



# St Ursula's Catholic Primary School

## HEADTEACHER'S NEWSLETTER

27.01.23

#9

Dear Parents and Carers,

This week we have added to our pupil voice groups as new Junior Traffic Ambassadors (JTAs) were elected. Pupils from Year 5 completed an application form that required them to explain why they wanted to take the role on and why they would make a good Travel Ambassadors. I had the pleasure of reading all the applications and it was wonderful to see how passionate our pupils are about making our school a safer place.

The Junior Traffic Ambassadors Scheme was started by Transport for London as part of the Mayor's Transport Strategy to help reduce the incidents of children hurt on our roads and increase the number children walking to school. With support from School leaders and Governors, the role of our JTA will be to spread the road safety message among the children and parents of the school and to improve the traffic situation around the school. To do this they will use a variety of strategies.

### Assemblies & Speaking Up

In the coming weeks the JTAs will give talks in assemblies to the whole school and in the classrooms. These assemblies will be about teaching road safety, traffic awareness and parking issues. Competitions and other initiatives will be introduced during these assemblies.

### Posters & Competitions

The JTAs will be running a Road Safety Poster competition and these posters will be put up around the school premises. These are to remind the pupils of road safety issues. The JTAs aim to run a variety of competitions over the year and hope that these will involve everyone and keep road safety at the forefront of people's thinking.

### Patrols

The JTAs have decided to first tackle the problem of illegal and dangerous parking and they will be patrolling outside the gates with a member of staff. With these regular patrols they hope the number of illegal and inconsiderate parkers will be cut dramatically! The JTAs cannot be there everyday, of course, and they realise that things revert when they are not present. However, I will support them by sending letters and emails to remind the parents to park considerately.

Congratulations to our newly appointed JTAs.

*Mr Ashburn*

*Get Cycling  
Bikeability Programme  
30th January*



Cycling is more than a hobby, it's a life skill. Next week, 30 of our Year 6 pupils will be taking part in a Bikeability programme where they will not only learn to cycle but gain independence, social skills and a sense of wellbeing.

Bikeability helps develop pupil confidence in responding to risks they may encounter when cycling. As a result of the programme, we hope that more children will feel confident to cycle to school which in turn will improve their physical health, mental health and wellbeing.

In addition to supporting pupil wellbeing and health, we are also helping to protect our planet! Pedal power has the potential to protect the planet from harm caused by vehicle emissions. It is also 20 times cheaper to maintain a bicycle than a car, so your pocket will thank you too! Travelling by bike instead of by car – even just once or twice a week – is a simple way to reduce your carbon footprint. Good luck to our pupils taking part!

## Attendance

### TOP FIVE - AUTUMN TERM

1	St Martin's	99.57%
2	St Paul's	99.17%
3	St Anne's	99.17%
4	St Margaret's	98.28%
5	St John's	97.52%

### SPRING TERM DATES

- 3rd Feb – Reception Vision & Hearing Screening
- 6th Feb – 9th Feb – Key Stage 1 & 2 Parents' Evenings
- 7th Feb – Year 1 trip to Discovery Centre
- 10th Feb – School Inset – School Closed
- 13th Feb – 17th February – Half Term
- 22nd Feb – Ash Wednesday Mass
- 22nd Feb – New uniform shop
- 2nd March – Year 1 trip to Harold Hill Library
- 3rd March – Year 5 & 6 C.S.I Road Safety Workshop
- 17th March Science Dress-up Day
- 28th March – Easter Production
- 29th March – Yr1 & Yr2 Road Safety Workshop
- 30th March – End of Term reports sent out (KS1 & KS2)
- 30th March – Curriculum Celebration Afternoon (KS1 & KS2)
- 31st March – Whole School Mass & Easter Egg Hunt

### ROAD SAFETY WORKSHOPS

The theatre-in-education company 'Riot Act' will be visiting to lead a Road Safety Workshop for our older pupils on Friday 3rd March. The workshop is called 'Road Safety C.S.I.' and our children will be exploring a range of evidence and will interview suspects and witnesses to find out what the main contributing factors of a traffic incident were. There is also a Year 1 & 2 Road safety workshop on



# 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.

### 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.

### 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.

### 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.

### 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](http://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.

### 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.

## 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](http://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word) | <https://haveibeenpwned.com>