


Hello. Lots of excellent learning and development undertaken this week, and the teaching team have really appreciated the conversations with parents and carers as part of the recent parent consultations. Thank you to everyone who participated.

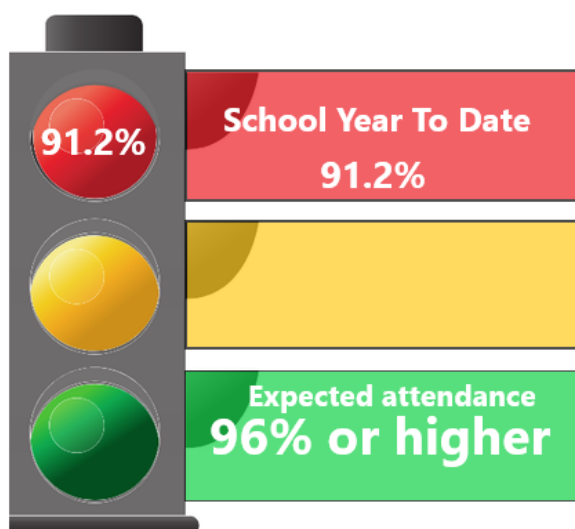


Parent/Teacher
Consultations

We are also aware of the significant changes to Covid measures and guidance from the government that come into effect on Friday 1st April, and will continue to advise families about what that means for education settings. See the update on page 2.

School Attendance - Ongoing Reporting.

The information below shows that whole school attendance for the dates between 6th September 2021 and 3rd March 2022 is currently **91.2%**, slightly down from when we reported 2 weeks ago. This is below the expected attendance rate of **96% or higher**.



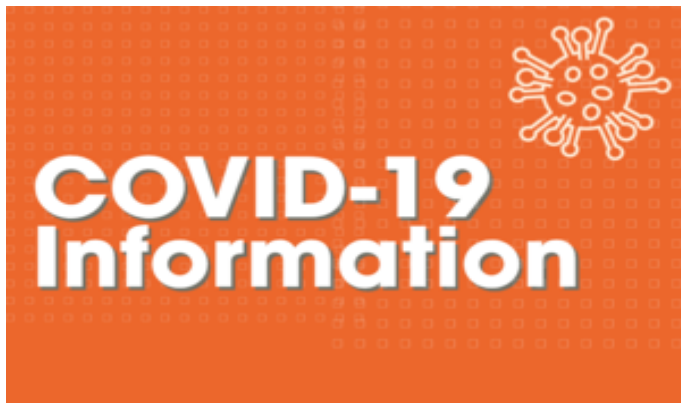
Considerate Parking. Thank you to everyone who has responded to our considerate parking appeal in the last newsletter. In that instance disabled driveways had been obstructed during drop off and collection times.

Following contact last week to school from concerned local residents can we make another parking appeal and ask families to never park on the yellow zig zag lines. Yellow zig-zag lines outside schools indicate the length of road where stopping or waiting is strictly prohibited. The Highway Code states that you should keep these areas clear of stationary vehicles, even if picking up or setting down children. Thankyou.

Holiday Activities and Food programme.

Devon County Council coordinate a Holiday Activities and Food (HAF) Programme. Its aim is to support children to eat more healthily, be more active over the school holidays and have a greater knowledge of health and nutrition. If you would like to know more about Easter holiday events in Exeter please visit the DCC website by clicking [here](#).





Changes to measures and guidance for managing COVID-19 in education and childcare settings from Friday 1 April.

On Tuesday 29th March, the Secretary of State for Health and Social Care, Sajid Javid, set out the [next steps for living with COVID-19](#) in England from this Friday 1 April. Universal testing will also end from 1st April 2022. The advice on the government website above states;

- Adults with the symptoms of a respiratory infection, and who have a high temperature or feel unwell, should **try** to stay at home and avoid contact with other people until they feel well enough to resume normal activities and they no longer have a high temperature.
- **children and young people who are unwell and have a high temperature** should stay at home and avoid contact with other people. They can **go back to school**, college or childcare when they **no longer have**

a high temperature, and they are well enough to attend.

- **adults with a positive COVID-19** test result should **try** to stay at home and avoid contact with other people for 5 days, which is when they are most infectious. **For children and young people aged 18 and under**, the advice will be 3 days.
- Regular asymptomatic testing is no longer recommended in any education or childcare setting and the school has been instructed by the Department for Education to not distribute any test kits to pupils or staff.

The government website states that the population now has much stronger protection against COVID-19 than at any other point in the pandemic. This means we can begin to manage the virus like other respiratory infections, thanks to the success of the vaccination programme and access to antivirals, alongside natural immunity and increased scientific and public understanding about how to manage risk.

Click [here](#) to see more information on the government website.

UKRAINE: FIVE WAYS TO TALK TO CHILDREN ABOUT CONFLICT



Some of our teachers have been asked about how best to help children understand and make sense of the conflict in Ukraine. In response to this need we can share the **Save the Children advice on how to talk to Children about Ukraine.**

To help with the difficult questions that children may ask, we have published a blog on our website containing the very helpful advice by Save The Children. Experts at the charity share 5 practical tools and tips that caregivers can use to approach the conversation with children. Click [here](#) to see the blog article on our school website.

What Parents & Carers Need to Know about **PHONE SCAMS**

Helpful advice for parents & carers about the increasing problem of mobile phone scams. Take a look at the info poster on page 4 of this newsletter, or check out the school blog [here](#) to be directed to the National Online Safety webpage to see the poster in more detail.

Headteacher's Award

Congratulations to Lily Croft, Cain Lee, Jaxon David and Leon Warsinski.

Key School Dates;

Easter Holidays. Monday 11th April to Friday 22nd April inclusive. First day back in school is Monday 25th April.

May Half Term. Monday 30th May to Friday 3rd June inclusive. First day back in school is Monday 6th June.

What Parents & Carers Need to Know about PHONE SCAMS

In a three-month period during 2021, no fewer than 45 million people in the UK experienced a suspicious attempt at being contacted via their mobile. Phone scams are a common form of cyber-attack where fraudsters engage directly with their intended victim through their smartphone. As our phones carry so many sensitive (and therefore potentially valuable) details about us, it's vital that trusted adults are alert to the tactics that scammers use to get access to user accounts, personal data and private information for financial gain.

WHAT ARE THE RISKS?

SMISHING

SMS phishing, or 'smishing' is one of the most common forms of mobile-based cyber-attack. Smishing is when a scammer texts their target, pretending to be a reputable person or organisation. They aim to trick the victim into supplying sensitive data such as bank details and personal information, so that they can then access the target's bank accounts and remove money.

IMPERSONATION

Fraudsters often impersonate someone else to trick the victim into actually transferring money directly. They might claim, for example, to be a friend or relative using a different number who urgently needs funds. Other common claims include sending fake texts informing the target that they have a package which requires a fee to be delivered, or that they have an unpaid bill to settle.

NUMBER SPOOFING

Here, the scammer takes impersonation one step further by cloning the phone number of a genuine company. So when the target receives a call or text, their phone recognises the sender's number as legitimately belonging to Amazon, HMRC, the NHS or the DVLA (who have all been impersonated in these cases). This makes the scam far harder to spot and the victim much more inclined to comply.

FAKE TECH SUPPORT

Attackers contact a target, pretending to work for their employer's IT support team. They then advise them to download some software to fix 'a technical issue' with their device. In reality, however, the software grants the scammers access to the victim's private data and sensitive information. This can be more common on desktop and laptop devices, but is still possible to accomplish on mobiles.

SIM HIJACKING

SIM hijacking switches control of a phone account from the victim's SIM card to one in the scammers' possession. Criminals use personal details placed together from social media (birthday, address, pet's name and so on) to pose as you, then instruct your phone network to transfer your number to their SIM - giving them access to all calls and texts meant for you, including one-time login passcodes.

Advice for Parents & Carers

DO SOME DIGGING

If you've received a call or text asking for specific information, research the caller's number. There are several websites that allow you to enter a phone number and will then display any relevant information about it - this usually includes feedback and comments from other people, so you can easily see if that particular number has been implicated in potential scams.

TRY A CALL BLOCKER

If a suspicious call comes through on your mobile, you can manually block the number if you believe it to be dubious or a nuisance caller. Alternatively, you could consider installing a call blocker service on your phone. They automatically stop calls getting through from numbers which have been reported as suspicious, halting potential scammers in their tracks before they can reach you.

VERIFY THE SOURCE

Never disclose confidential details to an individual or organisation you're unfamiliar with. If the caller claims to represent a company you trust but is still asking for personal information or payment on an outstanding charge, end the conversation. Then find the company's genuine number on a bill or on their website and call them directly to confirm if there really is an issue you need to address.

BREAK OUT THE TECH

Lots of anti-virus software now also protects mobiles. Some anti-virus apps can detect phishing links in text messages and alert you to the risk. When you're out and about, try not to use public WiFi for sensitive transactions: it's far less secure than your home WiFi network. Instead, you could consider installing a VPN (Virtual Private Network), which encrypts all data travelling to and from your phone.

REPORT INCIDENTS

If you or a family member does give out confidential information to a caller you aren't sure about, contact the actual company mentioned to check if the call was genuine. If they confirm that the call was not made by their organisation, you should report it as a potential scam via the Action Fraud website and (depending on exactly what information was divulged) consider involving the police.

BE WARY OF LINKS

If you get a message from an unknown number asking you to click on a link, report it as spam and do not open the link. One recent example 'warned' victims they'd been exposed to the Omicron variant and needed to click a link to buy a special test - only to find they had paid their money to scammers. Links can also install malware onto your device, so always treat them with extreme caution.

Meet Our Expert

Formed in 2016, KryptoCloud 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

Sources: <https://www.actionfraud.org.uk/news-centre/2021-uk-nation-people-targeted-by-scams/> & <https://www.actionfraud.org.uk/news-centre/2021-uk-nation-people-targeted-by-scams/>



www.nationalonlinesafety.com



@nationalonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 23.03.2022