Beech Hill Primary School Knowledge Organiser

Topic: Computing – Digital literacy	Year group	Term
Digital Citizenship 6	Year 6	Spring 1 5 sessions

Background knowledge

Digital Citizenship 6 aims to provide children with the knowledge and skills required to navigate the digital world safely and responsibly. This is a 'Big Question' unit and the children will be working towards answering the following question… How can we distinguish between reliable and unreliable information online? The steps in this unit include concepts and activities designed to support children in answering the unit's Big Question.

To teach this unit confidently, a good understanding of the advantages and disadvantages of the Internet is essential for explaining what we use the Internet for and the risks we face while online. To support children in their learning about misinformation, a secure understanding of how fake news is created and spread online is beneficial. Being able to explain different types of cybercrime and ways we can protect our online identity would be very helpful when discussing cybersecurity. Throughout the unit, you may want to refer to recent misinformation referenced by the media or example websites you can show children to explore reliable sources.

Familiarise yourself with the CPD for this unit to support your subject knowledge in this area.

What should I already know?

The children should have an understanding of what a digital footprint is and how their online behaviour has an impact on it. They should be able to explain what information should be public or private and begin to understand that what they put online can affect their reputation and future opportunities. The children should know that not everything or everyone online can be trusted and be able to explain some reasons why people create fake news.

National Curriculum Objectives / Key Skills	The Journey
NC Children should be taught to: * use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact; * use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content; * understand computer networks including the Internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration. **Key Skills** This unit provides the children with knowledge and skills that can be applied in their use of technology throughout the curriculum, for example: * being able to evaluate and analyse whether something is reliable and credible; * understanding the difference between fact and opinion; * being able to communicate online in a professional and respectful manner; * being able to summarise information that they find online; * knowing how to act if they are faced with something they are unsure of; * knowing strategies for dealing with inappropriate behaviour or content; * understanding the positives and negatives of risk taking.	1. To understand how misinformation is shared online. To understand the dangers of posting or sharing misinformation. (Task 1: Write / describe the different between disinformation and misinformation in less than 30 words.) (Task 2: Sort the statements into beliefs, opinions and facts.) (Task 3: Write your own examples of beliefs, opinion and facts). 2. To understand how to evaluate the reliability of online content. (Evaluating online comment. Children annotate the pdf in Word / powerpoint / smart notebook) 3. To understand how to manage a digital footprint. (Task 1: Sort the statements into Active and Passive digital footprints.) (Task 2: Summarise information found online about a famous person to see how big a digital footprint can become). (Task 3: Discuss: How can your digital footprint **be affected by others?**) 4. To identify possible online risks. (Use the Online Risks rescource) 5. To recognise ways to increase cybersecurity. (My strong password plan)

Outcomes

This unit works towards the following milestone concepts:

* Children will recognise online content which tries to make people believe something false is true or misleading.
* Children will be able to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.
* Children will recognise that the information, comments or images that are put online can be used by others.
* Children will develop an understanding of the risk of identity theft or targeted approach from fraudsters.
* Children will identify possible online risks and make informed decisions about how to act. They will develop their understanding of cybersecurity and ways to protect themselves from a range of cyber crimes.

Throughout the unit, children will:

I know the difference between online misinformation and disinformation.
I know what is meant by a hoax.
I know how fake news may affect someone's emotions and behaviour, and explain why this may be harmful.
I know the difference between a belief, an opinion and a fact and can give examples.

I know how to evaluate digital content and can explain how to make choices about what is trustworthy.
I know how to explain key concepts including: information, reviews, fact, opinion, belief, validity, reliability and evidence.
I know how to identify, flag and report inappropriate content.

I can search for information about an individual online and summarise the information found.
I know that some online services may seek consent to store information about me; I know how to respond appropriately and who I can ask if I am not sure.
I can use the terms influence, manipulation and persuasion and explain how someone might encounter these online.

I know that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my fault.
I know ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content.
I know what is meant by being sceptical; I can give examples of when and why it is important to be sceptical about things online.

I know strategies for keeping personal information private.
I know what to do if a password is shared, lost or stolen.
I know ways people can manage passwords.
I know that someone can get help if they are having problems and can identify when to tell a trusted adult.

Key Vocabulary

Misinformation – Information that is *not true*, but the person sharing it might not realise it's wrong.

Disinformation – *A lie that's told on purpose*, often to confuse or trick people.

Malinformation – True information, but it's *shared to hurt someone* or cause trouble.

Hoax – A made-up story or *trick to fool people* for fun, attention, or to cause fear.

Clickbait – *Tricky headlines or pictures* made to get you to click on something, even if it's not what it promises.

Fact – Something that is *definitely true* and can be proven.

Belief – Something a person *thinks is true*, often based on their own feelings, culture, or religion.

Opinion – What someone *personally thinks or feels* about something.

Reliability – How much you can *trust something to be true or accurate*.

Validity – Whether something *really measures or shows what it says it does*.

Warning Sign – A clue or hint that *something might be wrong or unsafe*.

Source – Where *information comes from*, like a website, person, or book.

Reputable – A source or person that is *known for being honest and reliable*.

Bias – When someone only *shows one side* of a story and leaves out the rest.

Evidence – *Proof* that something is true, like photos, facts, or witness accounts.

Evaluate – To *carefully think about something* before deciding what to believe or do.

Scam – *A sneaky trick* to steal your money or personal information.

Deepfakes – *Fake videos or images* made with special technology that can look very real.

Active Digital Footprint – Information *you choose to share online*, like posts and comments.

Passive Digital Footprint – Information collected *without you doing anything*, like websites tracking what you look at.

Cookie – A small file a website puts on your device to *remember things about you*, like your preferences.

Data – *Facts or information* collected about you or things you do online.

Data Leak – When personal data is *accidentally shared or stolen* from a company or website.

Digital Influence – How things online like videos or ads *try to change what you think or do*.

Digital Manipulation – When pictures, videos, or stories are *changed to trick or influence you*.

Digital Persuasion – When someone *tries to convince you online*, like a brand or an influencer.

Online Risk – Anything on the internet that could *hurt, trick, or upset you.*

Malware – *Bad software* that can damage your device or steal information.

Cybercrime – *Illegal acts done using the internet*, like hacking or stealing data.

Phishing – A fake message (usually an email) *trying to trick you into giving away private info.*

Sceptical – Being *careful and not easily fooled*—asking questions and checking facts.

Cybersecurity – The ways we *protect our devices and information online.*

Cyber Smart – Being *wise and careful* when using the internet or technology.

Strong Password – A password that's *hard to guess*, using a mix of letters, numbers, and symbols.

Question of the week.

1. Is this statement a belief, a fact or an opinion? (Teacher creates an example of one for children to discuss).
2. How do I know this information is unreliable? (Use pdf resource from lesson 2 for example of unreliable material).
3. Is this an example of active digital footprint or passive digital footprint?
(A shopping website remembering what you looked at even if you didn't buy it.)
(A comment you posted on someone else's Instagram post).
4. I agree to play an online game with a stranger over voice chat. What are the possible online risks of doing this?
5. Give me some tips for making a strong password.