

Woodford County High School for Girls

Bulletin

Issue No. 403

7th June 2022



We welcome student back to the summer term. Students have started their examinations this week, and we wish them good luck.

Please see below what is included in this weeks bulletin:

Page 2	Online Safety Training for Parents – New!!
Page 3	Year 7 & 8 Movie Night– New!!
Page 4	After school activities– New!!
Page 5	What you need to know about Apple Guided Access
Page 6	What you need to know about Social Media Scams
Page 7	Music Clubs
Page 8	PE Extra-Curricular
Page 9	Miss Runacres’s Fitness Sessions
Page 10	Cross Country Club
Page 11	Foster for Redbridge
	Follow us on Social Media
Page 12	Educational Psychology Parent Helpline
Page 13	Dates for the Diary
	Key Dates to Remember
	Reminder

Online Safety Training for Parents - June 2022

Dear Parents'

Our Online E-safety training course for parents June 2022 is available via the link below of via the school website.

This can be carried out in the comfort of your own home at a time that suits you best! There is no time limit once you commence the training but please allow yourself twenty minutes to complete this comfortably.

Don't forget to enter your name in full at the start as once completed you will be able to download your certificate. The most up to date training link can always be found [here](#) on the school website.

[Click here to start your online safety Training for Parents – June 2022](#)

Regards
Mrs Del Giudice
Network Manager



Movie Night



Year 7 & 8 Movie Night

***Tuesday 5th July 2022
4pm – 6pm***

***Black Panther (PG-
13/12A)***

Tickets on sale until 24th June 2022

£7: movie ticket, popcorn and drink.

Refreshments on sale.

Limited to 50 places !!

Location: Conference Room

Please make payment via ParentPay. Places are limited to 50, on a first come first serve basis.

Parents/guardians in years 7 and 8 will receive a separate notification, to provide permission for the student to watch the movie. This will be issued via email. Please make payment via ParentPay before completing the permission form.

After School Activities



There are still a few places available for after school activities, starting in June.

- ♦ Dance
- ♦ Musical theatre
- ♦ Jiu Jitsu beginner
- ♦ LAMDA.
- ♦ Sweet treats 2

Please book by Friday 10th June, to secure your daughters place.

Clubs cancelled for this half term are:

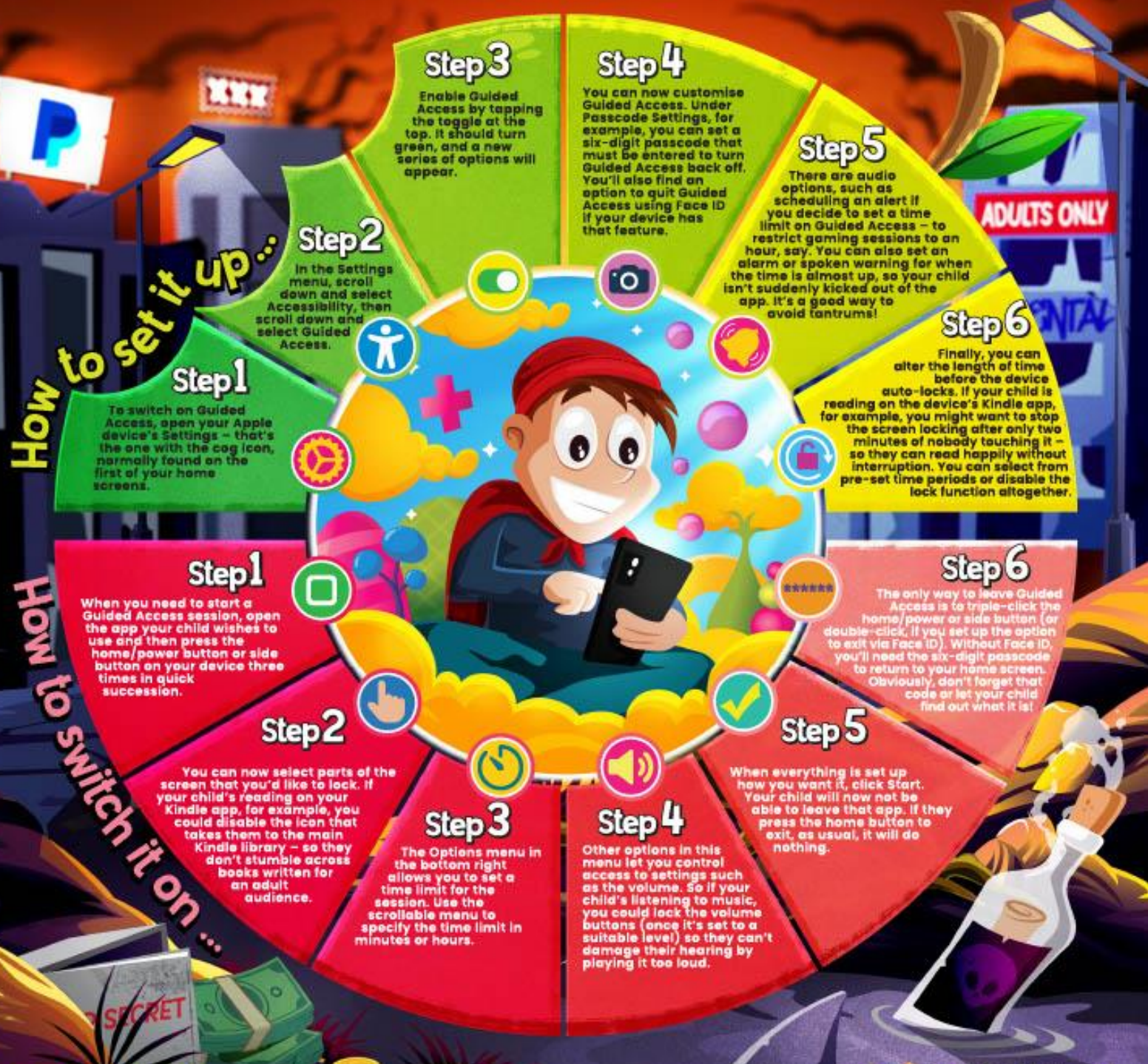
Calligraphy

Henna, Pop workshop and Drama due to low numbers

What Parents and Carers Need to Know about APPLE GUIDED ACCESS

iPhones and iPads don't offer separate user accounts. So when you hand your Apple device to a child to play a game or watch a video, you're also handing them access to your email, the web, messaging and numerous other apps through which they could accidentally do something regrettable.

Apple Guided Access solves this potential problem by letting you restrict the iPhone or iPad to one particular app whenever your child uses the device. If they try and leave that app, they will be asked for a password or Face ID, meaning they can't access anything they shouldn't elsewhere on the device. Here, we show you how to find and set up the Guided Access feature, so you can confidently let your child borrow your iPhone or iPad.



Meet Our Expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as the *Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *Newsnight*, *Radio 5 Live* and the *ITV News at Ten*. He has two children and has written regularly about internet safety issues.



SOURCES: <https://support.apple.com/en-gb/HT202612>



**National
Online
Safety®**

#WakeUpWednesday



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 13.10.2021

What Parents and Carers Need to Know about ... SOCIAL MEDIA SCAMS

On any social media platform, you'll often come across links to genuine-looking websites. They might include an exclusive offer for one of your favourite shops or invite you to complete a quiz in return for a particular reward. In some cases, clicking on these links takes you to a fake website where you are asked to provide your personal details. The whole enterprise is a ploy to capture sensitive details, such as your email address and password, which the scammers then exploit at your expense.

Clickjacking for fake rewards

Here, the attacker tries to lure you into clicking a link by offering something in return, such as a free gift for completing a survey. However, when the link is clicked, it collects the details of whoever fills out the survey. This might include full names, addresses, phone numbers and email addresses. Scammers could use these to hack into your other accounts or simply sell your data to other criminals.

Malicious app downloads

Some cybercriminals design software that appears genuine or helpful (and is normally free) but has been created to steal your personal information. There may be a pop-up ad encouraging you to download and install the app. Once the app is downloaded, the attacker can see any personal credentials you enter, and could then use this information for their own gain.

'Payment first' scams

Prevalent on sites such as Depop, these scams have spread to Facebook since it added the Marketplace feature. A user lists an item for sale and requests payment up front. Most online stores work this way, but the crucial difference is that scammers ask for payment via PayPal friends and family – not goods and services. This means you can't dispute the payment: the scammer keeps your money, and you never receive the item.

Threats disguised as quizzes

Most quizzes on social media seem harmless, but many come with hidden threats. When you submit your answers, you're also agreeing to terms and conditions which – in some cases – allow the quiz developer to sell your details to third parties. This puts you at greater risk of phishing attacks and spam advertising emails. It might also give the app permission to use information from your profile.

Untrustworthy URLs

It's common on social media for URLs in posts to be shortened (to meet Twitter's character count, for instance). This may seem harmless, but it opens an avenue of attack for scammers who may be disguising a malicious link as legitimate. These links can install malware on the victim's device, which could lead to passwords being stolen or even be the precursor to ransomware attacks.

Angler phishing scams

Using a fake corporate social media account, the scammer pretends to be from customer services. When someone complains about customer service on social media, the fake account messages them asking for their name, phone number and email. If the user provides this info, they are directed to a fake website where they enter their login details. The attacker can then steal their credentials or infect their device with malware.

Advice For Parents & Carers

Set strong passwords

Always ensure that your passwords are not easily guessable. Try to use a mix of letters, numbers and special characters so that criminals cannot forcefully get control. You should also change your passwords every so often to provide further protection against your accounts being taken over. If you have any concerns about your account's privacy, change the password.

Review your privacy settings

Regularly review your privacy settings on social media. You can restrict which parts of your profile can be seen and by who. We recommend making your personal information only visible to friends, which will help to limit the information a scammer could find out about you from social media. It's also safest to only accept friend or follow requests from people that you actually know.

Protect your personal information

Never enter personal information on unfamiliar websites. If you were redirected to a site from a social media post or an email link, putting in your personal details could give key information away to a scammer. Fraudsters may pose as someone you know to try and get your address or bank details for your family's. If this happens, block the user and tell your family, so the scammer can't try to deceive anyone else.

Avoid opening suspicious emails

When you get an email, always check the sender's address before opening it. If it's an unexpected email and the sender is a stranger, mark it as junk (in case they try again in future) and simply delete it. They could be a scammer who's simply seen your email address on your social media profile. Being aware of phishing attacks is the primary method of defence against scam emails like this.

Choose trusted download sources

Don't download apps or files from unknown sites – instead, use verified and trustworthy sources (such as Google Play or the App Store for download to mobile devices). You can recognise safe sources by their trust seals. The browser address bar on a secure site starts 'https' instead of 'http'. A shield or lock symbol in the address bar also indicates that a site is secure.

Install anti-virus software

Another key tip is to ensure that you have robust and reliable virus protection installed on any of your devices that support it. Anti-virus programmes will help to insulate you against cyber-attacks by blocking any malicious downloads or detecting any recently downloaded malware and removing it. Update your virus protection software regularly and carry out frequent scans of your device.

Meet Our Expert

Formed in 2016, KryptoKloud provides cyber security and resilience solutions to its customers. With offices in the UK, the company offers managed service operational packages including cyber security monitoring and testing, risk audit, threat intelligence and incident response.



**National
Online
Safety®**

#WakeUpWednesday

MUSIC CLUBS

	Monday	Tuesday	Wednesday	Thursday	Friday
Lunchtime	Junior Choir <i>(SF1)</i> 13:50- 14:35	Junior Band IBO <i>(SF1)</i> 13:50- 14:40	Jazz Band KHN <i>(SF1)</i> 13:25-14:15	Senior Choir KHA <i>(SF1)</i> 13:25- 14:05 Theory and GCSE/A-level support IBO <i>(SF2)</i>	Orchestra IBO <i>(SF1)</i> 13:30-14:20
After school	GCSE/A-level support IBO <i>(SF2)</i> 15:45-16:30 Brass Ensemble <i>(SF2)</i> 15:45-16:15	Chamber groups IBO <i>(SF1)</i> 15:45-16:30			

These music sessions will be on weekly, girls should bring their own instrument and no registration is required for the sessions.

PE Extra-curricular (Summer)

April - July 2022



@wchsukpe

	Monday	Tuesday	Wednesday	Thursday	Friday
Before School				Miss Runacres' Fitness Class <i>Sports hall / Dance Studio</i> 7:45 – 8:15 am	All Years Morning Mile <i>JBR – Field</i> 7:50-8:15
Lunch time (Times vary)	KS3 Netball shooting <i>Katelynn (Y12) – Top netball courts</i> 1:30 – 14:00	Running Club <i>Rachael (Y12)</i> Field/sports hall 14:00 – 14:20	Year 10 GCSE PE Theory <i>KRI - SH3</i> 1.30-2pm Year 7 & 8 Cricket <i>VJA – Sports Hall</i> 13:30-14:00	Y7/Y10 Dance <i>Anjola (Y12) – Dance studio</i> (Y10) 13:10–14:40 (Y7) 13:45–14:15 Year 9 & 10 Rounders KRI/KRU—Field Year 9 & 10 Rounders KRI/KRU—Field 13:40-14:20	All Years Athletics <i>KRI – Field</i> 13:30-14:10 Y8 Volleyball <i>JBR – Field</i> 13:30 – 14:15
After school	Y7 Rounders <i>VJA – Field</i> 15:45 – 16:45		All Years Football <i>TLE – Field</i> 15:45 – 16:45 Year 7 & 8	Year 8 & 9 Rounders <i>JBR/KRU – Field</i> 15:45 – 16:45	

Miss Runacres's Fitness Sessions

All Year groups welcome!

Will vary from:

- Legs, Bums & Tums class
- Circuits
- General fitness
- Ab attack class
- Zumba

**Thursday mornings
@7.45-8.15am**

Sports hall/Dance studio

*(Wear anything sporty & trainers
Bring a water bottle)*



The beats will be pumping!

All years welcome



CROSS COUNTRY CLUB

Date: Every Tuesday

Time: 2:00 – 2:20

Location: Go to the Sports building to meet me and get changed.

I will register you.

If it is sunny, we go to the field; if it is wet, we stay indoors.

Queries: Talk to Rachael Lam (Year 12)



New Year, New Challenge



Foster for Redbridge

020 8708 6068

fostering@redbridge.gov.uk

WWW.WOODFORD.REDBRIDGE.SCH.UK

FOLLOW US ON SOCIAL MEDIA



@WCHS_UK



@WoodfordCHS_UK

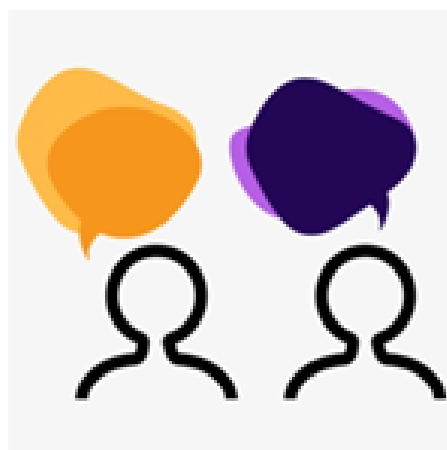


Educational Psychology Parent Helpline

Would you like to talk to someone about difficulties that you or your child are experiencing during the COVID-19 pandemic? Do you need some support with creating a daily routine for your child? Are you concerned about your child's emotional wellbeing? Are you struggling to motivate your children at home or manage sibling relationships? The Educational Psychology Service are here to support you.

The Redbridge Educational Psychology Service have a **dedicated telephone helpline for parents/carers** where you will receive advice and guidance from a professional psychologist.

The EPS helpline is available for all parents and carers - your child does not need to be known to the EPS, does not need to have a special educational need or additional support within school. We welcome calls from all parents and carers.



EPS Helpline

Telephone: 077 41 3 31 009

Opening hours:

Every Wednesday 10am - 4pm

Webpage: <https://www.redbridge.gov.uk/schools/educational-psychology-service/>



FIND: [Educational Psychology Service](#)

@Redbridge_aep Twitter account.

Dates for the Diary

SUMMER 2022		
Term	Tuesday 19 April 2022	Friday 27 May 2022
Half-term	Monday 30 May 2022	Friday 3 June 2022
Term	Monday 6 June 2022	Friday 22 July 2022
Non-Contact Day	Wednesday 29 June 2022	

KEY DATES TO REMEMBER

Week of 6 June—Internal Exams Week

15 June—Year 12 Chemistry Practical Day

20 June—UCAS fortnight begins

28 June—Year 12 Induction Day

29 June—INSET Day

1 July—Year 13 Leavers' Day

6 July—Summer Showcase

14 & 15 July—Summer Production Show



REMINDER

Please remind your daughter to bring in her lanyard, locker key and fob to school every day.

