St John's Primary School and Nursery

Warwickshire County Council

National Teaching School
designed by

Department for Education

National Support School
designed by

National College for Teaching & Leadership

Mortimer Road
Kenilworth
CV8 1FS

01926 854450
www.st-johns.warwickshire.sch.uk
Head Teacher: Mr D Barrow

15th February 2019

Dear Parents and Carers,

ONLINE SAFETY – YEAR 4

Essential question: How can you protect yourself from online identity theft?

This half term in our internet safety lesson, Year 4 thought about how we can protect ourselves, and our friends and families, from online identity theft. We started by thinking about the kind of websites that require information from us and the reasons for this. We thought about the benefits of sharing information online, but also about the safety and security risks of sharing certain types of information. We then discussed the types of information that can put us at risk of identity theft and other scams. Finally, we distinguished between personal information which is safe to share online because it cannot be used to identify us (e.g. age, gender and number of siblings) and private information which is unsafe to share and can be used to identify us (e.g. full name, phone number and address).

From 4P, 4T, Miss Perkins and Miss Taylor

Common Sense on Online Security

What's the Issue?

Learning to protect personal identity information, creating strong passwords and being cautious when downloading programmes and files are crucial to children's safety as well as the security of the information stored on their digital devices. Otherwise, children can expose themselves and their families to digital threats such as computer viruses, data and identity theft, and hacking.

To understand digital safety and security, you'll need to learn perhaps some unfamiliar words: phishing, malware, spyware, spam and yes, even junk. These refer to greedy little programmes that attach themselves to respectable-looking software, e.g. a downloadable game that looks really cool and then wreak havoc once installed on our computer.

Why Does It Matter?

If children don't protect their personal information, there are many potential risks: damage to the hardware, identity theft and financial loss. Children may not realise that they are putting their information in jeopardy because the warning signs aren't always obvious. For instance, another child might ask for your child's computer password to play a game and then access your child's private email account. Or your child might use a file-sharing programme that passes along a virus to your computer. Older primary school children might be asked to provide personal identity information such as home phone number, address, or date of birth, by a thief posing as someone else, all of which opens up the family to the risk of identity theft. Just like in real life, children online have to know who to trust with information.

common sense says

Help your child master the fine art of password creation. Teach them:

- **Not to use passwords that are easy to guess, such as their nickname or their pet's name.**

- **Not to use any private identity information in their password.** Identity thieves can use this information to pretend to be them.

- **Not to use a word in the dictionary as a password.** Hackers use programmes that will try every word in the dictionary to guess passwords.

- **To use combinations of letters, numbers and symbols.** These are harder to crack than regular words because there are more combinations to try.

Teach your children to be careful with what they download. Let them know not to download free games or videos to their computer. These programmes often come with spyware and viruses that will land the computer in the repair shop – and them in hot water. In the end, what seemed like free software often comes at a cost.

Let your children know how to identify and deal with spam. Teach them that spam is Internet junk mail. They should not open it because, if they do, they will just receive more of it. The best strategy is not to open email from addresses they don't recognise.

Private and Personal Information 🔑 🔍

Word Search

```
r  e  s  p  e  c  t  i  c
e  e  i  c  s  i  c  r  o
e  e  t  r  r  r  e  i  m
e  e  a  s  t  m  s  r  m
g  e  a  o  i  i  i  o  u
e  a  i  r  p  g  c  o  n
s  c  i  h  t  e  e  e  i
e  a  s  p  c  i  r  r  t
e  r  a  r  i  t  p  o  y
```

community   ethics   precise   respect   register

* **WHAT DO YOU THINK?**
What would be a good rule for kids about giving out private information online?

* **DO YOU REMEMBER ...**
How you can protect yourself from online identity theft?

1. Family Activity

Take a set of flash cards or cut a large piece of paper into smaller strips. With a family member, write different pieces of information about you, your family members, or your family on each piece of paper (for example: "I love dogs," "I'm in Ms. Smith's class," or "We live at 123 Pine Road."). Take two jars or cups and label one "private information" and the other "personal information." Then, sort the strips of paper into the correct jar to practise identifying which pieces of information are private versus personal.

2. Tech It Up!

Ask a family member to show you a website that collects information about users. Together, look at the information the website asks users to fill out, and see whether you can identify the questions that prompt you for personal information vs. private information. (Hint: If an adult in the family is a Facebook user, Facebook or another social media platform can be used for this exercise.)

3. Common Sense Says ...

Private information is information that can be used to identify you, such as your date of birth or your address. Personal information is information about you that can't be used to identify you, such as your age or your favourite foods. Personal information is usually safe to share online, but private information is usually unsafe to share