



St Ives Primary School,
Sandy Lane,
St Ives,
Ringwood,
Hants
BH24 2LE

Tel: 01425 475478
Email: office@stivesprimary.com
Web: www.stivesprimary.com
Company number 9809895
Headteacher: Mrs L Crossley

Newsletter 32 – 21st May 2021

Article of the Month 24 – Health, Water, Food, Environment

You have the right to good food and water and to see a doctor if you are ill.

Class News

- Nursery - have been enjoying watching the final stages of the MUGA be completed and have embraced their inner builders whilst exploring soil in the mud kitchen.
- YR - have been exploring materials to build houses that the big bad wolf can't blow down!
- Y1 - have loved learning about deciduous and evergreen trees and comparing their leaves in science.
- Y2 - have really enjoyed investigating habitats and hunting for mini-beasts in the nature area.
- Y3 - have enjoyed coding their own animations using Scratch.
- Y4 - have had great fun planning our own science sound experiments.
- Y5 - have enjoyed learning about the development of underground railways and how they transformed lives for those who accessed them.
- Y6 - have enjoyed finding out about the origins of the Ancient Greek Olympics and have made comparisons to the modern day Olympic games.

Dear Parents,

We have been working hard on showing respect to one and other this week and using our manners, lots of 'Wow' slips have been handed out, well done to all the children! In our assembly we have discussed the G7 Summit learning all about it and why it is so important. Some great learning and lots of debating ideas!

Books

Do you have books that your children have grown out of? Would you be happy to donate these to school? If so, our classroom libraries could really do with some more reading material. Thank you in advance!!

Football Kit

We are missing four school football kits, navy tops and shorts and socks. If you have one these need to come back into school. Thank you.

Swimming

The children will be starting their swimming on Monday 24th May. We would encourage children swimming first to wear their swim suits under their school uniform so they are ready to start ASAP.

Rash vests can be worn for sun protection and warmth. Please ensure your child has a swim hat and goggles if that is what they normally wear.

Swimming times – these are subject to change.

KS1

	Tuesday & Thursday
09:15	R
10:00	R

10:45	Yr2
12:45	Yr1
1:30	Yr1

KS2

	Monday		Friday
08:45	Yr5	08:45	Yr5
10:00	Yr4	09:40	Yr3
11:15	Yr6	10:30	Yr4
1:15	Yr3	11:20	Yr6

School Gates (after half term)

After half term our school start and finish times will be changing back to our normal times. Please note all KS2 will start at 8.40am and finish at 3.15 with all of KS1 starting at 8.50am and finishing at 3.05pm.

Gate	8.40am	8.50am	9.00am
Pedestrian		Reception	
1	Year 4	Year 1	
2	Year 3	Reception	Nursery
3	Year 5	Year 1	
4	Year 6	Year 2	

Gate	3.00pm	3.05pm	3.15pm
Pedestrian		Reception	
1		Year 1	Year 4
2	Nursery	Reception	Year 3
3		Year 1	Year 5
4		Year 2	Year 6

Internet Safety

Research suggests that around 1 in every 10 emails sent each day are bogus. From dummy websites resembling the real thing, to concealed malware, to messages alerting you of a 'problem' with your account, online fraudsters continue to invent plausible ways to access your personal information. The attached guide about email scams provides information on how to spot them and how to react safely to them.

Nursery

Nursery are in need of socks and trousers, any donations would be much appreciated.

PE Kits

Tuesday - Sporty Tuesdays are to continue for all. Reception - Y6 – Full PE kit

Wednesday - Year 3 & 4 – Full PE kit and shin pads

Friday – Year R, 1, 2, 5 & 6 – Full PE kit

Year 3 & 4 – School Uniform and trainers

Dates for the Diary:

May

w/c 24th - Swim assessments

31st May - 4th June – Half term

June

7th - Swimming lessons start

15th - Reception parent meetings

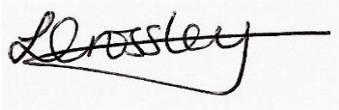
22nd - Climbing wall

July

5th - Whole school transition day

16th - Last day of term

Yours sincerely



Mrs L Crossley
Headteacher



What Parents & Carers Need to Know about EMAIL SCAMS

Email scams are when you receive a mail from someone purporting to be a genuine person or company, but is actually an online fraudster trying to trick you into disclosing personal information. This is often referred to as 'phishing'. Normally, people click on the links in an email assuming that they will be directed to a trustworthy website – but fake sites, closely resembling the real thing, are increasingly being set up by cyber criminals specifically to capture your personal information, which could in turn jeopardise your financial, emotional and possibly even physical wellbeing.

Disguised Deceptions

Some scam emails can appear to be from companies that you know and use. For example, you could receive an authentic-looking email advising of a problem with your account or payment method. Instead of reacting to the email and disclosing personal information like bank details, it's wise to call the company directly on a trusted number to confirm if there actually are any account issues.

Identity Theft

Another significant risk is falling victim to identity theft. If a scammer manages to acquire your usernames and passwords, they would then have access to your online accounts – and they could effectively pretend to be you. This could have a massive negative impact if changes were made to your accounts, for instance, or the scammer communicated with your contacts while posing as you.

Viruses and Malware

A particularly devastating hazard with scam emails is that some links, when clicked on, could result in dangerous viruses or malware being downloaded onto your devices. This could enable scammers to harvest valuable information without your consent (and sometimes even without your knowledge) or prevent you from accessing the device altogether, making it unusable.

Financial Damage

One of the primary consequences for victims of an email scam is the financial cost. If you do click on a scam email and disclose any personal information, it can then be used to take money from accounts belonging to you and your family. Depending on exactly what information the cyber criminals obtain, this could result in significant and far-reaching financial losses and personal stress.

Hijacked Accounts

A scammer with access to your accounts could – once they're logged in as you – deny you entry. If they were to change the password, it would – in most cases – not allow you any further access. Even for accounts with little or no financial value attached, this could be hugely inconvenient: you could permanently lose data and files that you had invested a considerable amount of time in.

Personal Safety

Another danger of scam emails is that, in extreme cases, they could ultimately lead to a threat to your physical wellbeing. If someone is demanding to meet with you and has accessed your personal information (your address, for example), they could attempt to confront you in person – which is of course exceptionally dangerous. Losing control of sensitive information could put you in a vulnerable position.

Advice for Parents & Carers

Protect Personal Details

Never input any personal information into websites that you are unfamiliar with. If you were redirected onto a certain page by clicking a link in an email, entering your personal details could then give away your location or other key information to the scammer. This could then put you in physical danger as the cyber criminals would know exactly where to find and approach you.

Beware of Suspicious Emails

If you are unfamiliar with the sender, it's safest to simply not open an email. When an email makes you wary, mark it as junk (to reduce the chance of any recurring issues) and then delete it. Awareness of phishing is the primary method of defence against malicious emails. Once someone knows how to identify and deal with scam emails, they are far less likely to fall prey to them in future.

Check Spelling and Grammar

Pay close attention to any spelling mistakes or grammatical errors. Many scam emails can be spotted this way, as they often tend to contain these types of mistakes. Make sure your child knows that if they do spot this sort of tell-tale error and is not sure who the email came from, it's a good idea to either delete the email or report it to a trusted adult to prevent any possible future harm.

Access Sites Manually

If you or your child wish to visit a particular website, it's safest to avoid clicking on a link in an email to take you there. Instead, find the site through your search engine or manually type the address into your browser. This significantly reduces the possibility of being redirected to a bogus website where fraudsters could capture your personal information after you enter it.

Don't Open Dubious Attachments

If you or your child ever see any files as attachments on emails that you are uncertain about, do not download them or even click on them: this could result in your systems being infiltrated. If your devices at home do not already have anti-virus software, you should install some and ensure it is regularly updated. This will help you to detect and remove any dangerous files as soon as possible.

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.



NOS National Online Safety®
#WakeUpWednesday

SOURCES: <https://www.infosecurity-magazine.com/news/education-disproportionate-spear/>, <https://www.impactm.biz/blog/cybersecurity-in-education-stats-2020/>