How to stay safe online

- Online relationships
- Privacy and Security
- Online Reputation
- Online Bullying

Potential harm or risk online	Description	What pupils are taught
Abuse (online)	Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal	• Explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation • Explanation of when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail • How to respond to online abuse including how to access help and support • How to respond when the abuse is anonymous • Discussing the potential implications of online abuse, including implications for victims • Being clear what good online behaviours do and don't look like.
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest.	• Explaining what an online challenge is and that while some will be fun and harmless, others may be dangerous and or even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • Explaining to pupils that it is ok to say no and not take part • How and where to go for help if worried about a challenge • Understanding the importance of telling an adult about challenges which include threat or secrecy ('chain letter' style challenges).
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence.	• Ensuring pupils know that online content (sometimes gang related) can glamorise the possession of weapons and drugs • Explaining that to intentionally encourage or assist an offence is also a criminal offence • Ensuring pupils know how and where to get help if worried about involvement in violence.

Fake profiles	Not everyone online is who they say they are.	• Explaining that in some cases profiles may be people posing as someone they aren't (i.e. an adult posing as a child) or may be "bots" (which are automated software programs designed to create and control fake social media accounts)
		• How to look out for fake profiles. This could include:
		  • Profile pictures that don't like right, for example of a celebrity or object
		  • Accounts with no followers or thousands of followers; and a public figure who doesn't have a verified account.

Grooming	Knowing about the different types of grooming and motivations for it, for example radicalisation, Child Sexual Abuse and Exploitation (CSAE) and gangs (county lines).	• Boundaries in friendships with peers and also in families and with others • Key indicators of grooming behaviour • Explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult; • How and where to report it both in school, for safeguarding and personal support, and to the police. Where there are concerns about sexual abuse and exploitation these can also be reported to Click CEOP.
Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children but it carries risk when carrying it out and watching it.	• Explaining the risks of carrying out live streaming. These include the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent. As such pupils should think carefully about who the audience might be and if they would be comfortable with whatever they are streaming being shared widely • Online behaviours should mirror offline behaviours and considering any live stream in that context. Pupils shouldn't feel pressured to do something online that they wouldn't do offline. Consider why in some cases people will do and say things online that they would never consider appropriate offline • Explaining the risk of watching videos that are being live streamed, for example there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance • Explaining the risk of grooming
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know/have never met.	• Explaining that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with • Identifying indicators or risk and unsafe communications, identifying risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before • Explaining about consent online and supporting pupils to develop strategies to confidently say "no" to both friends and strangers online.

Teaching online safety in school June 2019 DfE