

Friday 3rd July 2020

Mrs Wright Writes!

I always say these last few weeks of term tend to fly by with so much to do but I think this year has added a whole new list of other tasks. As some of you will be aware, the government published the guidelines for schools for September yesterday and there were questions about it at the briefing last night.

I will now produce a detailed plan for September to ensure we can welcome all children back to school in a safe and secure way. I am sure many of you will be pleased about this but I understand that there will be some anxiety from some parents. We will publish our risk assessment on our website once it has been agreed by the governors and the Trust. It is expected that all children will return in September so please contact me if you feel that this is not your plan. We are planning for our breakfast and after school club to be up and running in September.

Next week we are beginning our 'keeping in touch' afternoon sessions for all children not currently in school in a class bubble or a key worker bubble. I know this has caused some disappointment to those of you with children in school but we are not allowed to mix the children from existing bubbles with other children. The children who will be coming in have been at home. We had to survey the parents first to see who would like a session and as expected they have been very popular. We then allocated all the children to a session so all children can have at least one session. There were less responses from the children at home in the year groups currently in school so we were able to offer two sessions to these children, as the numbers were small. We have to ensure that we can accommodate the children inside if the weather changes so we could not have too many children on site at once. Unfortunately we can never trust the British weather and in the last few days have had torrential rain and hot sunshine all in the same afternoon!

We are asking you to ensure that the children who come in for this session are not showing any signs of Covid. We will be holding the sessions outside if at all possible with socially distanced measures in place. Please bring your child to the gate requested on the letter and ensure you socially distance and do not stay in a group waiting for them. It is important you bring them to the session allocated to you and that you do not turn up if you have not been allocated a place. Everybody who completed the survey has been allocated a place.

I have had emails from parents asking us to open more bubbles and have more children in school. While the risk is reducing across the area we still need to be cautious as the latest outbreak in Leicester has proved. It is not the time to be adding too many children in to school so for that reason we have kept our bubble size as ten; we have fourteen bubbles in school which is a lot of children and staff! There is also the logistic problem of space as we are currently using all classrooms for existing bubbles! Every teacher who can run a bubble is running one including teachers who do not usually teach that year group.

We set this up to ensure that all children who were signed up in the initial round from pre-school, Reception, Year One and Year Six were given a place. After three weeks we were able to add a few more children to these bubbles and they started with us this week for the last three weeks. I understand this has disappointed a few of you who wanted their child added to the bubbles. I know some of you felt we should then have opened afternoon bubbles for these children to allow them back to school. We are not allowed to open more bubbles unless we have the staff and the space to run them which we don't.

What we could do was offer all children at home a chance to have a session in school, ideally with their class teacher, over the next two weeks. I am afraid we do try to please everyone but accept that will never be the case. It doesn't stop us trying though!

I do appreciate that some parents of Reception, Year One and Year Six felt it was too early in June to make that decision and now feel it is safer which is the case. I also feel sorry for the other year groups who have not had the chance to be in school at all yet and hopefully these sessions will help with that. I cannot offer the other year groups more than this as teachers cannot work across two bubbles but the risk of an outside session, that is socially distanced for one session, is much lower. I do understand that everybody has their own opinion about our plans but would like to politely remind everybody that there is never a reason to be rude to staff who are all doing all they can to meet the needs of the children and families.

Next week we will be sending out the children's reports by email. The reports will come out to you between Wednesday 8th of July and Friday 10th July. If you have not received your report by Friday 10th July at 3pm then please let us know. If you have changed your email lately then please let us know that as this is often the reason things do not get through to you. I will also send you a letter on the Friday all about next year, who the teachers are etc.

Next Friday is also the day we go live with our new Management Information System so it will be an interesting week! The office staff have worked extremely hard to get all this in place so come September we will have a more efficient system for school and for parents.

Some things in the diary have gone ahead as usual this week such as Governor and Heads meetings but I am aware that we would have had the children in their new classes these last two days as part of their transition work. We will do our transition work in September and there will be a chance to meet the new teacher then as we always do. Our Year Six have been working on transition work from Cambourne this week and our SEND team are busy preparing transition booklets for all the children who require one.

One of our Reception children bubbles have made me smile this morning as they have made a huge (classroom floor!) picture of the jungle animals using a wide range of resources. If we can't go to the zoo as a year group then the animals will come to us!

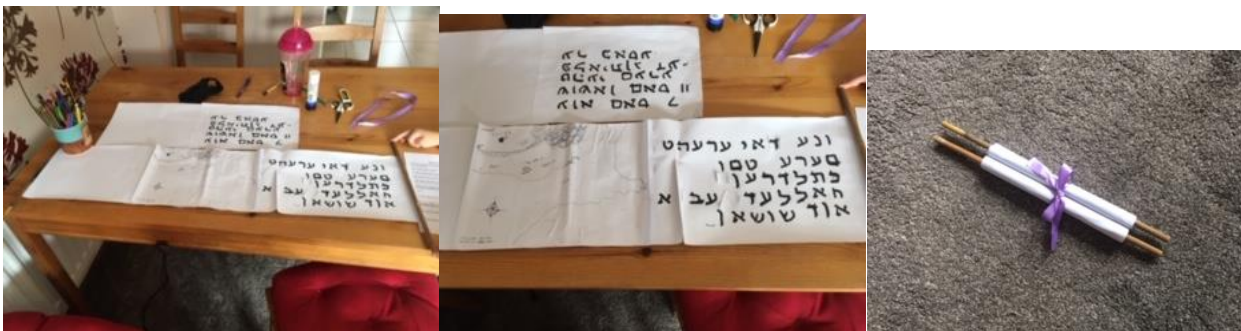
Have a lovely weekend!

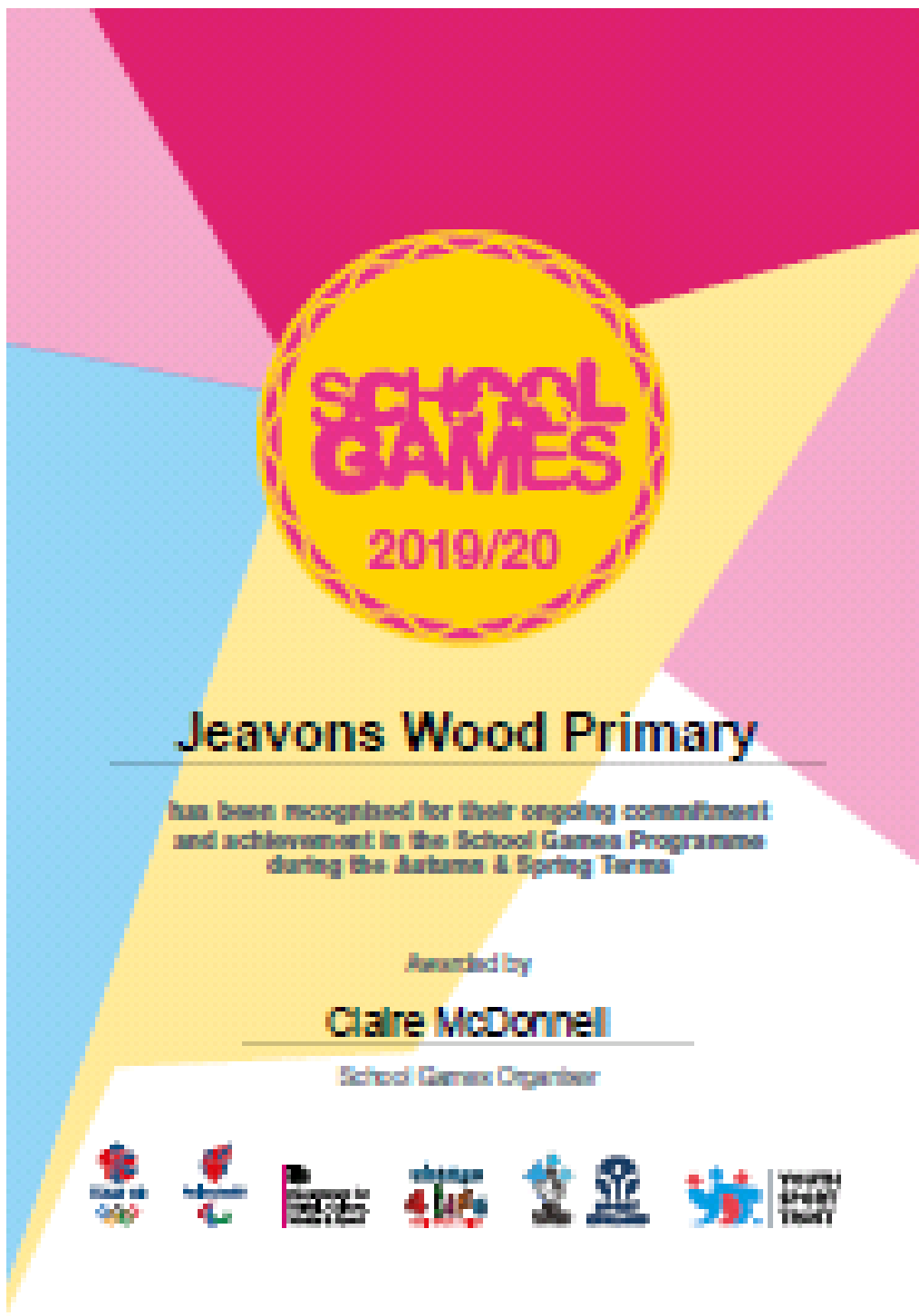


Ella from Bublebees with the coin ordering task. She really enjoyed it!



Here is Eva's (Squirrels) Hebrew scroll. It's amazing!





Cambourne food bank

As time goes on, many parents are finding it harder to stretch finances, especially while the children are at home. I want to make you aware that Cambourne food bank, who are at the Blue School on a Thursday from 10-12pm are still offering support for local families. This is in addition to the food parcels offered by Cambourne Crescent. Cambourne food bank offer roughly a weeks supply of food & other items to families via a voucher system. If you feel your family may benefit from this extra support please email ifsw@jeavonswood.org. You do not need to be in receipt of any benefits, and vouchers can be issued if the need is short term, or caused by Coronavirus events.

Personal data is a strange commodity. Cyber thieves can buy huge quantities of personal data on the black market for very little, yet your own personal data is hugely valuable to you. If your personal data falls into the wrong hands, it could lead to identity theft, bank fraud or something even more sinister such as stalking. The severity of that threat is multiplied when it comes to the personal data of children, when threats such as internet grooming begin to emerge. The bad news is that children aren't always great at safeguarding sensitive information, which is why they need parents' help and guidance. That's why we've created this guide to show you how you can protect your own and your family's personal data.



What parents need to know about PROTECTING PERSONAL DATA



EVERY DETAIL IS KEY

Which info should you be wary of sharing online? Aside from the obvious, such as full names, date of birth and address, think of the type of information you're asked for when answering security questions for services such as online banking. The name of your first school, your mother's maiden name, the names of your pets, your favourite band. Data thieves will harvest as much of this information as possible, so don't make it easy for them by publishing it anywhere online.



SOCIAL MEDIA VISIBILITY

Social media sites, such as Facebook, encourage us to share sensitive information in order to build our online profiles. Many people are lulled into thinking that only their friends can see such information, but that's rarely the case. Such information can easily be shared with 'friends of friends' or even anyone searching for you online because privacy settings are opaque. Keep social media profiles to the bare minimum. If you wouldn't be comfortable hanging a sign with that information on your front door, don't enter it into social media sites.



DANGEROUS GAMES

Online games are a particular risk for children. Many of the most popular games – such as Fortnite, Minecraft or Roblox – have voice or text chat facilities, allowing them to talk to fellow gamers. Or, sometimes, people pretending to be fellow gamers. It's very easy for children to be seduced into divulging personal data such as their address, birthday or school. It's critical parents both educate children on the dangers on online chat in games and take safeguards to protect children.



IMPOSTERS AND PHISHING ATTACKS

Even if you're scrupulous about keeping your data private on social media, it's easy to be lulled into handing it over to imposters. There are two golden rules for you and your children to follow: 1. Never divulge personal information to phone callers, unless you can be absolutely certain you know who they are. 2. Never click on links or open attachments in emails or social media, unless you're 100% certain they are genuine. So-called phishing emails are growing ever-more sophisticated, with fraudsters able to replicate the exact look of bank emails and even include details such as account numbers and IDs.



THE RISKS OF PASSWORD SHARING

Password sharing – using the same password for multiple sites – is one of the easiest ways to lose control of your personal data. Hacking of major websites, including usernames and passwords, is common. If you're using the same password for a hacked site as you do on your Gmail account, for example, you're handing data thieves an easy route into your inbox, where they will doubtless find all manner of sensitive information, such as bank emails and contacts. Your email account will often also let them reset the password on multiple other accounts. Don't share passwords; use password managers to create strong, unique passwords for every site.



NOS National Online Safety
#WakeUpWednesday

Safety Tips for Parents & Carers



LOOK OUT FOR LEAKS

Many security software packages have features that look for personal data leaks or prevent people from entering it into risky sites in the first place. For example, Bullguard Premium monitors dangerous sites for usage of data such as your email address, debit card numbers, passport number and more, and then sends you email alerts and details of how to take remedial action if it spots them being used. Such software also issues warnings if it sees personal data being entered into unprotected, high-risk sites.



KEEP DATA GUARDED

Don't give the thieves a head start by handing them pieces of sensitive information for free. For example, it's very common to see email address such as davesmith1976@gmail.com – an immediate clue that you were born in that year. If you have a less common name than Dave Smith, thieves could immediately start using that information to cross reference against public records or other database breaches, allowing them to start building a profile of information about you. Likewise, don't use your date of birth in a password. If that's hacked, you've handed the thieves another big clue.



DON'T OVERSHARE ON SOCIAL MEDIA

The biggest threat to your child's privacy is you. Parents often overshare personal information on social media: full names, names of schools, children's birthdays, names of their friends. All of this can be easily gleaned to build profiles that could be used to groom your child in online games or in real life. Exercise extreme caution with social media posts concerning your children.



BE WARY OF SHARED NETWORKS/SYSTEMS

Avoid entering any personal data into a web browser when you're using public Wi-Fi (in a coffee shop or airport, for example) or when using shared computers. Shared Wi-Fi connections are much easier to eavesdrop on than your home network, especially if they are not password protected or the password is shared freely with customers. Don't do online shopping, banking or enter any logins/passwords when using shared Wi-Fi. Likewise, if you're using a shared computer at work, for example, as it's very easy for a browser to save logins that could be used by others.



PLAY SAFE IN ONLINE GAMES

Children must be taught to treat strangers in online games with the same caution as they would treat strangers in the street. Don't allow children to use their real name as their username in games to prevent imposters conning kids into thinking they are real-life friends, and only allow them to add friends in the game that they know in real life. Regularly ask to monitor your child's friends list in such games and ask them to identify who the players are. With younger children in particular, ask them to only use voice chat in family rooms, so that you can hear conversations.



Meet our expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as *The Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *BBC Newsnight*, *Radio 5 Live* and the *ITV News at Ten*. He has two children and has written regularly about internet safety issues over the years.

