



www.stocksbridge-jun.sheffield.sch.uk

Issue No. 475

21/05/2021



Yesterday was World Bee Day, a subject close to our hearts at SJS as we eagerly await the arrival of a new swarm of bees for our school apiary.

Having bees at school allows the children to learn firsthand about their importance to our environment and food chain. Without bees, our supermarkets would only have half the fruit and vegetables that are currently available.

In the same way that a single bee could not create honey on its own, in school teamwork really does make the dream work. We stress the importance of supporting each other, being positive and, most of all, being kind. Like the bees, it is only by working together that we will succeed.

SJS STARS OF THE WEEK

- Y3AH: Mason Bonner
- Y3CP: Harry Clancy
- Y3RD: Harry Hanson
- Y4KT: Shannon Taylor-Cuss
- Y4RL: Liya Sudak
- Y5CS: Luke Warnock
- Y5DW: Erin Fox
- Y5HK: Eve Horsfield
- Y6ER: Taylor Millard
- Y6MC: Callum Ejogbamu
- Y6CH: Tao Pawson

Mrs Foster: Miley McCoid
Mr Tee: Lucy Martin

Lower School Lunchtimes: Millie Turner
Upper School Lunchtimes: Belle Carr

READING AROUND THE WORLD

Y3 - LONDON

Harley Steel

Y3 - PARIS

Kie Langley

Y3 - MADRID

Sarah Radford

Y3 - ROME

Noah Charlesworth
Priya Marshall

Y3 - BERLIN

Niamh Siddall
James Reed
William Powell
James Gourley

Niall Pritchett
Ellie-May Murray
Kate Blake

Y4 - RIYADH

Griffin Williams

Y4 - MOSCOW

Holly Swales
Violet Merrywest
Imogen Goddard

James Kelland
Alfie Jackson
Eloise Ruddlesdin

Y5 - WELLINGTON

Jake Crooks

Y6 - BRASILIA

Daniel Senior

Y6 - LIMA

Mika Butcher
Maisie Peacock
Daniel Senior

PARENTAL CONSULTATION

Early next week, we intend to share with parents a letter which explains our reflections with regards to arrangements for school timings. Following this we will be asking parents for their views on the two options we will be proposing. Please take some time to consider the information in the letter which we hope will enable parents to make an informed decision when contributing to the consultation.


NON-UNIFORM DAY

Children are welcome to come to school in their home clothes next Friday for a £1 donation.

BEARS OF SHEFFIELD

We have very nearly reached our fundraising target! To get us over the line, please ensure your child has entered our Bear Lotto which will be drawn next Friday!

NEXT WEEK'S SCHOOL DINNER MENU

WEEK 3 8/3-29/3-3/5-24/5-21/6-12/7	MONDAY <small>MEAT FREE</small>	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
MAIN DISH	Pizza of the day	Sausages and gravy	Roast chicken with Yorkshire puddings	Spaghetti Bolognaise 	Fish fingers
VEGETARIAN MAIN DISH	Pizza of the day	Quorn™ sausages with gravy	Vegetarian toad in the hole	Vegetarian spaghetti Bolognaise	Fish fingers
ACCOMPANIMENTS <small>5 ADAY</small>	Herby potatoes Seasonal vegetables Salad bar	Mash potato Seasonal vegetables Salad bar	Roast potatoes Seasonal vegetables Salad bar	50/50 pasta Seasonal vegetables Salad bar	Chips Seasonal vegetables Salad bar
DESSERTS	Cheese, crackers, and grapes	Sticky toffee muffins	Ginger biscuit with fresh fruit	Shortbread biscuit with mandarins <small>5 ADAY</small>	Fruit with ice cream <small>5 ADAY</small>
FRESH FRUIT & YOGHURT	Fresh fruit and yoghurt	Fresh fruit and yoghurt	Fresh fruit and yoghurt	Fresh fruit and yoghurt	Fresh fruit and yoghurt
JACKET POTATOES	Jacket potatoes with cheese, beans or tuna	Jacket potatoes with cheese, beans or tuna	Jacket potatoes with cheese, beans or tuna	Jacket potatoes with cheese, beans or tuna	Jacket potatoes with cheese, beans or tuna

SJS COVID-19 WEBPAGE

Our webpage ensures parents can access to the latest COVID information from school and Sheffield news and resources. Please visit <https://www.stocksbridge-jun.sheffield.sch.uk/covid-19-parent-information/>

					
Keep a safe distance from others	Wash your hands regularly, for 20 seconds	You must wear a face covering in enclosed spaces if you can	No one in your house should leave home if any other person has symptoms	If you have symptoms, stay at home and book a free test - visit NHS.uk or call 119	Reduce the number of people you have contact with

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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

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, 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.



SOURCES: <https://www.infosafety-magazine.com/news/education-disparities-are-real/>, <https://www.pactry.com/blog/cybersecurity-in-education-2019-2020/>



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: 18.05.2021