School News

01304 611360   www.eastry.kent.sch.uk
headteacher@eastry.kent.sch.uk

No. 19
2nd February 2023

DATES FOR YOUR DIARY

Friday, 3rd February - Inspire Day - NSPCC Number Day

Children may come to school dressed in a number/maths related themed costume if they wish for a suggested donation of £1. There will be raffle tickets for sale to win a maths game at £1 per strip, and we will be running 10p stalls for the children to take part in. All monies raised will be donated to the NSPCC.

Friday, 3rd February - Year 6 Leaver's Party Parents' Meeting at 2.00pm in the Library

Parents and carers of children in Year 6 are invited to the first meeting to discuss arrangements for the Year 6 Leaver's Party for their children.

Monday, 6th February - Parents Support Group Meeting in the Library at 2.30pm

Parents and carers are invited to join us for a get together with other parents and carers for an informal chat over tea/coffee and cake.

Tuesday, 7th February - E-Safety Day

Thursday, 9th February - Founder's Day Service at St. Mary's Church at 9.30am

Parents and carers are invited to join us for our Founder's Day Service on Thursday, 9th February at 9.30am at St. Mary's Church in Eastry.

Thursday, 9th February - Year 3 & 4 Swimming at the Duke of York's Royal Military Swimming Pool - LAST LESSON

Friday, 10th February - Open Classrooms 3.00 to 3.20pm

Parents and carers are invited to visit their child's class from 3.00 to 3.20pm to see some of the work they have done this term. You are then asked to leave the classroom at 3.20pm and wait on the playground for the children to be dismissed at 3.25pm

INTERNET/ONLINE SAFETY SECTION

E-Safety Week

Tuesday, 7th February is E-Safety day. During next week children will continue their learning about on-line safety which they will share with other year groups during our special worship on Friday, 10th February. Attached to this School News we have included '12 Top Tips for Building Cyber Resilience at Home' which you may find useful when thinking about internet security in your home.

OTHER SCHOOL NEWS

Cake Sale for Starfish Malawi

On Friday, 24th February, as part of our links with Starfish Malawi, we will be holding a cake sale after school to raise money for our partner school, Kaphatenga Primary School in Malawi. It will follow on from a worship that the children will have had that week about the charity. The cake sale will be run by the school council and **we would be grateful to receive donations of cakes and biscuits on the day for the sale.**

SCHOOL WEBSITE

On-Line Safety Help and Support

Our school website has lost of useful tips, information and links to help you to keep you and your family safe on-line which can be used to support the children's learning about internet safety next week. On this page we have gathered together many useful links to various support guides specifically aimed at primary school aged children. There are links to the major games console providers such as X-Box and Nintendo for advise on how to set up parental controls. We also have links to various on-line safety quizzes for children, and social media guides for parents.

If you have any concerns about your child's safety on-line please do let us know.

OTHER NEWS

Covid Vaccine Update

The autumn booster dose for those who are 50+, immunosuppressed and everyone **(including 12- to 17-year-olds**) who live in a household or are in regular contact with someone who is immunosuppressed offer closes 12 February 2023. If you are in this category, wish to have the booster but haven't yet taken up this offer, please ensure this is arranged before the deadline.

AFTER SCHOOL CLUBS **Week commencing 6.2.2023**	
MONDAY	
Ballet (3.30 to 4.15pm)	**Yes**
TUESDAY	
Dance Club (3.30-4.30pm)	**Yes**
Home Learning Club (with parent) (3.25-4.00pm)	**Yes**
WEDNESDAY	
Creative Station (3.30-4.30pm)	**Yes**
Netball Club (3.30-4.15pm)	**Yes**
THURSDAY	
Singing Club (8.00-8.35am)	**Yes**
Multi-Sports Club (3.30-4.30pm)	**Yes**
FRIDAY	
Football Club (3.30-4.30pm)	**Yes**

Kind regards

SMoss

Mrs Sarah Moss
Headteacher

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 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.

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.

NOS 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