Autumn Term 2024-25 Issue 9 Friday 8th November

This half-term, our core value is **RESPONSIBILITY**

Dates for the diary

Remembrance
Monday 11th November

Rocktopus Dance
Wednesday 20th November at Axminster Primary

Pantomime (tbc)
Tuesday 17th December

Christmas Lunch
Wednesday 18th December

Charlie Pig Storyteller
Thursday 19th December at Axminster Primary

Christmas ~Jumper Day
Friday 20th December

Christmas Service
Friday 20th December 3pm in the church

News

Welcome back to a new half-term. We have started off the half-term with firework related challenges! In history, KS1 started learning about the Great Fire of London by comparing past and present London while KS2 learnt about how the Roman Empire spread. In English, KS1 are learning to write instructions and KS2 have started working towards writing a finding tale with a focus on including dialogue.

Remembrance
On Monday, it is Remembrance Day. Year 5/6 will be representing the school at the Minster in Axminster while the rest of the school attends the gathering at the War Memorial in Membury.

Online safety
Online safety is always something we are teaching the children. There is a useful guide on the next page about building cyber resilience at home.

Reading at home
Reading at home everyday will help your children in many ways. Please record any reading in the yellow reading record. Older children can read to themselves and talk about what they have read.

Computing/coding club
This will be held on the following Thursdays this half-term: **Thursday 14th November , Thursday 21st November and Thursday 28th November.** Unfortunately we are unable to offer more this half-term due to staff training. Please let the office know if your child will be attending the club.

Miss Wickens

Amazon Wishlist https://amzn.eu/2S4J0FJ
Thank you for all the donations so far. We are aiming to improve our outside area to include a writing zone - we have a writing bench and would love some resources to make a special area.

Membury Star

Well done Oskar for showing our value **INDEPENDENCE** in his recall of how Rome was founded and understanding what an empire is.

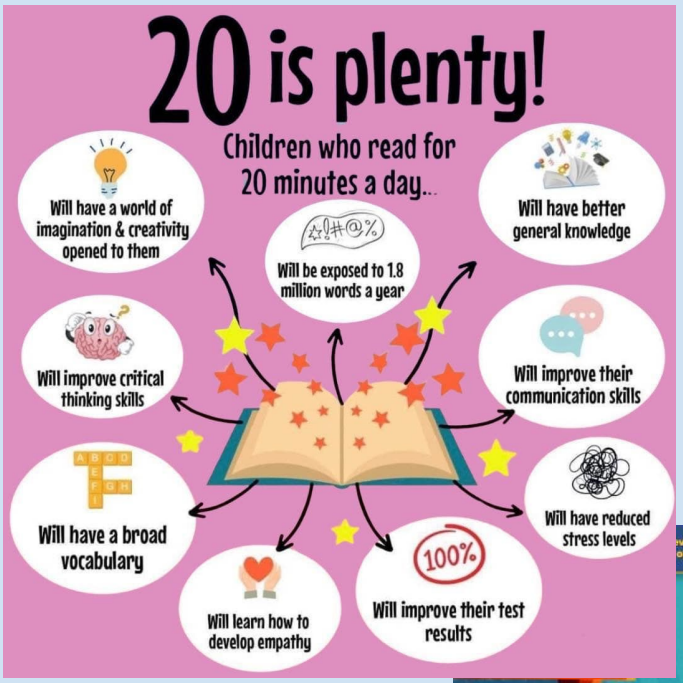
Thought of the Week

Weekly Attendance

Our attendance this week is 100%

Our attendance since September is 93.91%

Our target is 97%.


20 is plenty!
Children who read for 20 minutes a day...
Will have a world of imagination & creativity opened to them
Will be exposed to 1.8 million words a year
Will have better general knowledge
Will improve critical thinking skills
Will improve their communication skills
Will have a broad vocabulary
Will have reduced stress levels
Will learn how to develop empathy
100%
Will improve their test results


we in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.
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.
RESILIENCE MAN
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.
National Online Safety
#WakeUpWednesday
Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word | https://haveibeenpwned.com
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: 25.01.2023