

NEWSLETTER

Thursday 30th March 2023

SPRING 2 TERM

A word from the Headteacher

Hello everyone

The end of the spring term has arrived, and this newsletter continues to highlight the rich and engaging curriculum and personal development opportunities the children have had over the last couple of weeks.

I would like to say goodbye and thank you to Miss Caple, who has been undergoing her final school experience placement in Oak Trees class this last term. Miss Caple has been a great asset to Leavening School and on behalf of the staff and children, I would like to wish her all the very best and thank her for making such a positive contribution to our school during her time here.

The extra curricular clubs have been well attended this half term with over 65% of our pupils engaging in these. Thank you for encouraging your child/ren to attend and a special thank you to the staff who have run these clubs this half term. As mentioned in my previous correspondence regarding feedback from the parent survey, our extra curricular clubs will run again in the second half of the summer term. Due to small staff numbers, we have the capacity to run a wider variety of extra curricular clubs every other half term, equating to once a term. Details of the summer 2 term clubs will be send out towards May half term.

May I wish you all a very lovely Easter holiday and we look forward to welcoming you back to the summer term.

My best wishes

Sian Mitchell

Don't forget it is a staff training day on Monday 17th April Pupils will return on the 18th April

Reminder of our exciting Easter Day on Friday 31st March Please join us for a fun morning! Easter egg design competition. f1 entry. Payment via ParentPay. Prizes to be won! There will three class categories for Acorns, Conkers and Oak Trees. 9am-9.30am- Easter café with tombola 9.30-10.15am- Spring Concert 10.30-11am- Egg rolling/Playtime (parents to join) 11am-12pm- Easter Crafts in class Please let the office know if would like to sign up to join your child in their classroom for the Easter Crafts session. School Attendance

Last week our school attendance was 88.3% This is <u>below</u> the primary national average attendance of 94.5% Attendance **this week** so far: **95.2%** Attendance **this term** so far: **93.7%**

DIARY DATES MARCH

Friday 31st

Easter Day Last day of term

<u>APRIL</u> Monday 17th Staff training day **Tuesday 18th** Start of term **Thursday 20th** Pop-up library in school FOLS Meeting 2.15pm Monday 24th Nursery library visit- details to follow

<u>MAY</u>

Wednesday 3rd Quick Rounders Tournament YR3&4 Friday 5th Coronation Celebration Day Wednesday 10th Acorns visit to Woldies Lavender Thursday 11th

Pop-up library in school Wednesday 24th School photographer in Thursday 25th Pop-up library in school

<u>JUNE</u>

Thursday 15th Road safety day Pop-up library in school **Tuesday 20th&Wednesday 21st** Norton College Y6 Transition Days **Wednesday 21st** Rounders Tournament KS2 **Wednesday 28th** Malton School Y5 Experience Day **Thursday 29th** Pop-up library in school

<u>JULY</u>

Wednesday 5th

Summer Sports Tournament KS1 Rounders Tournament (mixed) Friday 7th FOLS Summer Sausage Sizzle 3.30pm Thursday 13th Pop-up library in school FOLS Summer Disco 5.30-7.30pm Friday 21st Last day of term

SAFETY IN THE CURRICULUM Fire Safety Day

The recent fire safety day (minus the fire fighters and their engine as planned, due to an emergency call out) enabled the pupils to have a focused afternoon on fire safety. The pupils learnt about preventing fires in the home, importance of fire safety, use of smoke alarms, stop drop and roll and how to respond in the event of a fire at home. The KS2 parents were encouraged to come home and discuss with their parents and carers, an emergency escape plan for their home in the event of a fire. We are pleased that the firefighters have scheduled to come back and visit us after Easter.

Medicine Safety

Pupils in EYFS and KS1 have been learning about medicines and how they can help us and what to do if they come across medicines. They enjoyed role playing and giving the teddies pretend 'medicine'. The key message from this learning was that medicines should only be given by a trusted adult.

WhatsApp

Please find below some useful guidance about the appropriate use of and legal guidance around WhatsApp which may be of particular use to parents of pupils with access to mobile phones and tablets in KS2. It is our responsibility to ensure our pupils are educated about online safety in the curriculum and we believe that parents play a key role in this too. <u>Our school website</u> has lots of useful links to support parents in online safety and so please do refer to these if needed.



What is WhatsApp?

WhatsApp is a free messaging app. It allows you to send text and multimedia messages (video, images and voice recordings) to people in the contact list on your phone. It also allows users to set up group chats where the administrators can invite up to 256 people to share messages and images publicly within the group. Although the age limit for WhatsApp was recently raised to 16 it is popular with primary age children and above. So what are the risks?

Safety Tips



As with all Internet activity, talk to your child about how they use WhatsApp and any issues they have encountered.



With your child, look through the groups they are members of and discuss any areas of concern you have. You may agree that it would be best to leave the group.



Go to the settings (by pressing the three dots in the top right of the screen) and ensure your child's profile is set to 'contacts only'.



To leave a group: Open the group in WhatsApp. Press the three dots in the top right of the screen and select 'Group Info'. Scroll down to 'Exit group'.



If an admin adds your child back into a group they have left, your child can ask them not to do this. If they keep adding them then you can prevent it by blocking the admin. To do this, WhatsApp provide the following guidance:

1. Go to the group in WhatsApp, then tap or click the subject of the group.

- 2. Tap or click the phone number of the admin you wish to block.
- 3. If prompted, tap or click Message {phone number} or Send Message.
- 4. A blank chat with the admin will open up. Tap or click the phone number at the top.

Reasons for concern

Group administrators can invite people your child does not know into group chats. Some of these people may not have innocent intentions or may be older and post age-inappropriate messages.

Some WhatsApp groups can contain images and messages which can cause distress to children. These might include violent images or videos, abusive messages and sexual content.

Chain messages are often shared through WhatsApp. These pressure children to post them on to their contacts, e.g. by claiming that failure to do so can

result in the child or a family member dying. Many children find such messages distressing but also feel they must share them with others due to fear of the threat. and killed him. A girl named Loran got this message. She laughed and deleted it. I later came to her house and killed her and buried her in a desert. A boy named

WhatsApp does not allow users to decide whether to join a group. Your child will be automatically added to any groups that their contacts add them to. If your child leaves the group the administrator can add them straight back in.

Your child may be in WhatsApp groups in which huge numbers of posts are made. The alerts this generates can be an unnecessary distraction and can disrupt sleep.

WhatsApp's default privacy settings are that anybody can see your child's profile photo and when they were last online.

WhatsApp 'dare games' have become popular with children. These involve the child making a quiz about themselves to share with others and this can lead to oversharing of personal information which can be publicly available.



Children can add and then remove other children from groups as a form of exclusion and bullying.

Recent highlights from across school Cafe Leavening

On Friday 17th March the whole school thoroughly enjoyed the French breakfast cafe. They travelled by Eurostar down the corridor to Cafe Leavening. They all spoke in French to order their food. Oak Trees class served each other and used euros to pay for their choices. It was a great success. Merci beaucoup for all the amazing French food and drinks that were sent in, c'etait magnifique!



FoLS Update

Thank you to all those who supported the recent FoLS Bingo night!

After expenses, we raised a fantastic **£84.28!** This is a great result. A huge thank you to everyone who supported the event and to those who helped on the night.

The Easter Movie afternoon this week raised a brilliant £72 and was very much enjoyed by the children. The next FoLS meeting to discuss proposed fundraising events for next term, will be:

Thursday 20th April at 2.15pm. All welcome!

Football Tournament

On Wednesday 22nd March, the Key Stage 1 football team participated in a local schools football tournament at Malton Sports Centre.

The team played fantastically and duly earned themselves a place in the semi-finals for their tremendous efforts! Well done everyone!



Oak Trees highlights



Oak Trees had a fantastic **Roman Experience Day** with Roman Ron! They learnt so much and had opportunities to handle many different artefacts.

Oak Trees enjoyed building shelters in Forest School this half term and developing their skills of collaboration, knot tieing and whittling.



Nursery highlights

As part of Nursery's 'My local area' topic, Acorns have been exploring Leavening, visiting the Church and even taking the Guinea Pigs for a field trip to the park.

Whilst exploring we even found some chocolate eggs from the Easter Bunny!



Damson jam will be on sale for £3 a jar made by Miss Cooke (the damsons were all picked by children in Acorns).

All proceeds will go towards the outside areas. Thanks for your support!

Donation plea for Acorns Nursery/Gardening Club

Miss Cooke would be very grateful for any donations of: jam jars with lids | bird seed (loose please) compost

Thank you in advance if you can help!

Conkers highlights

Children in Conkers class have been busy working on number recognition. They were set the challenge of placing the correct number of petals on the flower stem to match the number.



THORPE BASSETT FUN RUN

IN AID OF THORPE BASSETT CORONATION CELEBRATION FUND.

5k - Walk, Jog or Run Sunday 16 April 10.00am for 11.00am start

Starting from the Centre of Thorpe Bassett up to Rowgate and back across the Common

REFRESHMENTS PROVIDED



For entries, please email or textStuart.richardson@clawson.co.uk07860 528836stuartjgardiner@btinternet.com07854 402941

<u>Entry fee</u> Adults £10.00 Under 16's £5.00

Ten top tips for **STRONGER PASSWORDS**

Passwords continue to be the most common way to prove our identity online. A combination of a username and a password known only to the user provides access to our online accounts and data - and hopefully keeps unauthorised individuals out. As a security measure, though, passwords are relatively weak. People are often predictable in how we choose our passwords, for example – making them less secure. With increasing volumes of usernames and passwords being leaked online, what can we do to keep our data more secure? Here are our top tips for stronger passwords.

CCTN

IN OPERATION

BE UNPREDICTABLE

We often choose passwords which are easy to remember: featuring the name of our favourite sports team or favourite film, for instance. Those are predictable passwords. Cyber criminals will routinely try various combinations of passwords relating to sports teams, actors, musical artists and the like – and they often focus on these during major sporting events or around high-profile movie releases.

XXXX AVOID GETTING PERSONAL



HELLO

Many of us use passwords relating to our family, such as children's names or favoured holiday destinations. The problem here is that we also typically post about our holidays and our family on social media – making that information potentially visible to cyber criminals and supplying them with clues which could help them in narrowing down possible passwords we might have set.

NEW PLATFORM, NEW PASSWORD

Where cyber criminals gain access to an online service through a data breach, they often use the data they've stolen to try and access the victim's other accounts. This is because the criminals know that, for convenience, people often use the same password across different services. When we reuse passwords, our security is only as strong as the weakest site where we've used it.

LONGER IS STRONGER

Our passwords are often stored by online services in an encrypted format, in case the services suffers a data breach. The strength of this encryption, however, is dependent on the length of the password you've selected. If your password is only a short one, cyber criminals are significantly more likely to be able to break the encryption and identify your password. ***

CHECK SOCIAL MEDIA VISIBILITY

Staying up to date with friends and relatives on social media is part of everyday life now. We need to ensure, though, that we limit who can see our posts via each platform's privacy settings. It's also wise to consider what we're posting and if it's *really* safe to share online. If we restrict what cyber criminals can see, we reduce the chance of them using that information to identify our passwords.

Meet Our Expert

ed Information Systems Security Professional (CISSP), Gary Henders tor of IT at a large boarding school in the UK, having previously taug and colleges in Britain and the Middle Last. With a particular interest literathip and cyber security, he believes It is essential that we becom rare of the risks around technology, as well as the benefits.

(60)

Source: https://www.ncsc.gov.uk/

💓 @natonlinesafety



SECURITY

'DOUBLE LOCK' YOUR DATA

It's possible that cyber criminals may eventually discover your username and password. Enabling multi-factor authentication (MFA) on your accounts, however, reduces the chance of them obtaining access to your data, as they'd also require a code which is provided via an app, SMS message or email. MFA isn't infailible, but it does definitely provide extra protection and security.

DELETE UNUSED ACCOUNTS

Data breaches occur when cyber criminals gain access to an online service and all the data contained within it – including usernames and passwords. Whenever you stop using a service, it's wise to make sure that you delete your entire account and not just the actual app. If the service no longer has your data, there's zero risk of it being leaked should they suffer a data breach in the future.

TRY PASSWORD MANAGERS

Even though most of us have numerous online accounts to manage these days, it's advantageous to avoid password re-use. Specialist password management software (like Dashlane or OnePassword, among others) can help by storing a different password for every online service that you have an account with: the only one you or child will need to remember is the single master password.

Nt//

GET CREATINE

The British government's National Cyber Security Centre (NCSC) recommends the 'three random words' technique. This method helps you create a passwon which is unique, complex and long -yet which is memorable enough to stay in your mind ("FourBlueShoes", for example). The NCSC website, incidentally, also offers plenty of other useful information relating to personal cyber security.

STAY VIGILANT

00 The best way to protect your accounts and your data is to be vigilant and careful. If you receive an email or text message that's unusual or unexpected, treat it as suspicious until you're able to verify whether it's genuine and safe. Starting from a position of vigilance and caution will reduce the likelihood of you or your child being tricked by a malicious email, text or phone call.

National NOS Online Safety #WakeUpWednesday

AntionalOnlineSafety Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 22.03.2023

O @nationalonlinesafety

@national_online_safety

What Parents & Carers Need to Know about UN AND EUROS

WhatsApp is the world's most popular messaging service, with around two billion users exchanging texts, photos, videos and documents, as well as making voice and video calls. Its end=to=end encryption means messages can only be viewed by the sender and any recipients: not even WhatsApp can read them. Updates to its privacy policy in 2021 (involving sharing data with parent company Facebook) caused millions to leave the app, but the new policy was widely misinterpreted – it only related to WhatsApp's business features, not to personal messages.

WHAT ARE THE RISKS?

...TYPING ...

....

SCAMS

Fraudsters occasionally send WhatsApp messages pretending to offer prizes – encouraging the user to click on a link to win. Other common scams involve warning someone that their WhatsApp subscription has run out (aiming to dupe them into disclosing payment details) or impersonating a friend or relative and asking for money to be transferred to help with an emergency.

DISAPPEARING MESSAGES

Users can set WhatsApp messages to disappear in 24 hours, 7 days or 90 days by default. Photos and videos can also be instructed to disappear after the recipient has viewed them. These files can't be saved or forwarded – so if your child was sent an inappropriate message, it would be difficult to prove any wrongdoing. However, the receiver can take a screenshot and save that as evidence. FAKE NEW

ENABLING FAKE NEWS

WhatsApp has unfortunately been linked to accelerating the spread of dangerous rumours. In India in 2018, some outbreaks of mob violence appear to have been sparked by false allegations being shared on the app. WhatsApp itself took steps to prevent its users circulating hazardous theories and speculation in the early weeks of the Covid-19 pandemic.

POTENTIAL CYBERBULLYING

Group chat and video calls are great for connecting with multiple people in WhatsApp, but there is always the potential for someone's feelings to be hurt by an unkind comment or joke. The 'only admins' feature gives the admin(s) of a group control over who can send messages. They can, for example, block people from posting in a chat, which could make a child feel excluded and upset.

CONTACT FROM STRANGERS

To start a WhatsApp chat, you only need the mobile number of the person you want to message (the other person also needs to have the app). WhatsApp can access the address book on someone's device and recognise which of their contacts also use the app. So if your child has ever given their phone number to someone they don't know, that person could use it to contact them via WhatsApp.

LOCATION SHARING

The 'live location' feature lets users share their current whereabouts, allowing friends to see their movements. WhatsApp describes it as a "simple and secure way to let people know where you are." It is a useful method for a young person to let loved ones know they're safe – but if they used it in a chat with people they don't know, they would be exposing their location to *them*, too.

Advice for Parents & Carers CUCK HERE BACK!

...TEXT

CREATE A SAFE PROFILE

Even though someone would need a child's phone number to add them as a contact, it's also worth altering a young person's profile settings to restrict who can see their photo and status. The options are 'everyone', 'my contacts' and 'nobody' – choosing one of the latter two ensures that your child's profile is better protected.

LEAVE A GROUP

If your child is in a group chat that is making them feel uncomfortable, or has been added to a group that they don't want to be part of, they can use WhatsApp's group settings to leave. If someone exits a group, the admin can add them back in once; If they leave a second time, it is permanent. EXIT GROUP permanent.

Meet Our Expert

Parven Kaur is a social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience in the social media arena and is the founder of Kids N Clicks: a web resource that helps parents and children thrive in a digital world.

EXPLAIN ABOUT BLOCKING 🛛 💇

If your child receives spam or offensive messages, calls or files from a contact, they should block them using 'settings' in the chat. Communication from a blocked contact won't show up on their device and stays undelivered. Blocking someone does not remove them from your child's contact list - so they also need to be deleted from the address book.

DELETE ACCIDENTAL MESSAGES

If your child posts a message they want to delete, WhatsApp allows the user seven minutes to erase a message. Tap and hold on the message, choose 'delete' and then 'delete for everyone.' However, it's important to remember that recipients may have seen (and taken a screenshot of) a message before it was deleted.

REPORT POTENTIAL SCAMS

Young people shouldn't engage with any message that looks suspicious or too good to be true. When your child receives a message from an unknown number for the first time, they'll be given the option to report it as spam. If the sender claims to be a friend or relative, call that person on their usual number to verify it really is them, or if it's someone trying to trick your child.

CHECK THE FACTS

You can now fact-check WhatsApp messages that have been forwarded at least five times, by double-tapping the magnifying glass icon to the right of the message. From there, your child can launch a Google search and decide for themselves whether the message was true or not.





www.nationalonlinesafety.com

@natonlinesafety

THINK ABOUT LOCATION

If your child needs to use the 'live location' function to show you or one of their friends where they are, advise them to share their location only for as long as they need to. WhatsApp gives a range of 'live location' options, and your child should manually stop sharing their position as soon as it is no longer needed.

f /NationalOnlineSafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 02.03.2022

O @nationalonlinesafety

Top Tips for Adopting FE & H

Everyone has so much going on in their lives, and that includes children: from exams and deadlines to anxiety and mental health struggles. It's quite easy to send memes, make jokes and vent online about the things that irritate us, but when was the last time you – or your child – took a moment to share something kind or positive instead? In fact, when did you last stop and think about your family's online activities? To help keep them safe and teach them healthy online habits, we need to develop our children's digital resilience. There are lots of ways that children can become more digitally resilient, and we've pulled together some popular strategies here

WHAT IS DIGITAL RESILIENCE?

Resilience doesn't mean being so tough that nothing gets to you, and it's not about "putting up with things" either. Instead, it's the ability to recover from setbacks. Everyone feels sad, worried, scared or upset at times: it's how we respond and adapt to those situations which is important. Dialtal resilience is about making Digital resilience is about making choices that keep us safe and happy online, even when we're exposed to something negative or upsetting. Building your child's digital resilience will help reduce the impact of

- 0 Make time for the people and things that make you happy.
- Monitor your screen time and stick to your limits.
- make you feel good about yourself - and unfollow the ones who don't.
- Spread some positivity: post good 0

KEEP YOUR HEALTH IN MIND

- bike ride or a stroll to your local shop can really work wonders.
- Be strict with yourself about putting 0 devices away in plenty of time before bed: they can interfere with a good night's sleep, which is essential for staying healthy.

Meet Our Expert

Cayley Jorgensen is a registered couns Council of South Africa, working in priva children, teenagers and young adul a mobile app focusing on mental he providing resources and solutions to



🔰 @natonlinesafety

AutionalOnlineSafety Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 15.03.2023

O @nationalonlinesafety

@national_online_safety

REACH OUT FOR SUPPORT