



# HLA News



Friday 25<sup>th</sup> March 2022

Dear Families,

What a week! I am beginning to wonder where the time is going as it is nearly the Easter holidays – time is flying past.

As you will be aware we had our first inspection from Ofsted on Tuesday and Wednesday this week. Thank you to all of the parents and carers who completed the parent view survey and spoke to inspectors during their visit. It is great to get a wide representation of views of our school. Unfortunately I am not allowed to share the inspection judgement as yet due to their internal quality assurance processes. What I will say is we were extremely pleased with the result and all of the staff are smiling. Our school self-evaluation was very accurate and the few points for development that were identified we are already working on. The report will be available to parents to read in 4-6 weeks and we will love to share this with you when we are able. There will be lots of celebrations this weekend!

This week there has been some lovely creative work taking place in Wrens and Eagles. Students have been working to keep to a steady beat and read musical notation higher up the school. Inspectors commented on strong progression in learning which is lovely to see. I must say the Woodpecker song is my personal favourite in Wrens class.

Students in S4 have been learning about data handling and how to construct line graphs. They were great at being able to recognise the features of the graph and has started plotting information. Students in S3 have also been doing some great maths learning. They have been focussing on time and there were lots of wow moments in the lesson that I saw. Great work everyone!

Thursday this week was World Maths Day. We decided to combine our flair for the arts with maths and create a mural involving lots of patterns and maths concepts. Students have been learning about tessellation and patterns. We are looking forward to being able to share the finished piece of maths artwork with you when it is completed.

As part of our school focus on strengthening our learning values with our students we are altering the way we give awards at school. There will no longer be a weekly golden book award after the holidays. We want to focus on recognising our learning values at school so will be giving certificates throughout lessons where students have identified and applied these building character. Keep a look out in your children's bags for these certificates – some have been given out already.

Thank you all for your support, it is greatly appreciated.

With all best wishes,

Yvonne Skillern

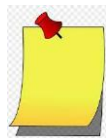
Head of School



## Golden Book Stars of the Week



- Puffins Student** for superb phonics work at the beginning of the week.
- Puffins Student** for careful independent work on Maths Day.
- Robins Student** for fantastic listening and answering questions in all areas of the Green Pathway.
- Swallows Student** for thinking hard in English to complete an independent piece of learning on verbs. He has also been using his thinking skills in reading by using his phonic knowledge to break down unknown words to be able to read them.
- S1 Student** for excellent participation in lessons.
- S5 Student** for focussing on and completing all of his priority work.
- S5 Student** for achieving Grade 4 in his GCSE maths mock.
- Wrens Student** for good engagement in group activities and using lots of speech.



### Important Information



- On 25<sup>th</sup> April 2<sup>nd</sup> Covid vaccinations will be taking place for the 5-11 year old students who had their 1<sup>st</sup> Covid vaccination back in February – please note further consent is NOT needed for the 2<sup>nd</sup> vaccination. If your child missed the first 5-11 year old Covid vaccination please contact the nursing team directly for advice t: 0300 555 5055 (option 1), e: [hct.csaiscampsb@nhs.net](mailto:hct.csaiscampsb@nhs.net)
- On 5<sup>th</sup> May MEN / DTP vaccinations will be taking place for Year 9 pupils and anyone in Year 10 who missed the vaccination due to Covid – the online consent deadline is midday 4<sup>th</sup> May. Letters have been posted on dojo with links to the portal to register.
- On 10<sup>th</sup> May HPV vaccinations are taking place for Year 8 students and anyone in Year 9 and 10 who missed the vaccination due to Covid – the online consent deadline is midday 9<sup>th</sup> May. Letters have been posted on dojo with links to the portal to register.
- Can I remind everyone that we are nut free school. If students bring products in containing nuts it will be necessary to confiscate them for the health and safety of all our learners.
- Secondary aged students please don't forget to test twice weekly and report results to [Covid.HLA@highfieldlittleport.org](mailto:Covid.HLA@highfieldlittleport.org) as well as the government website. The last batch of testing kits have now been distributed. As a school we are no longer able to order any more supplies unfortunately.
- Please remember that if your child is unwell or tests positive please keep your child off school to minimise transmission.
- Please see class dojo for a link to complete an online parent views survey. Your thoughts are very important to us and we want to take them on board to help us to continually improve. If you would like a paper copy please let us know. This survey will be open until the end of next week.





## Online Safety Tip of the Week:

# 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 2018, 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.

**NOS National Online Safety**  
#WakeUpWednesday

## Mental Health Tip of the Week:

Notice if you're feeling stress in your body. It might be a cue to take care of yourself.

