ST. JAMES' (C OF E) JUNIOR SCHOOL

Every Child, Every Chance, Every Day.

WEEKLY NEWSLETTER

FRIDAY 6TH DECEMBER 2024

A LASTING LEGACY...

Everyone at St. James' Junior School was deeply saddened to hear about the passing of one of our former teachers, Rhoda Salisbury. Rhoda worked at school during the 1990's and was passionate about the arts, especially music. She was a keen pianist and often led hymn practice in the school hall. Rhoda's legacy for inspiring children through music will continue, thank you to her children Hazel, Jonathan and Alistair, who have very kindly donated her piano to school. We look forward to being able to share some 'live' music performances with parents soon.

ADVENT SERVICE...

On Thursday 5th December, we held our Advent Service at Ozzy Road Church. As always, it was so special to celebrate at church and we thank the team at Ozzy Road for welcoming us. A huge thank you to all the parents who came along too, it was great to see you.

CHRISTMAS JUMPER DAY...

On Thursday 12th December, children can come to school wearing Christmas jumpers. Children must wear normal uniform bottoms and school shoes, but can wear a festive jumper if they wish.

CHRISTMAS DINNER DAY...

It is Christmas Dinner Day on Thursday 12th December. Children can have a Christmas Dinner for the same price as a normal school dinner (£2.35) and this can be paid for via ParentPay. Children who are entitled to free school dinners do not need to pay.

INSET DAY...

A reminder that school is closed to children on Friday 20th December. Children will finish at 3:15pm on Thursday 19th December and will return to school on Monday 6th January.

Don't forget that Breakfast Club starts at 8am and is completely free! All children must be in school by 8:45am.

Golden Book

This week's theme for the Golden Book is 'Someone who makes the most of every opportunity.'

This week's winners are:

3H	Lucas & Maryam
3W	Jeremy
3/4K	Saif
4A	Inayah
4B	Ramin
5F	Ife
5R	Emmanuel
5/6B	Hajra
6F	Raheem
6Q	Daniel

A huge well done to all this week's winners.

HEADTEACHER'S AWARD

'You have planted them, they have taken root, watch them grow and bear fruit.' - Jeremiah 12:2

Have an amazing weekend!

Mr. Walls

12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

As a society, we're increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off; streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops ... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It's essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS 'CYBER RESILIENCE?'

*Cyber resilience focuses on three key areas: reducing the **likelihood** of a cyber attack gaining access to our accounts, devices or data; reducing the potential **impact** of a cyber incident; and making the **recovery** from a cyber attack easier, should we ever fall victim to one.*

1. PASSWORDS: LONGER AND LESS PREDICTABLE

The longer, less common and predictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre's 'three random words' guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS

When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you've signed up for. If cyber criminals gain access your username and password for *one* site or service, they'll definitely try them on others.

3. USE A PASSWORD MANAGER

A good way to juggle different passwords for every site or service you use is to have a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, 1Password and Keeper are all excellent password managers.

4. BACK UP YOUR DATA

Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it's extremely important or sensitive information, you could even decide to keep more than one back-up version – by saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they *do* manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY

Some services let you set 'recovery questions' – such as your birthplace or a pet's name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals' task far harder.

7. SET UP SECONDARY ACCOUNTS

Some services provide the facility to add secondary accounts, phone numbers and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you're having trouble logging in or if you're trying to take back control of your account after a cyber attack.

8. KEEP HAVING FUN WITH TECH

Consider our tips in relation to the gadgets and online services your household uses. Protect yourself and your family, and don't let the bad guys win: devices are not only integral to modern life but also a lot of fun – so as long as you keep safety and security in mind, don't stop enjoying your tech.

9. CHECK FOR BREACHES

You can check if your personal information has been involved in any known data breaches by entering your email address at www.haveibeenpwned.com (yes, that spelling *is* correct!). It's useful if you're worried about a possible attack – or simply as motivation to review your account security.

10. CHANGE DEFAULT IOT PASSWORDS

Devices from the 'Internet of Things' (IoT), such as 'smart' home appliances, are often supplied with default passwords. This makes them quicker to set up, but also less secure – criminals can identify these standard passwords more easily, so change them on your IoT devices as soon as possible.

11. KEEP HOME DEVICES UPDATED

Download official software updates for your household's mobile phones, laptops, consoles and other internet-enabled devices regularly. Security improvements and fixes are a key feature of these updates – so by ensuring each device is running the latest version, you're making them more secure.

12. STAY SCEPTICAL

Cyber criminals commonly use various methods, including emails, text messages and social media posts. Be cautious of any messages or posts that are out of the ordinary, offer something too good to be true or emphasise urgency – even if they appear to come from someone you know.

Meet Our Expert

Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.

Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word | https://haveibeenpwned.com

National Online Safety®
#WakeUpWednesday