Altogether Better Policing

DURHAM

CYBER SAFETY

Durham Cyber's **Parents/guardian guide**

DURHAM CYBER

Altogether Better Policing

DURHAM CYBER SAFETY

We here at Durham Cyber have created this guide to help you set up parental controls to provide your child with a safer online environment. Parental controls can help to protect your child from seeing something that they shouldn't - although it is important to emphasise that no system is effective all of the time, so it is important to engage with your child and talk to them about their online life regularly.

If you require any further information please feel free to contact our team at Cyber.protect@durham.police.uk

internet matters.org

THINK U KNOW

GET SAFE ONLINE

IWF Internet Watch Foundation

CONTENT PAGE

PS5

Purchasing

App Access

Chatting

Timer

Online Games

Parental Controls

Privacy and Identity theft

Inappropriate content

Game ratings

Access to the PlayStation 5 console, and a PlayStation Network (Master) account in your name that you will use to create a sub-account for your child.

If you require any further information please feel free to contact our team at **Cyber.protect@durham.police.uk**

For more information scan the above QR Code.

XBOX ONE X

Purchasing

Chatting

Browser Access

Inappropriate content

Game ratings

Parental Controls for Xbox One X and Xbox One S can be set for each of your children's individual profiles, allowing you to prevent unauthorised purchases, ensuring your children only access age-appropriate content and restrict the ability to chat to strangers online.

For more information scan the above QR Code.

NINTENDO SWITCH

Browser Access

Chatting

Timer

Inappropriate content

Game ratings

The Nintendo Switch Parental Controls smart device app is a free app that can be linked with Nintendo Switch to monitor what your child is playing. The app creates a report so you can see which video games your child plays and how long for. It also allows you to set which games your child can play based on their PEGI age rating and restrict your child from sending/ receiving messages from other users.

For more information scan the above QR Code.

OTHER PLATFORMS SCAN QR CODE

Wii™

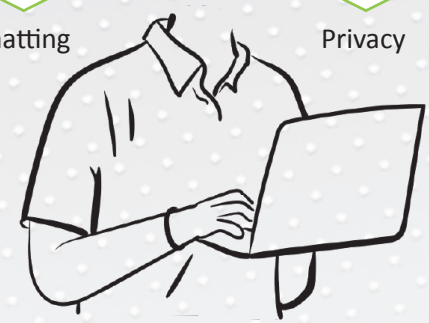
STEAM®

PSVITA
PlayStation®Vita

Discord

Chatting

Privacy



Parental Controls

App Access

Sharing Data

Social Networking

Launched in 2015, Discord is a platform for people with similar interests to share and communicate. It is popular among the gaming community as it offers a way for video game players to communicate with each other and develop a community outside of the games themselves.

However, it has grown into a full social network with over 140 million* active monthly users. It is no longer just popular among gamers.

For more information scan the above QR Code.

FORTNITE

Chatting

Calls and texts

Inappropriate content

Privacy and Identity theft

Parental Controls

Mobile Device

If your child loves gaming, there's a chance you've heard of Fortnite. Fortnite offers a range of parental controls to help you control what a player can see and do within the game. In addition to the controls within Fortnite, there are additional controls available on Playstation 4, Xbox One, Nintendo Switch, and iOS.

For more information scan the above QR Code.

ROBLOX

Chatting

Purchasing

Inappropriate content

Online Games

Roblox features a central dashboard to limit the chat functions, add a parental pin and account restrictions (to only access curated content by Roblox). Roblox also has a useful feature called 'Age Visibility' to determine settings for kids are age appropriate.

Social Networking

For more information scan the above QR Code.

MINECRAFT

Minecraft has parental controls on Xbox Live but they also have in-game safety settings. Please note, children under 13 years need parental permission to set up an account.

For more information scan the above QR Code.

Chatting

Online Games

OTHER GAMES SCAN QR CODES

WHAT ARE THE RISKS OF ONLINE GAMING?

TROLLING, GRIEFING AND SCAMS

Griefers are gamers who deliberately try to ruin the game for other players. This can also be called trolling. Players may also try to trick or scam young people into giving up 'skins' or other in-game items by offering them money or by hacking their account. Skins are a cosmetic feature that let players personalise their character and in-game items, they can be extremely rare and valuable so losing them can be upsetting for a child.

IN-GAME PURCHASES

Some games cost money to download, or players need to buy credits or items so they can keep playing. Many free games are designed to make the player want to continue but need payments to make this possible, which can be very frustrating. We suggest not storing payment card details on devices or in apps, to prevent charges building up.

BEING BULLIED

They may be deliberately excluded from a game by their friends, or criticised for how they play. Other players may swear or use abusive language over voice chat, and this can be upsetting for your child. If your child is experiencing bullying in online games, tell them they can talk to you or contact Childline and show them the blocking and reporting functions in a game, so they can prevent bullies from contacting them.

TALKING TO PEOPLE THEY DON'T KNOW

Young people can also use other platforms, like Discord and Reddit, to learn tips about the games they play and speak to other players with similar interests. Many popular games have official channels with thousands of members. This puts young people at risk of grooming or online forms of abuse, along with the risk of moving the conversation to other platforms or meeting up offline.

CHAT APPS

WHAT ARE CHAT APPS?

Chat apps allow the user to send messages, photos, videos and documents, as well as creating large group chats.

Some apps allow users to message people they don't know, so your child could receive messages from people they don't know - most apps have settings to allow this to be changed so that they only receive messages from people they know. With your child, make sure these settings are in place and show them how to reject requests from people they don't know.

Even with friends, your child might see something that upsets them. Explore each app to see if there are reporting and blocking features. Show your child how to use these features and talk about situations when they might want to report or block.

RANDOMISED CHAT FORUMS AND APPS

There are several sites and apps where the main aim is to randomly connect you to other users, this can be via text but also sharing images and videos as well as livestreaming. Many of these sites are designed for adults, however without age verification procedures in place young users can easily gain access.

There is a high risk that children could come across inappropriate or sexually explicit behaviour on this type of platform, as well as young people being contacted by adults they don't know. Monkey and Omegle are examples of this type of app.

LINGO & MEANING

AFK

Away from Keyboard

GG

Good Game

SMURF

Someone with high skills

BOT

Refers to a character that is controlled by a computer

TOXIC

Refers to a player who is irritated or rude to his teammates or the opposite team.

EASTER EGG

Refers to a hidden message

POGGERS

Expresses excitement or excess joy

PAH

Parents at home

KMS

Kill myself

Cul8r

Call you later

LINGO & MEANING

WTTP
Want to trade pictures

CYF
Check your Facebook

YTSFM
You're too sexy for me

LTD
Lovers 'til death

AYPWOL
Are your parents watching or listening

LMIRL
Lets meet in real life

ITILY
I think I like you

Po-Po
Police

26y4u
Too sexy for you

GN
Get Naked

SMART DEVICES

Children are using devices at a younger age so it's important to consider setting controls on the devices they use. Before you just hand over the device to your child.

Things to consider family, locations, pins.

Apple
Controls & settings and Family sharing.
Things you can monitor Screen time.

Amazon
In App purchasing
App Access
Inappropriate context.

Android
App Access, Online games
In App purchasing.

For more information on other devices such as Amazon, SkyQ, smart watches and more visit;

WIFI

Most broadband providers will have some form of parental controls for any devices connected to the wi-fi whether this is logging into the website or downloading a app. If your child turns off the Wi-Fi on there devices and only uses data it is important to ensure other safety controls are in place, see the device section for more information.

Virgin media

BT

sky

TalkTalk For Everyone

Things they can filter:

- Inappropriate context
- Social networking
- Phishing & Malware sites
- Weapons & Violence
- Gambling
- File Sharing

More guides or step by step instructions;

THINGS TO REMEMBER

- Whilst parental controls are a helpful tool there are limitations. They won't help if your child connects to a different Wi-Fi with no controls in place. For example, if you block a certain app or website on the broadband device if they then disconnect from that WI-FI and use another one, that app or website will no longer be blocked.

- Parental controls are just part of the way you can help keep your child safe online. Talk to your child and explain why we need to be safe online and the hidden dangers they could come across. Discuss together what they enjoy doing online and build up a level of trust so they can confide in you if anything happens.

- Set good, strong passwords on all of your accounts. Cyber aware recommends three random words. On some parental controls you can set a password which prevents settings and features from being changed. Don't make it too personal such as dates of births, this makes it easy for your child to guess them.

- Age is a major factor; as children get older, restrictions and controls you use will change. Only make changes if its appropriate and you feel like your child will use it safety.

COMMONLY USED APPS

Its important to know what apps your child is using and how to access all the parental controls. The best strategy for understanding your children's online activity is to sit down and speak to them, so they understand the dangers and how to apply the correct safety controls. Here are the most commonly used ages by young people.

INSTAGRAM 13+

What is it?
Photo and video sharing app.

Things to consider:
Account privacy - hidden words and phrases restrict any comments that contain a list of words you consider offensive or inappropriate.
Comments can be turned off on your photos.
Location tagging will show where the photo was taken and will let others who search that location see it.

SNAPCHAT 13+

What is it?
This is a messaging app that lets users exchange pictures and videos that disappear after they're viewed. It lets you use filters and effects and share it with friends.

Things to consider:
Location: Ghost mode - so location is hidden.
Privacy control - Contact me, View My Story, See My Location, See me in Quick Add. This can be changed so only friends can see or everyone (public). Snapchat accounts are often targets for sextortion scams.

COMMONLY USED APPS

YOUTUBE 13+

What is it?
a video sharing service where users can watch, like, share, comment and upload their own videos.

Things to consider:
If your child is under 12 YouTube Kids can be a great alternative. This allows parents to gear videos toward their age and sets time limits.
Restricted Mode is better suited for pre-teens and teens.
Both restrictions can help, but often times, they don't do enough to truly keep kids safe when using YouTube.
Teach children how to block and report.

WHAT'S APP 13+

What is it?
WhatsApp uses the internet to send messages, images, audio or video. The service is very similar to text messaging services

Things to consider:
Shows when you're online this cant be turned off.
Check the privacy setting for who can see your last seen, profile photo, about, groups and status.
Location sharing on WhatsApp.
If this setting is switched on, any images and videos shared will also show the location of where they were taken on a map.

COMMONLY USED APPS

TIK TOK 13+

What is it?
short-form, video-sharing app

Things to consider:
You can choose to have a public or private account. If you set your account to private, Family Pairing.
You can use Family Pairing to link your own TikTok account to your child's account. This will allow you to have controls such as, Screen Time, who can Direct Messages, Restrict inappropriate content and disable search bar.

KIK 17+

What is it?
Online instant messaging service

Things to consider:
Only need an email address to sign up.
No parental controls offered.
In Kik's privacy settings there's a 'Let Friends Find Me' option, which allows users who already have your contact details to connect with you. This option is turned on by default so make sure to switch this off.

COMMONLY USED APPS

YUBO 17+ OR 13+ WITH PARENTS' PERMISSION.

What is it?
A app designed to meet new people.

Things to consider:
Sharing location - 'Hide my city' to keep their location private.
Possibility your child can come across Inappropriate content.
Option to restrict friends to find them on the app using their mobile number.

OMEGLE 18+ OR 13+ WITH PARENTS' PERMISSION

What is it?
A video-chatting website and app that pairs random users identified as 'You' and 'Stranger' to chat online via 'Text', 'Video' or both.

Things to consider:
No parental controls.
Spy mode where another "Stanger" can observe and ask questions.
Lack of Moderation on Video Chat.

TELEGRAM 17+

Users of Telegram have privacy settings available to help you manage:

Who can see your phone number
Who can see when you were last online
Your profile photo
Who can call you
Who can add you to groups and channels

GOLDEN SOCIAL MEDIA RULES

- Enable Two-Factor Authentication with a strong password
- Check Login Activity
- Make Your Account Private
- Disable Activity Status - if you don't want people knowing your online
- Block, Restrict, or Report Accounts
- Don't put too much personal information out there
- Disable location
- Manage friends - if you don't know them, remove them from your friend list.
- Finally remember once it is online, its out there somewhere forever

While some of these features might not be available on all apps its important to consider them if offered. This will not only help protect your account but also helps reduce stalking, harassment and overall create a good management for your account.

STREAMING

NETFLIX

You could create a kid's profile which only includes content appropriate for children.

You can add a PIN to your account so a 4- digit PIN must be entered to either play any TV show or movie above a selected maturity level.
Apply new filters or Restrict specific title.
Looking at viewing history.

AMAZON PRIME

You can add a PIN to your account so a PIN must be entered to purchase or view restricted content.
You can create a child's private

DISNEY PLUS

Disney+ offers multiple parental control features for you, such as;

- Content ratings
- Kid's profile
- Profile PIN
- Profile creation restriction

HELPFUL WEBSITES

@DurhamCyber

We are on social media , Instagram, Twitter , Facebook Keep in the know and next door. This is not a reporting tool however we share the latest trends and cyber knowledge. You can also message us with any questions.

CEOP (Child Exploitation and Online Protection Centre) is for adults/ children report any online sexual abuse /grooming on behalf of themselves or someone they know.

Think U Know is the education side to CEOP so make young people think about whom they are talking to online and what activities they get involved in online.

Internet matters provides a large range of guides on parental settings which is used throughout this booklet.

Get Safe Online is the UK's leading source of unbiased, factual and easy-to-understand information on online safety.

Cyber Aware is designed for family and individuals giving the basic cyber security advice to keep you safe.

This offer online safety guides for all different aspects for online issues.

Altogether Better Policing

DURHAM CYBER SAFETY

D10-22