

For further information on what's happening in school please go to our website [www.sandylands.lancs.sch.uk](http://www.sandylands.lancs.sch.uk)



01524 410286



head@sandylands.lancs.sch.uk Next holiday– Bank Holiday Monday 2nd May 22



Wk beg. 25.04.22

# Newsletter

## Thank you Morecambe fC



A big thank you to Morecambe Football club for our family tickets over the holidays. As you can see some of our families had a fabulous time!



## Upcoming Jubilee!

A big Happy 96th Birthday to Her Majesty The Queen. We are really looking forward to celebrating her Platinum Jubilee later on this term with a big party! Watch out for more details!



## After school clubs



After school clubs will begin this week. You will be contacted via the parent app if your child has a place on the requested club.

Oh we do like to be beside the seaside

Year 1 and 2 went on walks in our locality as part of their Geography and Year 5 have been practising their crosshatching/shading skills in their Art sessions with a trip to Morecambe bay.



## Easter Raffle

What an 'eggstraordinary' few days before we broke up! The Easter raffle took place and the children were 'eggstatic', we had a great Easter lunch. It's no yolk ... Congratulations to our winners.

A huge thank you to the generous local shops and businesses who donated to our raffle.



LTA whole school recruitment

ASDA

Whitewells LTD CATERING SUPPLIES



Morrisons



## Dates for the Diary

Bank holiday  
Monday  
2nd May 2022



# Be Safe, Feel Well

April 2022

Telephone: **01524 410286**

Email: **inclusionteam@sandylands.lancs.sch.uk**

Website: [Inclusion Team](#)

A reminder our Inclusion Team is always here to help. If you have any concerns or would like to access support, contact us.

## Attendance

At Sandylands, we aim for all children to achieve their potential in school. This means that they need to be in school, on time, ready to learn at least 95% of the time. We ask that children are punctual to school for 5 to 9, where they can access the Grab'n'Go breakfast bagel on their way in.

## Every Minute Counts...

8.45-8.55	Your child is on time for learning and can access the Grab'n'Go breakfast	
9.05	Your child will be marked as late and has missed early morning work in class.	5 minutes lost
9.30	Your child will be marked as unauthorised absence. This equates to <u>18 days</u> learning a year.	30 minutes lost



## CHATS

Call out to all Lancaster and Morecambe parents and carers supporting a child or young person with any kind of emotional or mental health problem. You are not on your own. For more information and support go through the website link below.

[CHATS](#)

## Grief Cafe

A new free monthly drop in session for anyone experiencing grief. This is a chance for reflection and to share experiences with others in a relaxed environment. Every 2nd Tuesday of the month 3.30-5 at the Courtyard Café.

[Grief Support](#)



## Online Safety

The children learn about Online Safety in school through Education for a Connected World. This month, we are looking into how to support the area of commerce. Take a look at this guidance on scams.

Website: [Online Safety](https://www.nationalonlinesafety.com)

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

# 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 cons 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 cons). 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 employers' 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 con is 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 pieced 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, 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

Sources: <https://www.bbc.com/news/health-56111111> 45 million people targeted by scammers | <https://www.actionfraud.gov.uk/blogs/news/hoaxing-new-uk-trusted-estate-fraud-scams-committed-every-5-seconds> | <https://www.which.co.uk/news/2022/03/the-five-biggest-scams-of-2021/>

[www.nationalonlinesafety.com](https://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: 23.03.2022