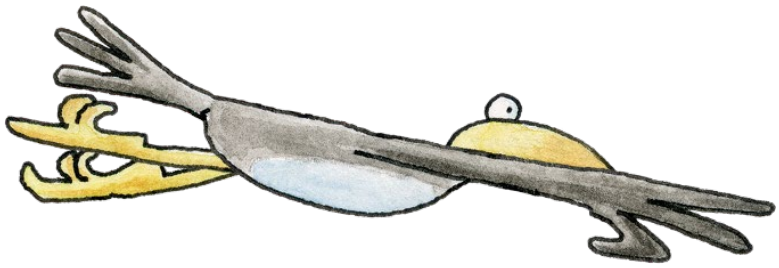
The Bongles

The Bongles and The Crafty Crows

Guide for Grownups



Links to the Scottish Curriculum for Excellence

Age Range: Early and First Level Curriculum for Excellence

Technologies: Digital Literacy - Cyber resilience and internet safety

Early Years

- I can explore, play and communicate using digital technologies safely and securely.
- Demonstrates an understanding of the importance of passwords and passcodes.

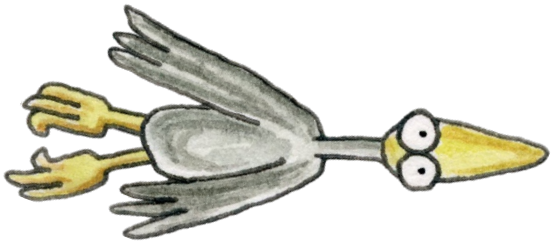
First Level

- I can extend my knowledge of how to use digital technology to communicate with others and I am aware of ways to keep safe and secure online.
- Demonstrates an understanding of the need for strong passwords.

Links to the National Curriculum

Key Stage 1
https://www.gov.uk/national-curriculum

There are alternative tasks within some of the activities, so that the grownups can keep referring to the book and use different activities to reinforce various aspects of the learning content in a way that will suit different children's needs and learning styles.



Activities 1 – Read, Respond, and Recap

The read and respond activity introduces new concepts from the book and heads up the accompanying activities.

These discussion points are designed for adults to lead on during the learner interactions.

The aim is to:

- analyse the story with relation to cyber resilience and internet safety
- encourage the children to talk about their opinions and thoughts on cyber resilience and internet safety in relation to the story

Activity 2 – Retell the Story

In this activity children are exploring their story comprehension and are encouraged to creatively retell their interpretation of the story through a variety of different media.

The aim of this activity is to explore the cause and effect of the character's actions, and their responses to the events.

Activity 3 – My Crate of Treasures

In this activity children will consider which belongings they'd put in a password protected crate, and the importance of keeping their own items secure (rather than the Bongles' items).

This links in with the first part of the book where The Bongles claim their treasure.

You want to encourage the children to consider how they'd keep important items protected.

The activity can lead to a discussion about the children's choices and reasons why they've made certain choices.

Key words to use are:

- secure
- hidden

- belongings
- protected

The children will need a certain amount of understanding about what it means to protect or look after things that are important.

Children can come up with ideas for the ways they could protect their treasured items in different environments, for example, at home, in school, at the park.

Activity 4 – Passcodes and Password Treasure Hunt

Refer to the subject matter factsheet for definition of passcodes and passwords.

In this activity children are exploring the environments around them, and encouraged to interact with them by searching for passcodes and password protected places or things within them.

This connects with the Bongles' attempts to lock their items in the shed in the story.

Children are also learning and investigating the difference between passcodes and passwords, what they might be protecting, and how they can be useful in different contexts.

Activity 5 – Tinkering with Passcodes

In this activity children are encouraged to physically interact with tools to deepen their understanding of randomness.

By interacting with one another and testing their findings, children will begin to learn how numerical sequences without an obvious pattern or logic are more challenging for their peers to guess.

Activity 6 – Generating Three Random Word Passwords

Refer to the subject matter factsheet for definition of three random word passwords.

The Bongles and The Crafty Crows

Subject Matter Factsheet

The subject matter factsheet is to help prepare teachers and parents for using the book with their children. It will give them a slightly broader understanding of cyber security, so they feel comfortable answering any questions that the children may have.

Passcodes

A passcode is a numeric sequence used to authenticate a user on a laptop, desk computer or electronic device.

The word 'passcode' is sometimes used synonymously with 'password' but technically, a passcode only contains numbers.

Passcodes are a way for you to protect your devices. They are usually 4 to 6 digits and are used to grant access to the device.

Passcodes to unlock devices is similar to the code you use for an ATM bank card or a debit card. The code for your bank card is known as your Personal Identification Number or PIN.

Setting a passcode on an iPad:

- Open the iPad or iPhone's setting on.
- Scroll down the left-side menu and select Passcode.
- Select the Turn Passcode On link.
- iOS will prompt you to enter a passcode. It may default to 4 or 6 digits, but you can select Passcode Options to choose another type of passcode. You need to enter it twice before iOS saves it.

If someone tries to access your iPad by guessing your code, the iPad disables itself for a period of time after a certain number of failed guesses.

One important option most people overlook is the ability to turn Siri and Notifications off while on the lock screen.

- By default, the iPad allows access to these features even when the iPad is locked. This means anyone can use Siri without typing in the passcode.

- And between Siri, Notifications, and the Today screen, a person can view your day's schedule, set meetings, set reminders, and even find out exactly who you are by asking Siri, "Who am I?"

- They can see text messages and other notifications as they pop up on the screen without unlocking the iPad.

Different passcodes and restrictions for a child's iPad

- The passcode used for unlocking the device and the one used for the parental restriction settings for the iPad are separate, so you can have different passcodes for each of these features.

- Restrictions are used to childproof an iPad and can limit (or disable) access to the App Store, limit the types of music and movies that can be downloaded, and even lock out the Safari web browser.

- When you set up restrictions, you're asked for a passcode. It can be different than the one used for the device itself, so your child can lock the device as normal.

- The passcode used for restrictions won't unlock the device unless the two passcodes are the same. So, you cannot use the restrictions passcode as an override to get into the device.

Did you know?

There are 256 combinations using numbers one, two, three and four.
If children were to use numbers between zero and nine to create a four-digit passcode, they could create up to 10,000 combinations.

Shoulder Surfer

Shoulder surfing is a simple method for spying on unsuspecting victims to collect personal data, such as passwords, Personal Identification Numbers (PINs), access codes and other login information.

There are two types of shoulder surfing.

- The first type of shoulder surfing is when direct observation is used to obtain access to data. This is when a person looks directly over the victim's shoulder to observe when they are entering data, such as their PIN.

- In the second type, a person's actions are first recorded on video. Someone can then analyse these videos in detail and obtain the desired information. It's possible to use video recordings to determine the PIN for unlocking mobile devices even if the display cannot be seen in the video. The movements of a user's fingers are enough to determine the PIN.

Tips for inputting a passcode, PIN, access code to protect yourself from shoulder surfing:

- you should cover the input device with your hand when entering your PIN.

- at cash machines you should also check for poorly mounted or suspicious-looking parts.

Passwords

Three Random Words guidance from the National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

The NCSC define a password as a 'series of characters'.

Weak passwords can be cracked in seconds. Avoid the most common passwords that criminals can easily guess (like 'password').

You should also avoid creating passwords from significant dates (like your birthday, or a loved one's), or from your favourite sports team, or by using family and pet names. Most of these details can be found within your social media profile.

If you're thinking of changing certain characters in your password (so swapping the letter 'o' with a zero, for example), you should know that cyber criminals know these tricks as well. So your password won't be significantly stronger, but it will be harder for you to remember.

The longer and more unusual your password is, the harder it is for a cyber-criminal to crack.A good way to make your password difficult to crack is by combining three random words to create a password (eg applenemobiro). Combine three random words to create a password that's 'long enough and strong enough'.

Or you could use a password manager, which can create strong passwords for you (and remember them).

Why does the NCSC recommend using 'three random words' as a way to create passwords?

By using a password that's made up of three random words, you're creating a password that will be 'strong enough' to keep the criminals out, but easy enough for you to remember.

Longstanding advice around making your passwords very complex (which suggests we should create passwords full of random characters, symbols and numbers) is not helpful. This is because most of us have lots of passwords, and memorising lots of complex passwords is almost impossible.

Passwords generated from three random words is a good way to create unique passwords that are 'long enough' and 'strong enough' for most purposes, but which can also be remembered much more easily. If you want to write your password down, that's also OK, provided you keep it somewhere safe.

If you want to find out more about why the 'three random words' technique works, you can read this blog by one of the NCSC's technical experts that further explains our thinking.

The NCSC policy is 'three random words', however we have to acknowledge that many account providers have policies that require other characters. The book and learning activities deal only with 'three random words' passwords. The introduction of special characters into passwords could be used as with an older age group and is not covered here.