UNIT 2.4

We are code masters

Generating strong passwords and keeping them safe

1 About this unit

UNIT SUMMARY

In this unit, children will understand that passwords are an important part of keeping information safe. They will discuss where passwords are required, including for devices, emails and other online activities and consider what happens if passwords are shared. They will then look at the rules for creating a strong password and discuss what makes a password weak. Finally, they will use these rules to practise generating their own passwords.

REPORTING ROUTES

In Year 2, children should know a range of ways to report concerns and inappropriate behaviour through:

- talking to a trusted adult.

This point should be re-emphasised in any teaching and learning where children are working online.

If any safeguarding issues or concerns arise during this unit, you must follow your School Safeguarding Policy.

ONLINE SAFETY FOCUS

In this unit, children will:

- understand that passwords are an important part of keeping information safe
- understand differences between strong and weak passwords
- understand that sharing a password makes it weak.

ENGAGING PARENTS AND CARERS

- In this unit, children will take what they have learned from this session and share it with their parents by asking them to generate strong passwords for their own online accounts.
- Include the importance of strong passwords in any online safety session you run for parents.

TEACHER KNOWLEDGE

- Passwords are an integral part of device and internet use. It is important that children understand what constitutes a strong password and how to best protect their personal information so they are confident internet users as their independence online increases.

CROSS-CURRICULAR LINKS

Computing
Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

2 Getting ready

ONLINE SAFETY PRINCIPLES

Think about how you can embed the online safety learning and outcomes from this unit within your whole-school online safety strategy through:

- whole-school e-team engagement
- online safety displays
- use of a website online safety area
- Twitter tweets. For example: 'This half term our Year 2 pupils are looking at what makes a strong password.'
- a school newsletter. You may wish to paste the following advisory text for parents and carers into your school newsletter, or send home in book bags (see editable *Newsletter text* on My Rising Stars): 'This half term, Year 2 pupils have been finding out the importance of strong passwords when using online accounts. Children have been asked to share what they have learned with their parents and carers and encourage you to come up with your own stronger passwords!'

THINGS YOU NEED

- Interactive whiteboard to show *Choosing strong passwords* photocopiable master and write examples of weak and strong passwords.
- Image of keyboard

THINGS TO DO

- Familiarise yourself with the steps of this activity before running this online safety session.
- If you wish to show any of the videos from *Useful links*, double-check the content of all websites before sharing in class.
- Print and photocopy the *Choosing strong passwords* photocopiable master – one per child.
- Find a simple image of a keyboard to share with children.

MY RISING STARS RESOURCES

- *Choosing strong passwords* (.pdf)

OTHER RISING STARS RESOURCES

- *Switched on Computing, Unit 2.5 – We are detectives* (looking more closely at email safety).

INCLUSION/THINGS TO CONSIDER

- Some children may not have access to technology at home and so may not be aware of the need for passwords. Use examples of passwords required in school to ensure everyone is included equally.
- Some children may reveal that they know their parents' passwords. In this case, consider asking them at the end of the session how they might teach their grown-ups to protect their information more safely. You may also wish to discreetly discuss this with parents on a one-to-one basis so they are aware that children will have the ability to access and use tools such as their email and messaging apps, and also the ability to change the password.

USEFUL LINKS

- CBBC resources for online safety: www.bbc.co.uk/cbbc/curations/stay-safe
- Smartie the Penguin; interactive book with scenarios: www.childnet.com/resources/smartie-the-penguin

3 Running the lesson

Resources

- Interactive whiteboard
- Image of a keyboard
- *Choosing strong passwords* photocopiable master – one for each child

Possible outcomes

- Children will use the knowledge they have learned in this session to create examples of strong passwords.
- They will then take their *Choosing strong passwords* sheet home to share with their family.

Step 1: Introducing the session

- Explain to the children that in this online safety session they are going to look at the importance of passwords and how to make them strong.
- Explain that passwords are codes used to keep our information safe. Just like personal information, passwords should not be shared; not even with friends.

Step 2: Discussing why we use passwords

- Ask the children if they can think of any time they, or their family, have needed a password on a device or online, e.g. tablet passcode, computer log-in, log-in to play a game, email, banking, etc.
- Explain that passwords are needed for lots of internet activity including using email. Explain that everyone has their own private password for their email and no one else knows it so that the information in the email stays safe.
- Ask them to think about what might happen if someone knows their password, e.g. money can be taken from a bank, someone can pretend to be you, etc.

Step 3: What makes a strong password?

- Explain that passwords are an important part of keeping information safe and there are some tricks everyone can use to make a password strong.
- Project an image of a keyboard on the interactive whiteboard. Point out all the characters that children might not necessarily use or notice, e.g. hashtag, money signs, question mark, etc. Ask the children how they might use these to make a strong password and write an example.

CONTINUED ON PAGE 54

- Explain that passwords can be made up of any characters on the keyboard. A strong password is at least 8 characters long and a mixture of letters (both upper case letters and lower case letters), special characters and numbers.
- Explain that a password can contain words but they don't have to be spelt correctly or have capitals in the right places. In fact, a strong word might have a capital in the middle and one at the end!
- Next explain that passwords should not contain any personal information. Ask the children for some examples, e.g. name, birth date, house number, etc. Explain that a password which contains personal information is weak as it is easier for someone else to guess.
- Explain that passwords should be different for every site, device or account that requires one. Ask the children why they think this might be. Prompt them as necessary (if you have the same password for all your accounts and someone finds out what it is, they will be able to get into all of your accounts!).
- Explain that passwords should be changed every 6 months to help information stay safe. Passwords are like your toothbrush – you should change them regularly!
- Reinforce that code masters apply all these rules every time they create a password.

Step 4: Generating passwords

- Explain to the children that to practise their code master skills, they are going to create passwords using the rules they have discussed.
- Provide each of the children with a copy of the *Choosing strong passwords* photocopiable master. Ask them to practise making a password using the rules they have learned. Make sure the image of the keyboard is still visible so children can refer back to this.
- Bring the class back together and ask children to share examples of the passwords they have created. How strong are each of the passwords? Ask children to suggest how the passwords could be improved.

Step 5: Summing up

- Recap that passwords keep personal information safe and prevent other people from accessing our accounts. Passwords should always follow the rules so they are strong and easy for the creator to remember. Secure passwords are not shared with anyone and are changed every six months.

4 Taking it further

- Ask the children to take home their *Choosing strong passwords* sheet and challenge their family to see who can create the strongest passwords. Ask them to carefully check everyone's attempt to make sure they follow the rules and see if they can come up with more ideas to make passwords even stronger, e.g. use a different language. They could even create a weak password and challenge their grown-ups to work out what it is.