

INSPIRED TO CARRY ON

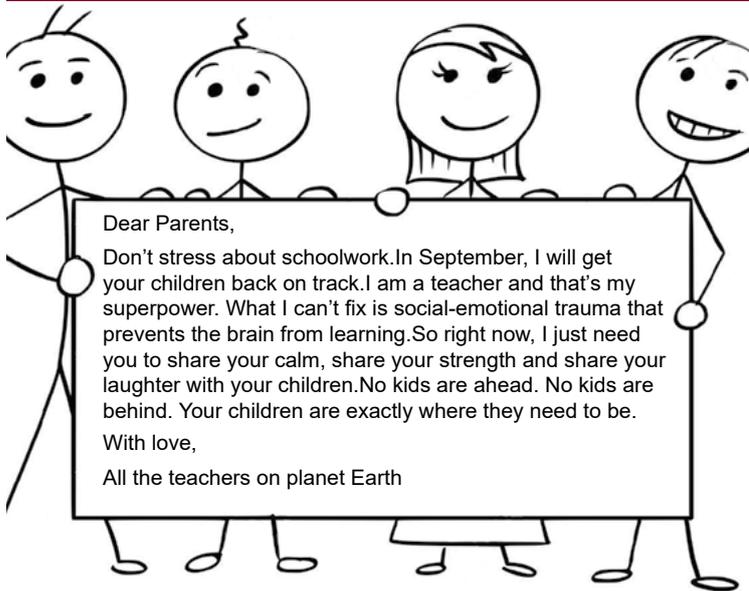
Parents, carers and students,

I have been, like many of you I am sure, completely inspired by Captain Tom Moore. He has become a beacon of hope in these challenging times. He reminded us that 'the sun will shine on us again and the clouds will go away'. A poignant moment for me was during the RAF flypast when Captain Tom's arm shot up in pride and when he told us that he was one of the few people to see the Spitfires flying in anger, and he was able to see them flying peacefully. The hope and unity that Captain Tom brought to our lives by raising over 30 million for the NHS has been heartwarming to watch. It called me to reflect on our school; despite being apart physically, we are always united as a community and the children, as always, are an unconditional source of hope. They are the reason we do what we do and we will always strive to do our best for them. Although it has been a very different start to the summer term, I hope that the students will continue to show commitment, develop new skills and become more self-reliant. We will continue to do all that we can in the circumstances to provide for them and we are always here for you as families if you need us.

Please do stay at home so we can all keep safe and save lives.

L. Swaine, Headteacher

A SMALL NOTE TO PARENTS AND CARERS



CAN YOU HELP? PTFA LASER-CUTTER APPEAL

Over the past few weeks, EBS has been making face-mask extenders to help front-line staff in the NHS – but we need a new laser cutter to make even more! Are you able to help? If so, please:

- Donate £5 - text the word EBSPTFA to 70970
- Donate £10 - text the word EBSPTFA to 70191
- Or visit www.easydonate.org/EBSPTFA to donate any amount - every little helps!

If you are a UK tax payer, please Gift Aid your donation and HMRC will add 25% at no cost to you!

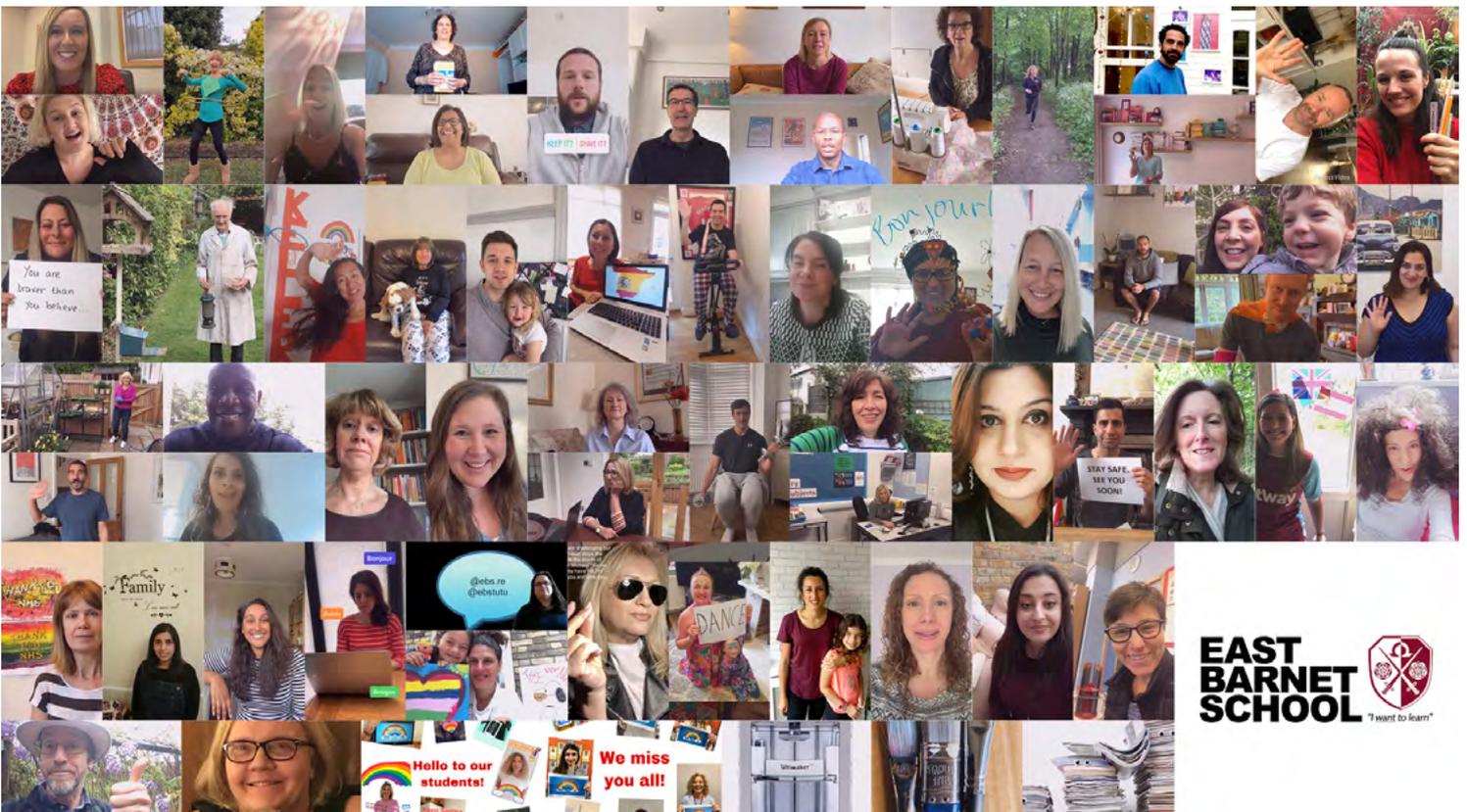
When school is back to normal, the £10,000 cutter will continue to be used in D&T lessons by all our students.

THANK YOU from EBS and the front-line staff of the NHS!

CHANGES TO THE SCHOOL DAY

Thank you for the questions and feedback. EBS will provide a response to queries by the 22nd May.

WE MISS YOU & WANTED TO SAY HI! CLICK BELOW - YOU MAY NEED TO LOGIN TO ONEDRIVE!



KEEP YOUR CHILDREN SAFE IF THEY USE HOUSEPARTY, ZOOM OR NETFLIX

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

LIVE

REC

AGE RESTRICTION

13+

WHAT IS HOUSEPARTY?

Houseparty is a live streaming app described as a face-to-face social network where people 'drop in' on each other's screens to watch live streams and hang out in real time. The app is available for iOS, Android, macOS and Google Chrome and has over 1 million users worldwide. It's important to note that children under the age of 13 must have a parent's permission to access the services, however, no proof of age is required to create an account.

HOW DO YOUNG PEOPLE USE IT?

Each time the app is opened, your child will be instantly connected to other users who are also on the app. Users can create groups conversations of up to eight people at a time. Each time a person joins, the screen splits to show everyone who is currently in the room. They can chat with each other via text messages, search for their usernames, and share a link to their profile. They can have as many rooms as they want and move from one to another by swiping across the screen. Along with this functionality comes a few associated risks to be aware of.

LIVE

What parents need to know about HOUSEPARTY

"STRANGER DANGER"

Friends of friends can join conversations on the platform without the need to be connected to known friends. While it does alert users when individuals that they know enter their chat room, it also suggests strangers might be a reason for partying. It's important to note that children under the age of 13 must have a parent's permission to access the services, however, no proof of age is required to create an account.

SEXUALISED MESSAGES

People may use the streaming app as a opportunity to engage in inappropriate or illegal activities. There have been reports of users directly linking to Houseparty live streams and incidents where two Manhattan children aged 11 and 12 were reportedly targeted by users appearing to message back in 2017. Outside of their close friendship group, it's also important to note that friends of friends can connect with your child via the app, which may include people with this intention.

CONTENT BEING SHARED

The 'ScreenShare' feature lets users share moments from their Houseparty conversations by recording and sharing 15-second clips of chats. They also have the option to save these moments to their gallery. For privacy purposes, every member of the conversation will see a notification if another member is recording. This could be used by your child to share something on live chat that they may not want others to see. Screenshots of live streams can also be taken and shared with others, which could be shared widely and embarrass users.

IN-APP PURCHASES

By tapping on the dice icon your child can play a game called 'Roll the Dice'. This game allows your child to describe someone or something and the other players can guess who or what they are. The game is free but in-app purchases can be made. The potential for your child to get into trouble playing the game while working up a small fortune.

OVERSHARING PERSONAL INFORMATION

Children often don't understand this involved in giving out too much personal information in a live stream or within a chat. They may not realise that the personal details shared during online conversations. One example of this is a live chat about their location. Parents should be aware of where they live or go to school without realising.

CYBERBULLYING

Cyberbullying is when people use technology to harass, threaten or embarrass others. It can be done in a group chat by using a bully to make negative or harmful comments to others in the group. Exclusion from friendship groups within the app can also be used as a way for your child to feel sad and left out socially excluded.

LIVE

TURN ON PRIVATE MODE

One additional tip to use the app settings to turn on 'Private Mode' which automatically locks the room instead of doing it manually. Parents with questions can email us at help@houseparty.com

LIVE

Top Tips for Parents

SAFER CONVERSATIONS

With live streaming being such a popular feature on apps, it's important that you are aware of the dangers associated with it in order to protect your child effectively. Have regular and honest conversations with your child about what apps they are using and how they are using them. It may be a good idea to have your child show you how they use Houseparty and how to navigate through the platform so you are aware of how it works.

PROTECT THEIR PRIVACY

Your child may unknowingly give away personal information during a live stream, including their location. Talk to them about what constitutes personal information and make sure they do not disclose anything to anyone during a live stream, even to their friends. Advise them to remove any items in their live stream (school uniforms, street name, posters etc.) that could potentially expose their location or personal information. Check your child's privacy settings thoroughly. You have the option to opt out of certain uses and disclosures of personal information, such as turning off the app's location sharing option.

REMOVE LINKS TO OTHER APPS

Users can link their contacts to both Facebook and Snapchat, or can simply share a link to their profile. We do not publicly share access to their online profiles as there is the potential for strangers to get hold of your child's information or communicate with them.

BE PRESENT

A study conducted by the Internet Watch Foundation (IWF) found that 96% of streams showed a child on their own, often in their bedroom or bathroom. If your child is going to conduct a live stream, ask them if you could be present for it. This will give you a greater understanding of what your child is doing during their live streams and who they are streaming to.

REPORTING AND BLOCKING

If your child faces a problem while using the app they can report it directly to the platform by clicking their phone's prompt will pop up allowing you to report issues immediately by clicking on the 'report' button. They also have the option to report and block users directly on the user's profile.

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or inappropriate, they should report it to the platform. Parents can also report inappropriate content to the platform by clicking on the 'report' button. This will give you a greater understanding of what your child is doing during their live streams and who they are streaming to.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and share meeting IDs with anybody you don't know and always set up a password function to allow other people to sign in. This should already be the default setting that is applied to all Zoom meetings.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number and other personal details. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not fraudulent. Signs of a phishing email include a suspicious sender, an unusual domain name or a slightly distorted logo. The email itself might also be poorly written or contain suspicious attachments.

TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can turn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chat can help to limit the risk of receiving any malicious data or unwanted information. You can also turn off unnecessary features such as screen sharing, chat and video. This should already be the default setting that is applied to all Zoom meetings.

USE THE VIRTUAL WAITING ROOM FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live stream cannot automatically join and must wait for the host to screen them before entering. This is a default function and adds another layer of security to reduce the risk of receiving any malicious data or unwanted information. You can also turn off unnecessary features such as screen sharing, chat and video. This should already be the default setting that is applied to all Zoom meetings.

KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest version of Zoom available and always update it if you get a prompt. These updates are usually to fix bugs and improve the app's performance. Check the official website to ensure you are using the latest version and compare it to your own.

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then it's important to make sure that the host is abiding by Zoom's Terms of Service. This includes the fact that they have given everybody's permission for the meeting to be recorded. The host should also have a screen sharing to host only and disabled the feature which helps keep the live stream secure.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 25.03.2020

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

LIVE

Zoom

LIVE

What parents need to know about Zoom

Zoom bombing

Zoom bombing is the term which has been coined to describe uninvited people joining Zoom meetings uninvited and broadcasting profane or inappropriate videos. An attacker can join a meeting by using a random ID number and a password. Not taking preventative measures or implementing privacy controls can expose the risk of children witnessing sexual or inappropriate content with little notice.

RISK OF PHISHING

The rise in popularity of Zoom has led to a rise in phishing operations and phishing campaigns. This is where participants are encouraged to click on links to join a meeting that is not legitimate. Zoom meetings via email, which are in fact fraudulent. These campaigns to obtain sensitive information such as login details, passwords and/or credit card information.

PRIVACY CONCERNS

Depending on how the app has been set-up, Zoom can offer very little privacy. In many cases, the meeting hosts can see detailed information about each participant including their full name, phone numbers and email addresses. Furthermore, depending on where the camera has been set up or where your child's computer is positioned, private or personal information could be stolen depending on what can be seen in the background.

LIVE RECORDINGS

One of the features of Zoom is the ability to record live meetings. By default, only the host of the meeting can record the sessions however other meeting members can also record if the host gives them access. Recording can be done on devices or in the cloud and can be downloaded and shared with no restrictions. The means that videos, audio clips and transcripts of recordings involving your children could be widely shared on the internet or without your authorisation or consent.

PRIVATE ZOOM MEETINGS

Zoom has a facility to set up breakout rooms, which enables a host to split the participants of the original meeting into separate sessions. This gives children the ability to speak privately away from the main group to other users however this can be abused by the host if the meeting has been made public. Children could be more vulnerable to experiencing inappropriate content.

LIVE STREAMING RISKS

At its very core, Zoom facilitates live streaming. This means it inevitably carries some of the associated risks that live streaming brings. These are likely to be minimal but a concern nevertheless. However, if your child is streaming content that could be on the internet, it's important to note that content that is not encrypted and/or has limited security settings, may be more likely to be exposed to others. This could be a risk of exposure to inappropriate content, which could be a risk to your child's safety and well-being.

Safety Tips for Parents

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or inappropriate, they should report it to the platform. Parents can also report inappropriate content to the platform by clicking on the 'report' button. This will give you a greater understanding of what your child is doing during their live streams and who they are streaming to.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and share meeting IDs with anybody you don't know and always set up a password function to allow other people to sign in. This should already be the default setting that is applied to all Zoom meetings.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number and other personal details. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not fraudulent. Signs of a phishing email include a suspicious sender, an unusual domain name or a slightly distorted logo. The email itself might also be poorly written or contain suspicious attachments.

TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can turn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chat can help to limit the risk of receiving any malicious data or unwanted information. You can also turn off unnecessary features such as screen sharing, chat and video. This should already be the default setting that is applied to all Zoom meetings.

USE THE VIRTUAL WAITING ROOM FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live stream cannot automatically join and must wait for the host to screen them before entering. This is a default function and adds another layer of security to reduce the risk of receiving any malicious data or unwanted information. You can also turn off unnecessary features such as screen sharing, chat and video. This should already be the default setting that is applied to all Zoom meetings.

KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest version of Zoom available and always update it if you get a prompt. These updates are usually to fix bugs and improve the app's performance. Check the official website to ensure you are using the latest version and compare it to your own.

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then it's important to make sure that the host is abiding by Zoom's Terms of Service. This includes the fact that they have given everybody's permission for the meeting to be recorded. The host should also have a screen sharing to host only and disabled the feature which helps keep the live stream secure.

Meet our expert

Emma Davis is a cyber security expert and former ICT Teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

National Online Safety

#WakeUpWednesday

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 08.04.2020

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

LIVE

AGE RESTRICTION

18+

What parents need to know about NETFLIX

Inappropriate content

Netflix has a wide range of content for all ages. It has a wide variety of films and TV programmes and its extensive catalogue can provide hours of entertainment. Children can watch almost anything but if they share the same account as an adult, it can also often mean up to viewing material that is not suitable for children. Parents should check what children could access films or shows that contain violence, nudity or foul language.

Risk of hacking

With millions of users over 190 countries, Netflix is often targeted by hackers and phishing scams which try to trick usernames and passwords to gain access to accounts. If successful, this could mean payment details or try to sell your data on the dark web, providing others with the opportunity to steal. Given Netflix doesn't provide 2-factor authentication, it's important to ensure your login details remain secure.

Binge-watching

With the ability to access Netflix on almost any device, it can be easy to fall into watching 'TV series, with users finding it difficult to turn off without knowing what happens next. The autoplay function also means that the next episode usually plays within seconds of the last one. This can lead to spending hours in front of the TV through the night, potentially affecting sleep, mood and the ability to concentrate the next day.

Screen addiction

In addition to binge-watching, the fact that Netflix is available on almost any device with an internet connection means that parents may find it difficult to prize children away from a screen. With a huge collection of children's TV programmes and the latest film titles, children could start watching on the TV, continue on the tablet and then on their smartphones. This means that children may spend less time learning playing outdoors, find it difficult to sleep or communicate less with family and friends.

Netflix party

Netflix Party is a free extension on Google Chrome that gives users the ability to watch a film or TV show online simultaneously with friends or family in different locations. It also provides the ability to chat to each other during the stream. Users can create a party and send a link to people they want to invite however the link can be copied and distributed further, meaning children could potentially be open to a group that with people they don't know. It should be noted that Netflix Party isn't an official Netflix product and needs to be downloaded separately to the app.

Safety tips for parents & carers

Create a Netflix Kids experience profile

One of the biggest advantages of Netflix is the ability to control what content your children can watch. Setting up a Netflix Kids experience profile means that children only have access to TV shows and movies which have been created specifically for kids. The look and feel of the app is simpler and children can access any account settings.

Set maturity ratings & block content

If your child is a little older, parents can create a specific profile for their own use with a maturity rating that means children will only see TV shows and movies that are suitable for their age. Parents can also block specific TV shows and movies from individual profiles which means they don't show up in the browse or search results.

Have an open & honest conversation

Parents can review the TV shows and films that have been watched on their own profile and see what their child seems upset or shocked by something they have seen. If your child is concerned about anything they've viewed, try to talk to them about it and have an open and honest conversation to help understand any concerns.

Switch off autoplay

Netflix has two autoplay features that can be switched on and off across different accounts and takes effect across all devices. Parents can switch off the autoplay feature for episodes to play automatically and for previews to play when they watch. This can help to limit the amount of time children spend on the app.

Lock your profile

It's important to keep your own account secure so that children can't access your profile. Locking your profile means that only you can access their own profile which means only they can access their own content.

Set screen time limits

Although watching off autoplay will limit content programmes playing continuously, children can just sit and watch content on their own profile. Netflix has no options to help limit viewing time, many devices have their own parental controls or screen time, so you can switch off the app automatically when you think they've had enough.

Create a strong password & always log out.

Given that Netflix doesn't use 2-factor authentication, the need for a unique username and strong password is even more important. Try to use a different password to one you've used before and use a mixture of letters, numbers, symbols and punctuation. Always log out when using your account so that if your device is lost or stolen, your account remains inaccessible.

Meet our expert

Paula Burt is a cyber security expert and former ICT Teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

National Online Safety

#WakeUpWednesday

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 22.02.2020

ENRICH AND EXTEND YOUR LEARNING

Are you finishing your work early? Do you have spare time to fill during your days? Please take a look at the resources and opportunities below to extend and enrich your learning;

VIRTUAL SPEAKERS FOR SCHOOLS TALKS

Speakers for Schools are streaming some fascinating talks from a number of leaders in their fields covering a variety of topics from Acting, Journalism and Fake News to Football, Charity and setting up your own business. You can even get involved in the Q&A sessions, which form part of the talks. Please check out some of the really inspirational speakers performing in the upcoming weeks by clicking [here](#).

EXPLORE

Explore is an innovative digital outreach portal from the University of Oxford. As the 'Home of Big Questions' it aims to engage 11 to 18 year olds with debates and ideas that go beyond what is covered in the classroom. Big questions tackle complex ideas across a wide range of subjects and draw on the latest research undertaken at Oxford. Explore aims to realise aspirations, promote broader thinking and stimulate intellectual curiosity. Find out more about topics from Archaeology to Zoology and answer questions such as 'Could we end Poverty?' or 'Can War be a good thing?' This truly is a fantastic resource and should be used to extend your learning when perhaps your schoolwork has been completed early. Click [here](#) to access the site.

VIDEO MAKING - Divergent Thinking are offering FREE online mobile video-making workshops for young people aged 16-25 years old. 9th or 16th May, plus chance to win £50 worth of vlogging equipment. Click [here](#) for more info.