Progression route

Learning Journey		E-Safety			
KS1 NC aims: 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.		**KS2 NC aims:** Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.			
Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**
To know what personal information is and be able to give examples. Recognise that there may be people online who could make people feel sad, embarrassed or upset. To know who to go to for help with problems regarding digital activity.	Explain how other people's identity online can be different to their identity in real life, also understand that any things that is artificial intelligence is not a real person. To know what private means and which data should be kept private. To know that we do not share personal information with real people we do	To know how to create a secure password. To confidently know how to search the internet safely (including AI tools) and choose age-appropriate resources and website, including responses that are produced by AI. To know what a digital footprint is and that any information online	To know the reasons why we need to limit our technology use and explain the risks linked to it (health risks), including mental health. To know what a virus is and how we protect computers from harm. Explain why they need to think carefully about how content they post might affect	To distinguish between appropriate and inappropriate uses of technology, including AI (including excessive use) (link to mental health/social risks). To know the risks and rewards of the internet, including the use of AI. To know a variety of ways to report concerns both on and offline. To	To know how to protect themselves from being victims of cyberbullying and causing harm to others. To know how to respect, including gaining consent, others online and understand their responsibility for how their information and that of others can affect themselves and others.

Describe how to behave online in ways that do not upset others and can give examples.	not know, as well as AI. To know to ask a trusted adult before clicking 'yes' 'I agree' or 'accept'. To identify safe and unsafe online behaviours, including online devices without supervision. Begin to know how to search the internet safely, including that some responses maybe AI generated.	can be used by others, including the use of AI. To know how to create a positive online presence. Explain what it means to 'know someone' online and why this might be different from knowing someone in real life. To understand that AI is not a real person but is a computer programme that is trying to emulate being a human.	others, their feelings and how it may affect how others feel about them. To become aware of 'fake news' and learn how to assess what they read. To understand that not all AI provided content is correct or factual and therefore may not be reliable.	understand reporting concerns to AI is not a trust adult. To know how to use social media and online gaming apps effectively, while keeping an adult informed of their activity. To understand that many social media platforms have age limits in their user agreements for safety reasons. To know what copyright is and how to interpret information found online. To know what adverts/pop ups/ phishing emails are and how they are specifically	To know what the CEOP button is and why it is important in keeping safe online. Describe ways in which some online content, including AI, targets people to gain money or information illegally and can describe strategies to help them identify such content. Learn how to use the skills they have to respond to any challenges they might face when they leave primary school.

				targeted at individuals. To know that target phishing emails, adverts and pop ups can be informed by AI related digital footprints.	

Revision in other units:

Programming: Using the technology for its intended use.

Data Processing: Data must be handled safely and confidentially and not shared for anything other than the purpose it was created.

Multimedia: Asking for consent for photos. Assess and justify when it is acceptable to use the work of others- copyright. Demonstrate how to make references to and acknowledge sources I have used from the internet.

Networking: Not giving out personal information. Links to digital footprint- what you say can never be truly deleted. Internet searching safety tips (+ kids for safe and relevant information)

Digital fluency: Not giving out passwords. Not logging in as someone else.