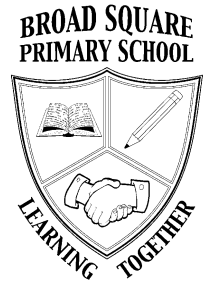




**BROAD SQUARE PRIMARY SCHOOL**  
**BROAD SQUARE**  
**LIVERPOOL**  
**L11 1BS**

**TELEPHONE No. 0151 226 1117**

**Website: [www.broadsquareprimary.co.uk](http://www.broadsquareprimary.co.uk)**  
**Email: [office@broadsquare.liverpool.sch.uk](mailto:office@broadsquare.liverpool.sch.uk)**



**Headteacher: Mrs. Charlotte Foden**

Dear parents and carers,

This term seems to be flying by. Our children continue to work hard and make excellent progress. I have had a number of visitors in school over the past two weeks and one thing that everybody comments on are the beautiful manners of our children and how well they are working in their classrooms. The children should be very proud of themselves.

A letter has gone out this week to inform the parents and carers of class 2C that Mrs Cantor will be leaving at half term to start her maternity leave. Miss Jones and Mrs Baldwin will be taking over as class teachers. We wish Mrs Cantor and her husband the best of luck and we are very excited to meet our new Broad Square baby.

### **Strike day**

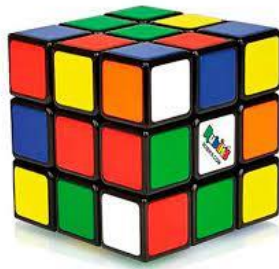
Communication has already been sent out informing all parents and carers that **school will be closed to all pupils on Wednesday 1<sup>st</sup> February.** This decision was made after I completed a full risk assessment. I understand the disruption that this may cause to some families and apologise for that; however the health and safety of all pupils is the key factor in the school closure. There is further strike action planned; however I will inform parents and carers of arrangements for those days closer to the time.

### **Prime bottles**

There is a brand of drinks that are causing a bit of fuss within some classes. Please do not bring Prime drinks or any other energy drinks to school. We are asking that Prime bottles are not used for water bottles either. We encourage our children to stay hydrated with water and we do provide cups for any children who may forget their bottles. Thank you for your understanding with this.



**Enjoyment, Compassion, Excellence, Perseverance, Respect, Community, Responsibility**



### Request for Rubik's cubes

Mrs Bird is running a Rubik's cube club in school for our junior children. There has been a lot of interest. If anyone has one at home that they no longer want to be frustrated with, can we ask that they are donated to school so that as many children can get involved as possible, thank you.

### Educational trips

We have some class visits that are coming up – please make sure that parents and carers have completed the permission slips and made any outstanding payments

Year 4 - Formby Trip 9<sup>th</sup> Feb

Year 3 - World Museum Trip 24<sup>th</sup> Feb

Year 5 - Llandudno Trip 21<sup>st</sup> April

### Good news



Our nursery children have been learning about patterns and prints. The children have been working so hard learning all sorts of pattern names. After reading the book 'Rainbow Fish' the children made their very own using paper plates, paint and glitter- we think it is fantastic!

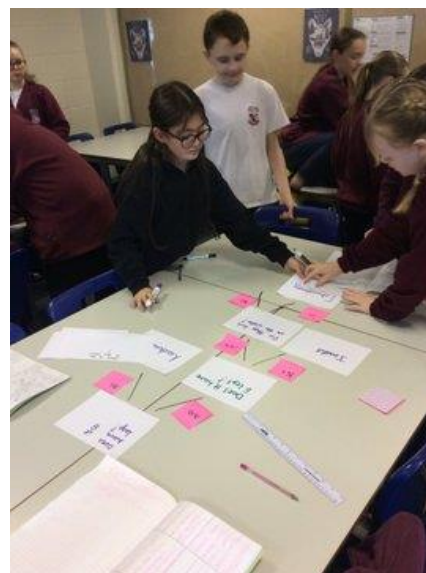
Our year 4, 5 and 6 pupils turned out in force on Monday – over 50 children and staff completed our cross-country training. We are really impressed with improvements to fitness and pace. Keep it up.





All children in the infants and juniors had a Safeguarding assembly this week with Mrs Taylor that focused on stranger danger. The children listened well and engaged in useful discussions.

Our year 6 pupils have been completing science work around classification. They created their own classification keys to distinguish between different invertebrates.



Our year 3 pupils have been working very hard understanding division this week. Here they are practically representing division.





On the final page of the newsletter are some tips for parents and carers on how to keep your children safe online.

I hope you and your families have a lovely weekend.

Thank you,

*Mrs C. Foden*

Head teacher



**Enjoyment, Compassion, Excellence, Perseverance, Respect, Community, Responsibility**

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.

# 12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

## 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](https://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**  
Guy Henderson is the Director of IT at a large secondary school in the UK, having previously taught in schools and colleges in risk and the 'black box' with a special 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/section/101/protecting-yourself-secure-online/three-random-words](https://www.ncsc.gov.uk/section/101/protecting-yourself-secure-online/three-random-words) | <https://haveibeenpwned.com>

**NOS National Online Safety**  
#WakeUpWednesday

[www.nationalonlinesafety.com](https://www.nationalonlinesafety.com) @natonlinesafety /NationalOnlineSafety @nationalonlinesafety



Liverpool Attendance Quality Mark

