a result, Apex Legends has been rated as suitable for players aged 16+.

### FIFA 20
If your children are football fans then you'll know all about FIFA, and every year sees the release of a new edition of their officially licensed game. Players can work through a season of football in 'Story Mode', or play against each other in split-screen or online modes.

Some players can get aggressive in multiplayer modes, but the thing to watch out for with FIFA games is the hidden costs. The Ultimate Team mode allows players to build a dream team of their favourite footballers, some of which can be bought using real money (see the **Loot Boxes** section below for more information). Although there's often little difference between the new editions of the game released every year, children can feel pressured to upgrade to the latest version!

### Animal Crossing: New Horizons

Available on the Nintendo Switch, Animal Crossing is a game about relaxing with friends on a deserted island, and is suitable for young children. Players can visit each other's islands online in order to hang out and share resources, but only if they share a special code or are already friends through the console. Parents who want to limit interaction can use the Nintendo Switch Parental Controls to do so (see the **Know Your Stuff**) guide for more information.

### Minecraft

Minecraft is a hugely popular game that allows players to build amazing worlds out of 3D blocks. While it's generally safe for smaller children to play - there's only mild violence against cartoon monsters like spiders and skeletons - there are still issues to watch out for.

Strangers could theoretically contact children under false pretences, and other players can engage in unkind behaviour like stealing resources or destroying someone's creations. It's also worth noting that many streamers and YouTube stars play Minecraft, which could lead your child to develop a **parasocial relationship** with them (see below).

## Common Issues and How to Deal with Them

## Bullying

Sadly, cyberbullying can be common in online games, as children can forget that the other players are real people whose feelings can be hurt. It can be as simple as banter between friends turning sour, or can be done by people who just want to make others feel bad.

It's important that your child feels comfortable talking to you about bullies they encounter online. Be honest with them; if they know that not everyone they encounter online will be nice, they will find it easier to deal with any incidents that occur. Most online games have methods to report or block users that are being abusive, and you can disable features like online cat to prevent unkind words from getting through. If the bullying is coming from a person that your child knows in real life, like a school friend, suggest your child have a discussion with them about the impact of their behaviour. Many people behave very differently online than they do in real-life situations.

## Interaction with strangers

Online games can allow players from all over the world to interact with each other and even form friendships, but you should be careful about allowing your child to interact with strangers online. Any online game makes it likely that children will encounter either unkind behaviour or inappropriate language, and parents should use their discretion when deciding whether to allow their children to play online.

Your child will want to start expanding their social circle to include people they meet online. Be sure to stress to them the importance of keeping their personal information private - they should never give away details of their address, age or full name, and you can adjust parental settings on your devices to keep this information hidden (see our **Know Your Stuff** guide for more information). Never allow your child to meet online friends in real life without a trusted adult present!

## Grooming

As they are in a space where anonymous users can strike up conversations with strangers, online games provide an environment for abusers to begin the process of grooming children. See the **Common Issues** section of the guide for more information on the signs that a child might be being groomed and how to address them.

## Loot boxes and premium currency

A loot box is an optional extra that you can unlock in a video game. They might be cosmetic upgrades that can be seen as a symbol of status in the world of the game, or they may even give bonuses that make it easier to win. These are often paid for using a special kind of currency that exists within the game world, but you can use real-life money to pay for that currency.

The problem with loot boxes is that you don't get to see what's inside until after you've purchased it, meaning every purchase runs the risk of disappointment. While loot boxes aren't legally considered a form of gambling in the UK, they can use the same sort of psychological techniques as online gambling sites to encourage people to keep buying.

Letting your children occasionally buy a new outfit for their favourite game character as a treat isn't dangerous, but if left unchecked the pressures put on them by both the games and their peers can become too much. Talk to your child about the games they're playing, and try and play them with your child to increase your understanding. You should also agree with your child that they will ask your permission before buying any add-ons for their games, and set spending limits on devices they use (see our **Know Your Stuff** guide for more information).

## Parasocial relationships

**Parasocial relationships** are any relationship where all of the emotional investment comes from one person. This is common among fans of popular YouTubers and Twitch streamers: many people who watch this content can come to feel a connection with the creator - even thinking of them as a 'friend' - while the creator remains completely unaware of their existence.

Parasocial relationships are not an inherently negative thing: they can allow children to feel less lonely, inspire their creativity, or act as role models. But it's crucial that children understand the reality of these relationships, and not come to think of their favourite content creators as their friends. Talk to your children about the videos and streams they watch, and encourage them to think about why they find certain content creators so appealing.

# How Can Natterhub Help?
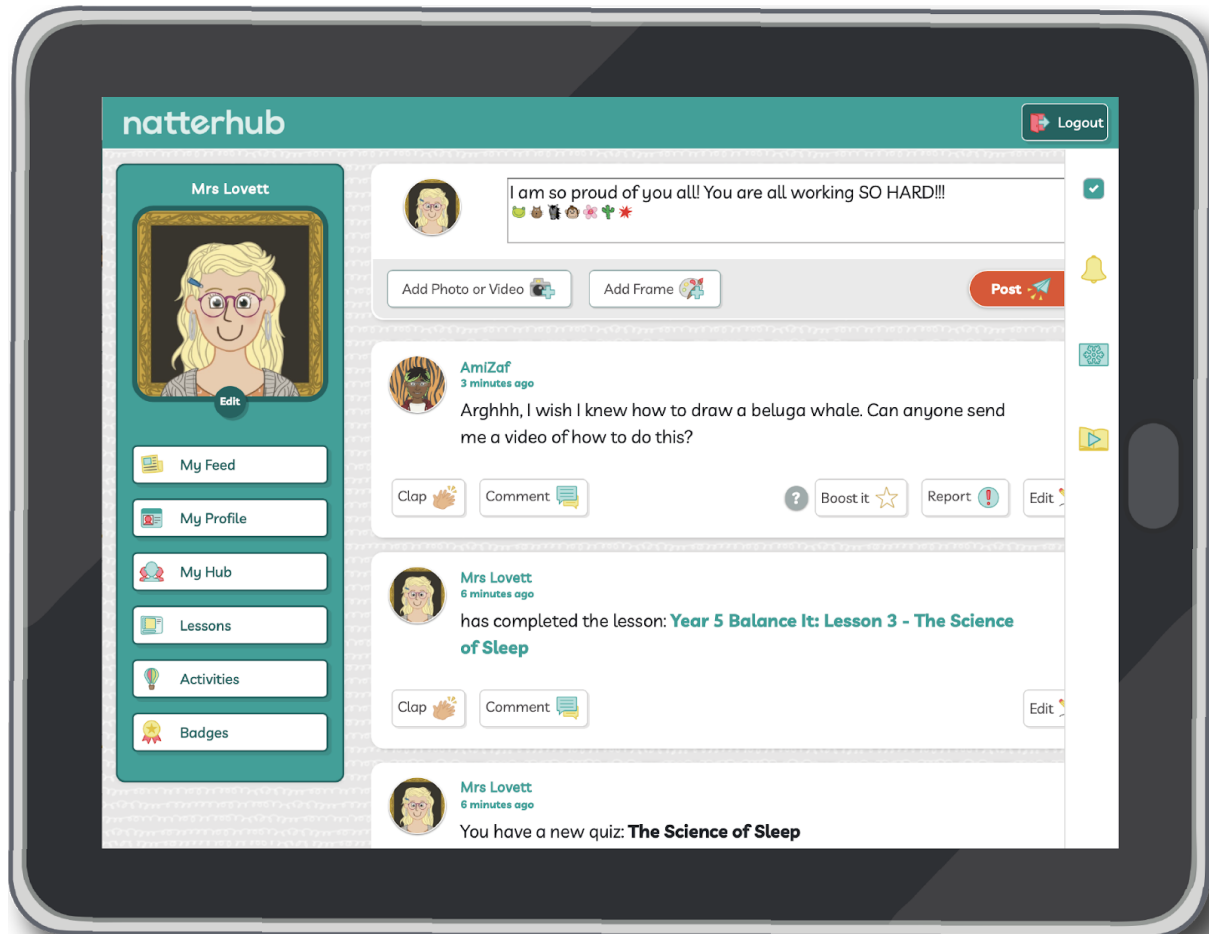


Lessons within Natterhub are split into eight different categories, which help children to internalise some of the most important rules for online behaviour:

## Balance It

*We take care of our minds and bodies.* It's important to moderate the time you spend on screens, take regular breaks for exercise, and put devices to bed so that you get a good night's sleep.

## Chat It

*We use respectful words when we chat to people.* People can often forget that other internet avatars have real people behind them, so don't say anything to a person online you wouldn't say in real life.

*Continued overleaf*

## Feel It

*We are kind and thoughtful to people.* Spread positivity online by encouraging others and praising them for their achievements.

## Learn It

*We use technology to help us in different ways.* Think about how you can use technology to help you do school work, or do something creative! Use photos and videos to show others what you've been up to.

## Mind It

*We are kind and honest online.* If you see another person online doing something that isn't right, you should challenge them on it, or speak to a trusted adult.

## Question It

*We ask questions and are open-minded.* Be open to the experiences of other people, but think carefully about everything you read online and make sure it's trustworthy.

## Secure It

*We keep ourselves safe online by using privacy settings and common sense.* Make sure all your devices and accounts are protected by passwords, and think carefully about what should and shouldn't be shared online.

## Think It

*We think carefully about what we do.* Imagine everything you post on the internet is written in permanent ink - check your own behaviour, and challenge others who are being inappropriate.

Children who show a good understanding of these rules will be awarded **Badges of Honour**, which can be powered up by their teachers at the end of every lesson. By reinforcing these behaviours in a classroom setting, we can make sure that children are ready for anything and everything that they encounter in the digital world, through primary school and beyond!

If you would like to contact anyone from the Natterhub team to discuss how Natterhub might support your school provision for Online Safety, please contact us at **info@natterhub.com**
**Stay safe!**