

 S' George's	 Year 5	Mid- Term Plan: Computing	Term: Autumn 1	C O D E
		Unit Title: Internet Safety and Coding		
Key Themes / Vocabulary: Safety, passwords, document, copy, paste, font, bold, italic, underline, minimise, maximise, animation, onion skin, frame		Cross Curricular Links: SMSC – Keeping ourselves safe		
Overview: ICT – Logging on, internet safety and digital literacy. Introduction to block coding, learning key coding language and basic coding skills.				
UK National Curriculum (KS2 Computing)				
- Digital Literacy & Safety: Use technology safely, respectfully, and responsibly; recognize acceptable/unacceptable behavior; identify a range of ways to report concerns about content and contact. - Computer Networks & Data: 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. - Algorithms & Security: Understand how data can be encrypted, transmitted, and decrypted securely across digital networks.				
ISTE Standards for Students				
1.2 Digital Citizen: 1.2.a: Cultivate and manage a digital identity and reputation and be aware of the permanence of their actions in the digital world. 1.2.b: Engage in positive, safe, legal, and ethical behavior when using technology, including social interactions online or when using networked devices. 1.2.d: Manage personal data to maintain digital privacy and security and be aware of data-collection technology used to track their navigation online. 1.6 Creative Communicator / 1.5 Computational Thinker: 1.5.a: Formulate problem definitions suited for technology-assisted methods such as data analysis, abstract models, and algorithmic thinking.				

CSTA K–12 Computer Science Standards

- **1B-NI-04: Model how information is transformed into digital data and transmitted over local devices and networks.**
- **1B-NI-05: Discuss real-world cybersecurity problems and how personal information can be protected (e.g., strong passwords, encryption techniques).**
- **1B-AP-11: Decompose (break down) problems into smaller, manageable subproblems to facilitate the program development process.**

Week / Lesson	Weekly Overview
ICT Lesson 1	ICT room rules Keeping our passwords/information safe and why it is important. Logging on successfully. Setting our password and introduction to teams / typingclub.
ICT Lesson 2	Legends family adventure Interland
ICT Lesson 3	Legends family adventure Interland
ICT Lesson 4	Legends family adventure Interland
ICT Lesson 5	Code.org cyper cracking

ICT Lesson 6	Code.org blockchain
ICT Lesson 7	Code.org blockchain
ICT Lesson 8	Code.org blockchain

Week /Lesson	Learning Goal and Success Criteria	Teaching input and learning opportunities <i>Including lesson structure, key vocabulary and questioning</i>	Key questions for the lesson	Differentiation/ Universal design <i>e.g. support, scaffolding and challenge, focus groups</i>	Resources
ICT Lesson 1	• UK NC: R5.4 (Identify reporting routes), R5.5 (Describe and practice good online behavior). • ISTE: 1.2.d (Manage personal data to maintain digital privacy and security). • CSTA: 1B-NI-05 (Discuss cybersecurity problems and personal data protection).	0–10 Minutes Students log onto their workstations and launch the typing practice link on the class website to complete a targeted warm-up. This custom typing session focuses on key cybersecurity terms—such as <i>password</i>, <i>security</i>, <i>network</i>, <i>privacy</i>, and <i>protection</i>—to introduce the unit's core vocabulary while building finger muscle memory. Circulate around the room to ensure lower-attaining students prioritize keyboard accuracy and proper hand positioning over speed. 10–30 Minutes Gather the whole class to introduce the ICT lab safety rules and physical hardware care (handling tower units, keeping liquids away, and logging out securely). Direct students to launch the embedded "Password Security & System Operations Module" on the class website. Students work through the first two interactive slides: confirming the four ICT suite safety rules and using the "Password Crack Time Inspector" to test password strength. Guide pupils through typing sample passwords into the estimator to observe how adding length, numbers, and special characters exponentially increases crack time from milliseconds to billions of years. Demonstrate how to evaluate smart alternatives using three random words linked by special characters (e.g., Teapot#Rocket\$99). Finally, instruct pupils to complete Slide 3 by typing an incident response plan detailing what steps to take if they suspect their account details have been compromised. Once verified, guide them to click "Download Security Verification Report" and save their generated HTML summary into their personal network folder.	☐ Retrieval / Understanding: Why is it unsafe to use simple passwords like your name or 123456? ☐ Application: What specific steps should you follow if you suspect someone else knows your password? ☐ Critical Thinking: Why does the school require everyone to change their default password, and why must your new password match your	Teacher to assist as needed. More able pupils to support nearby peers. Consider seating plan or ICT buddy system.	Log in details

		30–50 Minutes Direct students to the "Shield Studio" creative extension module on the webpage to deepen their engagement with password creation and physical device care. Working individually or in pairs, pupils first complete Part A by creating an original 3-random-word passphrase and writing a brief explanation of why passphrases are easy for humans to remember but computationally difficult for brute-force hacking scripts to crack. Students then move to Part B, using the enlarged drawing canvas to design a custom "Cyber Defender Badge" or illustrate a key workstation care rule (such as cable management or headphone storage). Once complete, students click "Download My Security Badge Artwork" to download their .png drawing to their student drive. 50–60 Minutes Lead a whole-class discussion reviewing the lesson's key outcomes. Have selected students share their created passphrases and explain why simple or default passwords put personal digital identities at risk on a shared network. Oversee a secure account logout procedure and ensure all students leave their desks, chairs, and cables clean and tidy before exiting the suite.	record sheet exactly?		
ICT Lesson 2	• UK NC: R5.5 (Recognize online behavior and respect privacy boundaries). • ISTE: 1.2.a (Manage digital identity/reputation), 1.2.b (Respect privacy boundaries of others). • CSTA: 1B-NI-05 (Analyze risks)	0–10 Minutes Students log onto their workstations and open the typing practice link on the class website to complete a targeted warm-up. This custom typing session focuses on digital identity vocabulary—such as <i>footprint</i>, <i>reputation</i>, <i>profile</i>, <i>assumption</i>, <i>opinion</i>, and <i>privacy</i>—to establish finger placement while introducing the core concepts of the lesson. Circulate around the room to ensure lower-attaining students prioritize keyboard accuracy and proper posture over speed. 10–35 Minutes Direct students to launch the embedded "Interactive Profile Inspector & Drawing Studio" module on the class webpage. Explain that students will act as digital detectives to analyze three distinct online activity feeds (Gurpreet, Mark, and Leah) side-by-side with	☐ Retrieval / Understanding: What is the difference between a fact, an opinion, and an assumption when reading someone's online profile? ☐ Application: Looking at Gurpreet, Mark, or Leah's posts,	Teacher to assist as needed. More able pupils to support nearby peers. Consider seating plan or ICT buddy system.	Log in details

	associated with public data sharing).	specific analytical questions. Working individually or in pairs, students examine each character's posts, check-ins, and searches—distinguishing between proven facts (e.g., event check-ins or posts) and unproven assumptions a stranger might make. For each character, pupils type their findings into the input fields, read the revealed true biographical facts, and use the integrated drawing canvas to draw an icon or scene representing that person's true hobbies and identity. Once all three profiles are evaluated, pupils complete a final reflection on Slide 4 explaining why online profiles can lead strangers to form incorrect judgments. They then click "Download Complete Portfolio & Drawings" to save their HTML assessment summary—complete with embedded canvas artwork—into their personal network folder. 35–50 Minutes Instruct students to click the Interland link on the website and launch the "Mindful Mountain" mini-game. Students navigate the virtual mountain rapids by evaluating real-time scenario prompts, making quick decisions about what information is safe to broadcast publicly versus what must be kept private or shared only with trusted contacts. This gamified practice reinforces the digital footprint and privacy concepts explored during the profile inspection activity. 50–60 Minutes Conclude the lesson with a whole-class verbal Exit Ticket. Ask individual students to explain why an online profile can never provide a complete or fully accurate picture of a person's real-life identity. Oversee a secure account logout procedure and ensure all desk spaces, chairs, and peripherals are left clean and tidy before students exit the computer suite.	what kind of image do they project to someone who doesn't know them personally? ☐ Critical Thinking: How can posting a single photo or comment online create a permanent impression that might be hard to change later?		
ICT Lesson 3	• UK NC: R5.4 (Understand risks of online contact and	0–10 Minutes Students log onto their workstations and launch the typing practice link on the class website (typingclub.com or your portal). Direct the pupils to start from the last level they achieved, focusing on correct finger placement, speed, and accuracy.	☐ Retrieval / Understanding: How might a parent, a	Teacher to assist as needed.	Log in details

	content), R5.5 (Digital relationships). • ISTE: 1.2.a (Understand permanence of digital footprint), 1.2.b (Respect privacy context). • CSTA: 1B-NI-05 (Evaluate data visibility across public and private settings).	Circulate around the room to support any pupils requiring log-in assistance. Keep all children on the typing task for an additional five minutes after everyone is logged in to ensure they have an opportunity to improve. 10–35 Minutes Gather the class to watch the embedded 'Beware What You Share' (Legends Family Adventure) video. Following the video, direct pupils to the interactive widget on the class website to answer the three reflection questions: <i>What did they notice? What issues were raised? What concerns did they have?</i>. Once completed, instruct students to click "Download Answers" to save their .txt file, open it, and copy-paste their reflections into their ongoing Computing Word document created in Lesson 1. Next, transition to the "Take a new point of view" activity. Split the children into groups and assign them to look at a character's online profile through the eyes of someone else (e.g., parents, teachers). Groups must discuss what conclusions these people would reach and decide what information should be crossed out or hidden from that specific viewer. Have each group present their findings to the rest of the class. Discuss how different situations call for different privacy levels, and how seeing the world from someone else's viewpoint is key to getting privacy right. 35–50 Minutes When the conversation reaches a natural pause, allow the children to move to the Interland link. Pupils may choose to explore one of the four gamified worlds: 'Tower of Treasures', 'Reality River', 'Mindful Mountain', or 'Kind Kingdom' to practice their internet etiquette. After they have completed a meaningful amount of their chosen level, use the screen control software to pause their screens and bring their attention back to the front. Ask the class to summarize the safety messages the game required them to follow. 50–60 Minutes Conduct the lesson plenary by recapping the core concepts of public versus private information. Ask the class the Exit Ticket question: <i>Why does "seeing the world from someone else's point of view" help us decide what is safe versus unsafe to share</i>	teacher, or a future employer view your profile differently than your friends would? ☐ Application: Which pieces of information on a public profile would you cross out or keep hidden if you wanted to protect your personal privacy? ☐ Critical Thinking: Why does "seeing the world from someone else's point of view" help us decide what is safe versus unsafe to share online?	More able pupils to support nearby peers. Consider seating plan or ICT buddy system.	
--	--	--	---	---	--

		<i>online?</i>. Invite children to share any big successes or problems using the screen share software to invite peer support. Oversee a secure account logout procedure and ensure all desk spaces, chairs, and cables are left clean and tidy before exiting the suite.			
ICT Lesson 4	• UK NC: R5.4 (Know different ways of reporting concerns about content and contact). • ISTE: 1.2.b (Engage in safe, ethical behavior), 1.2.d (Protect personal data). • CSTA: 1B-NI-05 (Identify cybersecurity risks and response mechanisms).	0–10 Minutes Students log onto their workstations and open the typing practice link on the class website. Direct the pupils to start from the last level they achieved, focusing on correct finger placement, speed, and accuracy. Circulate around the room to support any pupils requiring log-in assistance, giving the class an additional five minutes after logging in to ensure everyone has had a chance to improve. 10–35 Minutes Gather the class to watch the 'Hack Me If You Can' episode from the Legends Family Adventure. Following the video, direct pupils to the interactive widget on the class website to answer the three reflection questions: <i>What did they notice? What issues were raised? What concerns did they have?</i>. Once completed, instruct students to click "Download Answers" to save their .txt file and copy-paste their reflections into their ongoing Computing Word document. Next, transition to the "Keeping it Private" activity. Split the children into 5 groups and assign one scenario to each group. Groups must read the scenario, discuss their answers to the questions, and decide on the best course of action. Have each group present their findings to the class, focusing on the concerns and learning points raised during their discussions. 35–50 Minutes When the conversation reaches a natural pause, allow the children to move to the Interland link. Pupils may choose to explore one of the four gamified worlds: 'Tower of Treasures', 'Reality River', 'Mindful Mountain', or 'Kind Kingdom' to practice spotting scams and protecting their data. After they have completed a meaningful amount of their chosen level, use the screen control software to pause their screens and bring their	☐ Retrieval / Understanding: What is the difference between personal information (like your favorite food) and private information (like your home address or bank details)? ☐ Application: If you receive a message or see content online that makes you feel uncomfortable or unsafe, what are the exact steps you should take to report it? ☐ Critical Thinking: Why do some	Teacher to assist as needed. More able pupils to support nearby peers. Consider seating plan or ICT buddy system.	Log in details

		attention back to the front to discuss the messages they were being asked. 50–60 Minutes Conduct the lesson plenary by recapping the core concepts of the lesson. Ask the class the Exit Ticket question: <i>If you receive a message or see content online that makes you feel uncomfortable, what are the exact steps you should take to report it?</i> Invite children to share any big successes or problems using the screen share software to invite peer support. Oversee a secure account logout procedure and ensure all desk spaces, chairs, and cables are left clean and tidy before exiting the suite.	websites or online strangers try to collect your private details, and what tactics do they use to trick people?		
ICT Lesson 5	• UK NC: P5.1 (Understand variables/data transformation), P5.5 (Algorithm analysis). • ISTE: 1.5.a (Formulate problems for algorithmic solutions). • CSTA: 1B-NI-04 (Model data transformation), 1B-NI-05 (Encryption fundamentals). •	0–10 Minutes Students log onto their workstations and open the typing practice link on the class website (typingclub.com or your Ndovu portal). Direct the pupils to start from the last level they remember achieving, reminding them about correct finger placement and encouraging speed and accuracy. Keep all children on the typing task whilst you support those logging in, and then give the class an additional 5 or so minutes so everyone has had a chance to improve their typing skills. 10–35 Minutes Gather the class to introduce the concept of Encryption and the need to protect data. Explain that a Caesar cipher works by shifting the alphabet by a specific value. Direct students to launch the "Interactive Caesar Cipher Simulator" widget on the class website. Allow them to experiment with the slider to see how changing the shift value encrypts their text. Discuss the concept of <i>frequency analysis</i>—explaining that by looking at the most common letters in the English language (like 'E' or 'T'), codebreakers can easily crack random substitution ciphers. Instruct pupils to answer the three reflection questions in the widget, click "Download Answers," and copy-paste their responses into their ongoing Computing Word document. 35–50 Minutes Transition the class to the main coding activity by instructing them to click the "Launch Code.org Sign In" button (studio.code.org/users/sign_in). Once logged in, students	☐ Retrieval / Understanding: How does a Caesar cipher work, and how do you use a shift value to encrypt or decrypt a message? ☐ Application: How can frequency analysis (looking at the most common letters in a language) help you crack a random substitution cipher?	Teacher to assist as needed.	Log in details

		should navigate to the Encryption module (section_id=6731025). In this module, students will try their own hand at cracking a message encoded with the classic Caesar cipher and a Random Substitution Cipher. Encourage children to work at their own pace, utilizing frequency analysis to solve the puzzles. Note that this is a large module, and they should simply go as far as they can during the allotted time, supporting peers who need help. 50–60 Minutes Bring the class back together to recap the content of the lesson. Conduct a verbal Exit Ticket asking: <i>Why are simple substitution ciphers considered weak, and why is strong encryption essential for daily life on the internet (like online banking or secure messaging)?</i>. Use screen sharing software to allow children to show what they have achieved or to share any big problems and invite support from their peers. Oversee a secure account logout procedure and ensure all desk spaces, chairs, and cables are left clean and tidy before exiting the suite.	☐ Critical Thinking: Why are simple substitution ciphers considered weak, and why is strong encryption essential for daily life on the internet (like online banking or secure messaging)?		
ICT Lesson 6	• UK NC: P5.1 (Data manipulation), P5.2 (Selection/Conditionals in systems). • ISTE: 1.5.a (Understand distributed computational models). • CSTA: 1B-NI-04 (Network data transmission and verification), 1B-NI-05 (Cryptographic keys).	0–10 Minutes Students log onto their workstations and open the typing practice link on the class website. Direct the pupils to start from their last saved level, encouraging speed and accuracy. Keep all children engaged in the typing task while you support those logging in, giving the class an additional 5 minutes to settle. 10–30 Minutes Gather the class to introduce the concepts of Public-Key Cryptography and Blockchain. Explain that public and private keys are used together to create a unique digital signature that proves a message's authenticity. Direct pupils to Simulator 1: Digital Signatures on the class website. Instruct them to type a message containing details a hacker might want to change (like an amount of money or a person's name), sign it, and then act like a hacker by altering the text. When they click	☐ Retrieval / Understanding: What is the difference between a public key and a private key in cryptography? ☐ Application: How does a digital signature prove that a message came from a specific person without	Teacher to assist as needed. More able pupils to support nearby peers. Consider seating plan or ICT buddy system.	Log in details

		verify, the simulator will flash a red hack detection warning, proving the signature broke. Next, direct them to Simulator 2: Mine a Blockchain. Explain that a blockchain is a shared ledger where everyone has a copy. Instruct them to click "Mine" on all three blocks to secure the chain (turning it green). Then, ask them to play the role of a hacker by changing the transaction text in Block 1. They will physically see that because Block 2 relies on Block 1's "Fingerprint" (hash), the entire chain breaks and turns red if tampered with. 30–40 Minutes Have students watch the embedded widescreen YouTube video ("<i>Blockchain: Societal Impact</i>") to understand how blockchain is used beyond cryptocurrency, such as for tracking energy grids or replacing lawyers for secure contracts, as well as noting its environmental impact. Have them answer the two reflection questions on the webpage, click "Download Lesson 6 Report," and paste their work into their ongoing Word documents. 40–55 Minutes Transition the class to the main Code.org activity. Instruct students to click "Launch Code.org Blockchain" which will take them directly to Level 1 of their assigned Blockchain unit. In this module, students will dive deeper into simulating blockchain transactions, mining blocks on a larger scale, and seeing how public ledgers prevent cheating by allowing everyone to view the transaction history. Support students who need help as they progress at their own pace. 55–60 Minutes Bring the class back together for the plenary. Conduct a verbal Exit Ticket asking: <i>Why is it impossible for a hacker to change information in an old block without everyone on the network noticing?</i> Use screen sharing software to allow children to show off what they have achieved on Code.org or invite peer support for any challenging puzzles. Oversee a secure account logout procedure and ensure all desk spaces are tidy before the class is dismissed.	revealing their private password? ☐ Critical Thinking: How does a shared, public ledger (blockchain) allow people to make secure transactions without needing a bank or central authority to trust?		
--	--	--	---	--	--

ICT Lesson 7 and 8	• UK NC: R5.5 (Evaluate online financial/informational risks), P5.1 (Variables in financial modeling). • ISTE: 1.2.d (Understand digital technology economics/privacy), 1.5.a (Analyze system variables). • CSTA: 1B-NI-05 (Real-world application of encryption and digital assets). •	0–10 Minutes Students log onto their workstations and open the typing practice link on the class website. Direct the pupils to start from their last saved level, encouraging speed and accuracy. While they type, introduce the key vocabulary for the next two weeks (<i>investment, stablecoin, cryptocurrency, NFT, volatile</i>). 10–35 Minutes Gather the class to introduce the "Crypto Investment Firm" simulation. Explain the goal: students will start with \$1500 and must decide how to invest it across three different digital assets—a volatile Cryptocurrency, a safe Stablecoin, and a highly unpredictable NFT. Group the students into pairs. Explain the Multiplayer Challenge: 1. One student in each pair decides on a secret "Market Code" (e.g., APPLES-99). 2. Both students type that exact code into the Setup Screen on their individual computers and click Start. 3. <i>Teacher Tip: Because the simulation uses "Seeded Mathematics", sharing the code ensures both students experience the exact same "fake news" events and price crashes, allowing them to compete fairly side-by-side.</i> Instruct the pairs to play through the 5 "Months" (rounds). They must read the news flash each month, discuss how they think the news will affect public perception, and make buy/sell decisions. When the game ends, have them compare their Final Net Worth. Encourage them to hit "Play Again," invent a new Market Code, and try a different investment strategy. 35–45 Minutes Bring the class back together to discuss the impact of fake news and public perception on financial value. Direct the pupils to the Evaluating Risk Reflection section on the website.	☐ Retrieval / Understanding: How does news or public perception change the financial or social value of digital assets like cryptocurrencies and NFTs? ☐ Application: When fake news or sudden market stories occur during the simulation, how should an investor analyze the information before deciding to buy or sell? ☐ Critical Thinking: Beyond purely financial investments, what are some practical or	Teacher to assist as needed. More able pupils to support nearby peers. Consider seating plan or ICT buddy system.	Log in details

		Have them type their answers to the two questions, click "Download Lesson 7 & 8 Report," and paste their final net worth and answers into their ongoing Computing Word document. 45–55 Minutes For students who finish early, direct them to click the "Launch Code.org Blockchain" extension button at the bottom of the page. They can use this time to continue progressing through their assigned Level 2 modules, gaining further insight into how the blockchain mathematically supports these digital assets. 55–60 Minutes Conduct the lesson plenary. Ask the class the Exit Ticket questions: <i>How did fake news stories impact the price of the NFT? Did anyone manage to beat the market, or is investing in highly volatile assets essentially gambling?</i> Oversee a secure account logout procedure and ensure all desk spaces are tidy before the class is dismissed.	ethical reasons why blockchain technology might be useful or risky for society in the future?		
--	--	---	--	--	--