Potential Risks Online

- Managing Online Information
- Copyright and Ownership
- Privacy and Security

Potential harm or risk online	Description	What pupils are taught
Age Restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.	• That age verification exists and why some sites require a user to verify their age. For example, online gambling and purchasing of certain age restricted materials such as alcohol • Why age restrictions exist - for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers • Helping pupils understand how this content can be damaging to under-age consumers, • The age of digital consent the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations. Why it is important and what it means in practice.
Content: How it can be used and shared	Knowing what happens to information, comments or images that are put online.	• What a digital footprint is, how it develops and how it can affect future prospects such as university and job applications • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something a user wishes they had not shared • Ensuring pupils understand what is illegal online, especially what may in some cases be seen as “normal” behaviours, for example youth-produced sexual imagery (sexting). This could include copyright, sharing illegal content such as extreme pornography or terrorist content as well as the illegality of possession, creating or sharing any explicit images of a child even if created by a child.
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.	• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online • How to measure and check authenticity online

		• The potential consequences of sharing information that may not be true.
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other gain.	• How to look out for fake URLs and websites • Ensuring pupils understand what secure markings on websites are and how to assess the sources of emails • Explaining the risks of entering information to a website which isn't secure • What to do if harmed/targeted/groomed as a result of interacting with a fake website or scam email. Who to go to and the range of support that is available.
Fraud (Online)	Fraud can take place online and can have serious consequences for individuals and organisations.	• What identity fraud, scams and phishing are • That children are sometimes targeted to access adult's data, for example, passing on their parents or carers details (bank details, date of birth, national insurance number etc). Therefore there is a need to keep everyone's information secure not just their own • What "good" companies will and won't do when it comes to personal details, for example a bank will never ask you to share a password or move money into a new account.
Password phishing	Password phishing is the process by which people try to find out your passwords so they can access protected content.	• Why passwords are important, how to keep them safe and that others may try to trick you to reveal them • Explaining how to recognise phishing scams, for example those that seek to gather login in credentials and passwords • Importance of online security to protect against viruses (such as keylogging) that are designed to access/steal/copy passwords information • What to do when a password is compromised or thought to be compromised.
Personal data	Online platforms and search engines gather personal data. This is often referred to as 'harvesting' or 'farming'.	• How cookies work • How data is farmed from sources which look neutral, for example websites that look like games or surveys that can gather lots of data about individuals • How, and why, personal data is shared by online companies. For example data being resold for targeted marketing by email/text (spam) • How pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential • The rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR) • How to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time.
Persuasive design	Many devices/apps/games are designed to keep users online for longer than they might have planned or desired.	• Explaining that the majority of games and platforms are businesses designed to make money. Their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue • How designers use notification to pull users back online.
Privacy settings	Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared.	• How to find information about privacy setting on various sites, apps, devices and platforms • Explaining that privacy settings have limitations, for example they will not prevent someone posting something inappropriate.

Targeting of online content Including on social media and search engines	Much of the information seen online is a result of some form of targeting.	• How adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts • How the targeting is done, for example software which monitors online behaviour (sites they have visited in the past, people who they are friends with etc) to target adverts thought to be relevant to the individual user • The concept of clickbait and how companies can use it to draw people onto their sites and services.

Teaching online safety in school June 2019 DfE