Great Denham Primary School

Inspiring excellence; everyone, everyday

EXCELLENCE . . . . RESPECT . . . . COURAGE . . . . DETERMINATION . . . . FRIENDSHIP . . . . EQUALITY

9th April 2020

A message from the head.....

This week has been a little quieter at care club but the children have still had lots of fun and enjoyed Easter activities as well as the nice weather. It was particularly exciting to see SpiderMan this morning!

At these difficult times please do not be too hard on yourselves regarding the new 'home schooling' arrangements. This is not home schooling; this is an unprecedented emergency situation impacting the whole world. You are, and have always been your child's primary educator. If you decide that your child isn't going to engage with learning some days then let them have a day of playing, baking or watching TV, it is your choice.

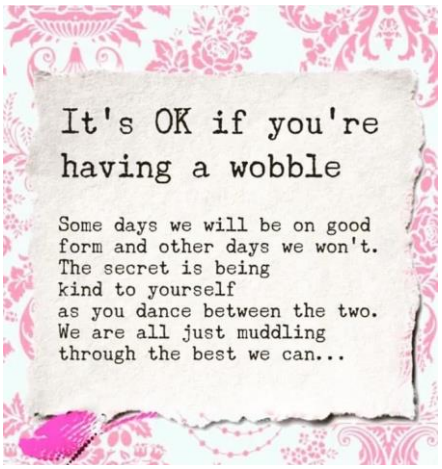
Please do not feel stressed or guilty about this! When the new learning packs come out there is a lot of work in them, however, we have tried to ensure there is plenty of variety for the children for those who want it. There will be example timetables in the packs again, but please they are not timetables that must be followed, they are purely there as an example. What works for one family will not work for another, so do not worry. Minimising stress at this difficult time is vital for you and your families well-being. So please take care and stay safe and have a lovely Easter weekend and enjoy this weather!

Denise Burgess

Headteacher

Home Learning Packs – Summer 1 term

The teachers are currently busy preparing home learning packs for next half term. The packs this time will include enough work to last until May half term. Again they will be a mixture of written work, creative work and online learning. Packs will be available for collection (as part of your daily exercise allowance) on the following days from the community room. Please only come at your allocated slot and please let me assure you we will be keeping to social distancing rules. If you are unable to collect your pack due to self-isolation we will deliver them to you, please let us know via email. For siblings please just pick one of the relevant dates. If you would like new reading books for your child**, please bring the current ones back to exchange them.**



Monday 20th April :	**9 – 11am**	**Year 4**	**1 – 3pm**	**Year 2**
Tuesday 21st April :	**9 – 11am**	**Year 1**	**1 – 3pm**	**Year 3**
Wednesday 22nd April :	**9 – 11am**	**Year 6**	**1 – 3pm**	**Year 5**
Thursday 23rd April :	**9 – 11am**	**Pre School**	**1 – 3pm**	**Reception**

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 to video chat, leave messages and hang out in groups. The app is available for iOS, Android, macOS and Google Chrome and has tens of millions of 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 group conversations of up to eight people at one time. Each time a person joins, the screen splits to show everyone who is part of the conversation. Your child can add contacts via phone numbers, search for their usernames, and share a link to their profile. They can have as many rooms as they want and move from chat to chat by swiping across the screen. Along with this functionality comes a few associated risks to be aware of...

What parents need to know about HOUSEPARTY

"STRANGER DANGER"

Friends of friends can join conversations on the platform without the need to be connected or known to all the other users in the chat. Houseparty calls this feature 'Stranger Danger'. While it does alert users when individuals they may not know enter their chat room, it also suggests strangers might be a reason for 'party time'. There's also the danger of people attempting to deliberately mislead others by using false names or usernames.

SEXUALISED MESSAGES

People may use live streaming apps such as Houseparty to engage in inappropriate or illegal activities. There have been concerning reports directly linked to Houseparty, including one incident where two Mancunian children aged 11 and 12 were reportedly targeted by men exposing themselves back in 2017. Outside of their close friendship group, it's also important to note that friends of friends can also connect with your child via the app, which may include people with this intention.

CONTENT BEING SHARED

The 'facemail' feature lets users share moments from their Houseparty conversations by recording and sharing 15-second snippets of chats. They also have the option to save these moments to their gallery. For privacy purposes, every member of the group will see a notification if another member is recording - this could be a concern if your child shares something in the live chat they may later regret. Once recorded, they lose control over the video and how it is used. Screenshots of live streams and private messages can also be taken which could be shared widely and embarrass users.

CYBERBULLYING

Cyberbullying is when people use technology to harass, threaten, embarrass, or target another person. Group chats can be used by bullies to make negative or hurtful comments which may cause offence or be harmful to others in the group. Exclusion from friendship groups within the platform may make your child feel sad and left out/socially excluded.

OVERSHARING PERSONAL INFORMATION

Children often don't understand the risks involved in giving out too much personal information in a live stream or within their profile. They may also be less protective of personal details during online conversations. One example of this within a live chat could be their background revealing information about where they live or go to school without realising.

IN-APP PURCHASES

By tapping on the dice icon your child can play a game called 'Heads Up!' where one person gives clues to describe someone or something and the other players guess. Three cards are included for free but additional decks cost real money. There's the potential for your child to get carried away playing the game while working up a small fortune.

Top Tips for Parents

SOURCES:
https://www.thetimes.co.uk/article/houseparty-the-chat-app-thats-taking-over-facebook-[illegible]
[illegible]
https://www.houseparty.com

National Online Safety
#WakeUpWednesday

TURN ON PRIVATE MODE

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

SAFER CONVERSATIONS

With live streaming being such a popular feature on apps, it is 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.

CHECK COMMUNICATIONS

Also, it's important to be aware of who is on their friends list and who they are communicating with. Remind your child to not communicate with people they do not know and trust. If they experience something on the app that makes them feel uncomfortable then they should tell a trusted adult immediately. Remind your child that if they get an invite to join a Houseparty room from someone they don't recognise, then they should ignore the request.

'LOCK' ROOMS

In regards to communicating with users on the platform, we advise that your child uses the 'lock' feature to make their conversations private. This means that other users, especially strangers, can't join their conversations.

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 uniform, 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.

PROTECTING YOUR CHILD'S DIGITAL FOOTPRINT

As the videos are live, it may lead to the misconception that whatever happens in the video will disappear once the live stream ends. All content shared on the app can be recorded or screenshotted and shared to a wider community. It is important that your child knows that what they do now may affect their future opportunities. In addition to this, the video chats can't be reviewed later which means unless a parent or carer is sitting nearby during a call, they won't know what has been said. It's worth bearing in mind that parents can see when their child has last communicated with someone and for how long for under the 'We Time' feature.

REMOVE LINKS TO OTHER APPS

Users can link their account to both Facebook and Snapchat, or can simply share a link to their profile. We advise that your remove these links and remind your child not to 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 direct to the platform by shaking their phone. A prompt will pop up allowing you to report issues immediately by clicking on the 'report now ' button. They also have the option to report and block users directly on the user's profile.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

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.

Founded in 2011, Zoom is one the world's leading video conferencing software providers. It has a number of features, including video and audio conferencing, real-time messaging, screen-sharing and the ability to upload, share and search for content. Users can start their own meetings or they can join meetings set up by others. The app is available to use across PCs, laptops, tablets and mobiles phones and is free to download on both the app store and on Android.

What parents need to know about ZOOM

ZOOM BOMBING

'Zoom bombing' is the term which has been coined to describe unauthorised people joining zoom meetings uninvited and broadcasting pornographic or inappropriate videos. An attacker can hijack a meeting if they know the meeting ID and it isn't reinforced with a password. Not taking preventative measures or implementing privacy controls could open up the risk of children witnessing sexual or inappropriate content with very little notice.

RISK OF PHISHING

The rise in popularity of Zoom has led to a rise in hacking operations and phishing campaigns. This is when participants are encouraged to click on links to join what they believe to be legitimate Zoom meetings via email, but which are in fact fraudulent. These scams aim to obtain sensitive information such as user 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 maybe even location data. 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 usually record live sessions however other meeting members can also record if the host gives them access. Recordings can be stored on devices or on the cloud and can be downloaded and shared with no restrictions. This means that videos, audio clips and transcripts of recordings involving your children could be widely shared on the internet or between users without your authorisation or consent.

PRIVATE ZOOM MEETINGS

Zoom has a facility to set up breakout rooms, which enables a private meeting within the main Zoom session. The host can choose 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 chats aren't always monitored by the host and if the meeting has been made public, children could be more vulnerable to experiencing negative comments.

'LIVE STREAMING' RISKS

At its very core, Zoom facilitates live streaming. That means it inevitably carries some of the associated risks that live streaming brings. These are likely to be minimal within a controlled environment (for instance when used in a classroom setting for remote learning). However, live streaming means that content isn't always moderated and children who use the app unsupervised or with limited security settings, may be more at risk of exposure to viewing inappropriate material. Other risks can include downloading malicious links, sharing personal information or even potential grooming.

Safety Tips For Parents

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or upset then they need to talk about it and report it. Parents can report unwanted activity, harassment, and cyberattacks to Zoom directly. To help your child, you could try setting up a checklist before they go online, with an agreed set of rules and what they should do if they see something inappropriate.

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 less likely to be hacked. It's important to never 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 a default setting that is applied on Zoom.

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, etc. Create your child's account under a false name or pseudonym and always set a custom background to help hide details in your home. 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 an unrecognisable email address, an unofficial 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 chats can help to limit the risk of receiving any malicious attachments or receiving any inappropriate messages. In addition, you can turn off the camera if it is not needed or mute the microphone when not in use.

USE THE 'VIRTUAL WAITING ROOM FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the host to screen them before entering. This is now a default function and adds another layer of security to reduce the likelihood of zoom bombing.

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 security holes and without the update you will be more vulnerable to an attack. Check the official website to see what the latest version is 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 gained everybody's permission for the session to be recorded. The host should also have set screen sharing to 'host only' and disabled 'file transfer' to help 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

SOURCES: https://zoom.us/privacy | https://zoom.us/ | https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf
https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing