

**Which Week?****This Week: Monday 22nd April (Week 1)***Next Week: Monday 29th April (Week 2)*

Sixth Sense

**“Start Spreading the News...”**

Next year's February half term trip to New York City, led by Mrs Ridley, will be launched this week for any students in Year 8, Year 9, Year 10 or Year 12 (who will therefore be in the next year up by the time of the visit).

A £150 deposit will be required to secure a place on the trip and a further payment plan, outlined on the trip letter will then require further payments throughout the course of the year to support parents and carers, or indeed, you, in realising this opportunity for you to absorb the cultural capital of an itinerary that takes in all of the sights and sounds of this incredible city. Mrs Ridley literally puts together a once-in-a-lifetime-trip to be able to tick New York off the



Podcast recommendation of the week!
Sport and the British (BTEC

Sport and Exercise Science, A Level History)

Despite this being a slightly older podcast, with it being historical in nature, it still remains utterly relevant and links strongly to the Sociology of Sport unit covered by our BTEC Sport and Exercise Science students.

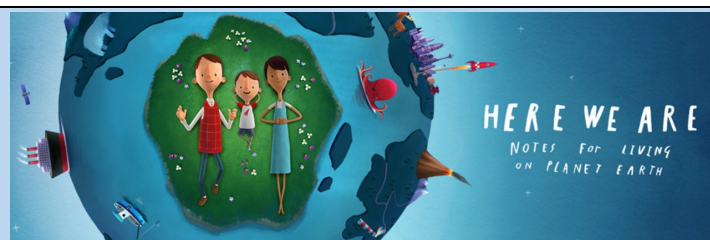
The popular presenter, Clare Balding, a sports enthusiast herself, charts how Britain has shaped sport and sport has shaped the British.

Apart from the English language itself, the invention of modern sport has been our major cultural legacy to the rest of the world.

In this narrative history series with the help of the academic team from the International Centre for Sport History and Culture at De Montfort University, Clare looks at the unique and vital role sport has played, and continues to play, in our national life.

With thirty episodes to choose from, all of which (again) are a 'bitesize' 15min in length, there is an incredible range of programmes from the rise in Olympism to the exporting of football to the journey that women have faced in sport (in Britain). If you think you know about sport, this podcast will help to rethink this knowledge and develop your understanding.

Link to home page for this series of podcasts on website: <https://www.bbc.co.uk/programmes/b01b9h7c>



The 22nd April marks 'Earth Day'. The first Earth Day in 1970 mobilised millions of Americans from all walks of life, giving birth to a broad new movement to protect the planet. This group of 10% of the U.S. population at the time took to streets, college campuses and hundreds of cities to protest environmental ignorance and demand a new way forward. Earth Day is now recognized as the planet's largest civic event each year.

The pressure from the weight of support from Earth Day led to the passage of landmark environmental laws in the United States, including the Clean Air, Clean Water and Endangered Species Acts and the establishment of the Environmental Protection Agency (EPA). Many countries, including the UK, soon adopted similar laws, and in 2016, the United Nations chose Earth Day as the day to sign the Paris Climate Agreement into force. You will look at this to a greater extent in form time this week, but essentially allows all of us to think about how we could be even more of a 'force for good' for climate change, whether that is ensuring we are more mindful of recycling versus simply putting something into a bin and switching off lights when rooms are not in use and being less wasteful with water. Simple changes can accumulatively have such a large impact!

Online Safety: Zoom

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 mobile phones and is free to download from both the App Store and Google Play.

With the increase in use of video conferencing as part of recruitment processes for employers, apprenticeship providers and potentially, universities, the guide on page 2 of the newsletter provides tips on a number of potential risks such as 'Zoom bombing', phishing and privacy concerns.





Founded in 2011, Zoom is one of 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>