

Appendix 5 - Senior School - Computer Science

1 st Year	Cyberbullying	Define the term Cyberbullying Give examples of forms of Cyberbullying Define the term trolling. Identify ways to prevent/ report Cyberbullying & trolling
	Social Media	List the features & issues of common social media apps Understand that some people are not who they say they are online Identify the dangers of using social media List the ways to make your profiles private
	Fake news	Know what is meant by fake news and why people publish it. Understand a number of ways in which you can spot fake news. Demonstrate your understanding of fake news in a given scenario.
	Online Challenges & Trends	Know what is meant by an online challenge, trend and hoax Identify when challenges are safe and when they become dangerous Identify ways to stay safe and what to do if challenges are not safe
	Online Security	Know what is meant by phishing and online scams. Be able to spot an online scam and how it can present themselves in different formats. Identify the measures that can be put in place to avoid becoming a victim of an online scam.
	AI	Know what AI is Understand how AI learns Understand how AI recognises images Discuss the benefits and drawbacks of AI Understand AI Bias
RSE Points Covered- Autum Term Topic 2- Online Safety <u>Respectful relationships, including friendships</u> -The characteristics of positive and healthy friendships (in all contexts, including online		

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help

-how stereotypes, in particular stereotypes based on sex, gender, race, religion, sexual orientation or disability, can cause damage (for example, how they might normalise non-consensual behaviour or encourage prejudice)

Online and media

-their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.

- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.

- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.

- what to do and where to get support to report material or manage issues online.

- the impact of viewing harmful content.

- how information and data is generated, collected, shared and used online.

Internet safety and harms

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online.

-how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

2 nd Year	Autumn Term- Topic 1- Cyber Security	
	Introduction to Cyber Security	Explain the difference between data and information Critique online services in relation to data privacy Identify what happens to data entered online Explain the need for the Data Protection Act
	Social Engineering	● Define social engineering - Social engineering is manipulating people into handing over confidential information such as a PIN or password. ● There are several forms: blagging/ phishing/ shouldering ● Define the term shouldering/ Give examples of shouldering/ Explain how to prevent shouldering ● Define the term blagging/ Give examples of blagging/ Explain how to prevent blagging ● Define the term phishing/ Give examples of phishing / Explain how to prevent phishing
	Malware	● Define the term malware & give examples ● Understand the term malicious intent ● Malicious intent includes: Disabling hardware/ Data theft/ Forced advertising/ Sending email spam/ Extorting money ● Give the categories of malware – viruses/ trojans/worms/adware/ spyware/ ransomware ● Define the categories of malware ● Discuss precautions of malware ● keeping your operating system up to date ● using up to date anti-virus software ● not opening an email attachment unless you are expecting it and know the source ● not allowing other users to use their own memory stick on your system ● only downloading files from reputable web sites ● avoiding software from unreliable sources ● Describe Antivirus software ● Describe how a firewall works ● substantial financial loss arising from: theft of corporate information/ theft of financial information (eg bank details or payment card details)/ theft of money/ loss of business or customers/ Loss or reputation/ Legal consequences - GDPR

	Network Security	Understand what threat is the greatest and poses the most risk Describe ways to prevent or secure networks from Cyber attacks including Anti-Malware, Auto Updates, User Authentication & User Permissions	
	Encryption	What does the HTTPS symbol mean on a web address What is Encryption? Why do we need to encrypt our data? What data would you want to be encrypted? Why? Explain the process of encryption • A key is used to encrypt plain text into meaningless cipher text • The same key is used to decrypt the data back into its original form. • Only someone who knows the key can decrypt the cipher. • If you don't have the key you need to crack the code. • Which famous computer scientist studied and worked in cryptography in WWII? / What code did they break? Discuss Alan Turing & show the video of breaking the enigma machine • The Caesar cipher is one of the simplest and most widely known encryption techniques. Each character is shifted in the alphabet a fixed number of positions	
RSE Points Covered <u>Online and media</u> - about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online. - not to provide material to others that they would not want shared further and not to share personal material which is sent to them.			

- what to do and where to get support to report material or manage issues online.

-How information and data is generated, collected, shared and used online.

Internet safety and harms

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, **how advertising and information is targeted at them and how to be a discerning consumer of information online.**