

E-SAFETY STRAND	<u>EYFS</u>	<u>National Curriculum</u>	South West Grid for Learning Skills (E-Safety Week) Additional Purple Mash content Reporting concerns / Gaming & media / Online Behaviours & reputation / Passwords & Sharing Personal info / Stranger Danger / Virus Danger / Copyright / Lifestyle
Reception	*ELG Technology: Talk about how they used technology at home *ELG Health & Self Care: talk about how to stay safe	/	<ul style="list-style-type: none"> Identify safe behaviours in their day to day world and how this applies in the online world. Understand what constitutes a trusted adult and identify the trusted adults in their lives. Understand that they should only go online or play games that are approved by trusted adults If they come across something upsetting to tell a trusted adult immediately. Know how they should behave and interact with others in the real and that these behaviours should be the same in the virtual world. Identify the activities, content and games they are accessing in school / home and demonstrate or talk about how they would do so safely and politely.
Year 1	/	use technology safely and respectfully, keeping personal information private;	<ul style="list-style-type: none"> Know to tell a trusted adult any worries Begin to understand the idea of personal information and they should not give out information about themselves. Understanding the need to have permission to share photos Being kind online just like in real life Logging in with a password Ownership of creative documents
Year 2	/	identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies	<ul style="list-style-type: none"> Understand that they should only go online or play games that are approved by trusted adults and that if they come across something upsetting to tell a trusted adult immediately. Understand that when they are playing games or online the characters they are interacting with could be computer generated characters or real people in other parts of the world and they should be able to identify if they are real or fictitious. Begin to understand the idea of personal information and that this includes their full name, address, school name, phone number and date of birth and why using a nickname is a safer way to interact online. Know to talk to a trusted adult before submitting or sharing their full name, address, school name, phone number and date of birth online. Ensure a trusted adult is aware of who they are interacting with online and has approved the interactions because some people online may not be who they say they are. Identify appropriate online communication that is polite and respectful. Understand that just because they cannot see the person they are communicating with it doesn't mean that they should communicate differently. The person will still be hurt or upset by things you say or do online that are unpleasant. Know to tell a trusted adult if others are communicating / interacting with them in an unpleasant manner. Understand that passwords should only be shared with trusted adults and describe what might happen if somebody else has their login details. How to talk to people online who are not there in front of us Putting work online leaves a digital footprint

<p>Year 3</p>	<p>/</p>	<p>Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact</p>	<ul style="list-style-type: none"> • Know to get a trusted adult's approval before clicking links, pop ups and attachments that they may come across online and in games and be aware of some of the consequences of clicking such links. • Be able to identify / classify personal information about themselves, their friends and others and comment on the types of information they can find about people in the newspapers and online. • Be able to identify a range of personal information and justify who they might safely share it with in discussion with a trusted adult. • Understand that sharing personal information with people they do not know or trust (through games and other online activity) could lead to strangers trying to meet up with them or communication they find upsetting or confusing. Children should know to report such communication to a trusted adult immediately. • Explain what bullying is and identify some acceptable and unacceptable ways to communicate / interact with others in the real world. • Discuss the various technologies they use to communicate / interact with each other and how they can be used to communicate in a positive manner. • Understand the term cyberbullying and be able to explain what to do if they or a friend is cyberbullied. • Know not to believe or accept everything they see online as correct or truthful and know to check this with a second site or only use sites recommended by trusted adults • Safe passwords • Contributing correctly to a blog and emailing safely • Website aren't always true • Age restrictions and PEGI rating • Who to ask for help online
<p>Year 4</p>	<p>/</p>	<p>Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact</p>	<ul style="list-style-type: none"> • Understand the PEGI system and be able to describe the icons for the ratings. • Be able to classify some of the games they play and explain why they are or are not appropriate for a given age group. • Understand that many websites ask for personal information to set up an account and why this is often age restricted to 13. • Know not to enter personal information online without the help of a trusted adult and question why the site needs their information and what they will do with it. • Describe some of the reasons this information might be shared and the problems it might cause. • Identify the similarities and differences between written and verbal communication and understand that sometimes these can be misinterpreted. • Understand the concept of 'Netiquette' and how other online users can make positive and negative judgements about a person based solely on our online interactions. • Describe and share ways our online interactions can ensure that we create a positive online persona. • Understand what constitutes a strong password and discuss strategies for creating strong personal passwords that are easy to remember. • Describe the reasons to set passcodes / passwords for all devices and the implications of leaving these devices unlocked when not in use • Children should know to report problems in communication to a trusted adult immediately. • Protection from online theft • Digital print can aid theft • Risks and benefits of installing apps and software • Copyright • Plagiarism and consequences

			<ul style="list-style-type: none"> • Appropriate behaviour during collaborative work • Balanced lifestyle
<p>Year 5</p>	<p>/</p>		<ul style="list-style-type: none"> • Know what plagiarism / copyright are and understand people often plagiarise without thinking by cutting and pasting. • Understand the legal and moral reasons not to plagiarise or infringe copyright, the impact it can have on the creator of the content and know legal download sites for video and music. • Understand how to simply reference others people's work you have permission to use and know how to search for copyright free content. • Be aware that anybody can publish information online and identify examples such as blogs, YouTube, etc. Identify simple steps to help ensure information is accurate and reliable such as using multiple sources and identifying reliable sources such as the BBC, National Museums, etc. • Children should know how to report or block users within the games, apps and websites they use and make reports to external agencies including CEOP and ChildLine in conjunction with a trusted adult. • Children can unsubscribe and block emails they do not wish to receive. • Children should be able to differentiate between online only 'friends' and real world friends they connect to online. • Children should not share personal information with people they do not know in the real world. □ Understand that once content is shared online it can be almost impossible to remove from the Internet. • Know how to configure appropriate security settings including accepting and blocking 'friends' and ensure their parents are aware of all the online friends they are interacting with. • Understand how technology can be misused to cyberbully and the short and long-term consequences this can have on the victims. • Outline strategies and behaviours they can embrace to ensure they are not involved in cyberbullying and how to report cyberbullying incidents using real world and online reporting mechanisms. • Impact of sharing • Responsibility of online behaviour • Maintain secure passwords • Altering images digitally • Referencing sources • Reliability of search results - checking validity
<p>Year 6</p>	<p>/</p>		<ul style="list-style-type: none"> • Understand the concept of a balanced lifestyle and be aware of the amount of time they are spending in front of a screen and the impact this may have on their physical and mental health. • Describe non screen activities they can engage in to ensure they have a balanced lifestyle. • Understand that any information about them shared online by themselves and others could be accessed by anybody in years to come and that this 'trail' of digital information creates a 'digital footprint' about them. • Identify all the different sources and types of information that might already be online about themselves and what control they have over this information. • Describe positive and negative implications of anybody accessing their 'digital footprint' now and in the future. • Describe what steps they can take to creating a 'positive online image' including defining acceptable and unacceptable online behaviour and the benefits this will have to them now and in the future. • Understand that to remain safe and secure online you need to ensure the devices you use to connect online are suitably secure and that you are using a secure connection including, games consoles, tablets and mobile phones.

			<ul style="list-style-type: none">• Ensure you have approval from a trusted adult before using a webcam.• Understand the terms antivirus, firewall, security updates, pop up blocker, scams, phishing, HTTPs, location based settings, in app purchasing, trolling, filtering, malware, etc.• Create and regularly update strong passwords and do not use the same password for all accounts and devices.• Use PEGI ratings and other criteria to identify the (e)Safeguarding issues with regard to a range of games and online content to make informed judgements on the suitability of the content for a given age range• Risk and benefits of location sharing• Identifying private sites - https padlock. Benefits and risk of giving access to different software• Own digital footprint• Appropriate online behaviour• Longevity of online information• Balanced lifestyle• Moderation on blogs
--	--	--	---