Department for Education

Teaching online safety in school

Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects

June 2019

Contents

Summary

1. This is non-statutory guidance from the Department for Education.

2. It outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. It complements existing and forthcoming subjects including Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing. It does not imply additional content or teaching requirements.

Expiry or review date

3. This guidance will be reviewed before September 2020.

Who is this publication for?

4. This guidance is for school leaders, school staff and governing bodies. It applies to all local authority maintained schools, academies and free schools.

5. The interventions and support information may also be helpful for early years settings, colleges and other post-16 institutions.

Main points

6. It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app (page 6).

7. However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils (page 8).

8. Schools can refer to the Education for a Connected World Framework for age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

9. When planning their curriculum, and how online safety fits within it, there are a number of areas we recommend schools consider, for example how to support vulnerable pupils (page 24).

10. We recommend that schools embed teaching about online safety and harms within a whole school approach (page 26).

Introduction

11. Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

12. We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

13. This advice brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach.

Curriculum context

14. From September 2020, Relationships Education will be compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England.

15. Through these new subjects, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.

16. This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

17. There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example citizenship education covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

18. This advice supports schools to consider what they are already delivering through the curriculum, and build in additional teaching as required to ensure their pupils are receiving a fully rounded education with regard to online safety, both in terms of how to stay safe but also how to behave online.

Teaching about online safety

Underpinning knowledge and behaviours

19. The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

20. It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching must always be age and developmentally appropriate.

21. Underpinning knowledge and behaviours include:

- **How to evaluate what they see online -** This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

  Schools can help pupils consider questions including:

  - is this website/URL/email fake? How can I tell?
  - what does this cookie do and what information am I sharing?
  - is this person who they say they are?
  - why does someone want me to see this?
  - why does someone want me to send this?
  - why would someone want me to believe this?
  - why does this person want my personal information?
  - what's behind this post?
  - is this too good to be true?
  - is this fact or opinion?

- **How to recognise techniques used for persuasion** – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

  Schools can help pupils to recognise:

  - online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
  - techniques that companies use to persuade people to buy something,

- ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and
- criminal activities such as grooming.

- **Online behaviour** – This will enable pupils to understand what acceptable and unacceptable online behaviour look like. Schools should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

  Schools can help pupils to recognise acceptable and unacceptable behaviour by:

  - looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
  - looking at how online emotions can be intensified resulting in mob mentality,[1]
  - teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and
  - considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

- **How to identify online risks** – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

  Schools can help pupils to identify and manage risk by:

  - discussing the ways in which someone may put themselves at risk online,
  - discussing risks posed by another person's online behaviour,
  - discussing when risk taking can be positive and negative,
  - discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example,

[1] Mob mentality describes how people can be influenced by their peers to adopt certain behaviors on a largely emotional, rather than rational, basis

- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

- **How and when to seek support –** This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

  Schools can help pupils by:

  - helping them to identify who trusted adults are,
  - looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
  - helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Harms and risks

22. Understanding and applying the knowledge and behaviours above will provide pupils with a solid foundation to navigate the online world in an effective and safe way. However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils.

23. The tables below will help school staff understand some of the issues their pupils may be facing and where these could be covered within the curriculum. Schools should consider when it might be appropriate to cover these individual harms and risks. Any activity that does look at individual harms and risks should be considered in the broader context of providing the underpinning knowledge and behaviours, as set out in the previous section of this guidance.

24. Throughout the following sections we signpost to the Education for a Connected World Framework which includes age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives, including how to navigate online safely. This was developed by the UK Council for Internet Safety.

How to navigate the internet and manage information

25. This section covers various technical aspects of the internet that could leave pupils vulnerable if not understood.

26. Age specific advice on these potential harms and risks can be found in the following sections of the Education for a Connected World framework:

- Managing online information
- Copyright and ownership
- Privacy and Security

The potential harm or risk[2]	Description	Curriculum area this could be covered in
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching could include: • 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.	Health Education core content – internet safety and harms. "why social media, some computer games and online gaming, for example, are age restricted" Computing curriculum – some schools may want to discuss age restrictions as part of e-safety (all ages) "use technology safely and respectfully"

[2] There are activities which although not in and of themselves harmful, could, if not understood be a risk to a child's safety or in some cases their privacy or personal data.

The potential harm or risk[2]	Description	Curriculum area this could be covered in
Content: How it can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching could include: • 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.	Relationships education core content (all stages) – online relationships. "how information and data are shared and used online" Relationships education, relationships and sex education and health education – the law "Pupils should be made aware of the relevant legal provisions when relevant topics are being taught" RSE (Secondary) core content – online and media. "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." and "not to provide material to others that they would not want shared further and not to share personal material which is sent to them." and "that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail." Health education core content (all stages) – internet safety and harms "how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted." Computing curriculum (all key stages) – "identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies." Computing curriculum – may use

The potential harm or risk[2]	Description	Curriculum area this could be covered in
		this as part of wider teachings around how information online is stored and used. “protecting their online identity and privacy”
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated. Teaching could include: • 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.	Relationships education (all stages), relationships and sex education (secondary) and health education (all stages) – the law “Pupils should be made aware of the relevant legal provisions when relevant topics are being taught” Computing curriculum (key stages 2 and above) - “use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content” Citizenship: Key Stage 3 - Pupils should use and apply their knowledge and understanding while developing skills to research and interrogate evidence, debate and evaluate viewpoints, present reasoned arguments and take informed action Citizenship Key Stage 4 - Pupils should develop their skills to be able to use a range of research strategies, weigh up evidence, make persuasive arguments and substantiate their conclusions
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. Teaching could include: • how to look out for fake	Relationships education (all stages), relationships and sex education (secondary) and health education (all stages) – the law “Pupils should be made aware of the relevant legal provisions when relevant topics are being taught” Computing curriculum (all key

The potential harm or risk[2]	Description	Curriculum area this could be covered in
	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.	stages) - "use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content"
Fraud (online)	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching could include: • what identity fraud, scams and phishing are, • that children are sometimes targeted to access adults 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.	Relationships education core content – online relationships. "that people sometimes behave differently online, including by pretending to be someone they are not." Computing curriculum (all key stage) – "use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content"
Password phishing	Password phishing is the process by which people try to find out your passwords so they can access protected content. Teaching could include: • why passwords are important, how to keep them	Relationships education core content (all stages) - online relationships. "the rules and principles for keeping safe online" Computing curriculum (all key stages) – "use technology safely, respectfully and responsibly"

The potential harm or risk[2]	Description	Curriculum area this could be covered in
	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'. Teaching could include: • 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,	Relationships education core content (all stages) – online relationships. "how information and data is shared and used online" RSE (secondary) core content – online relationships. "how information and data is generated, collected, shared and used online" Computing curriculum (all key stages) – "use technology purposefully to create, organise, store, manipulate and retrieve digital content. Computing curriculum (all key stages) – "use technology safely and respectfully, keeping personal information private"

The potential harm or risk[2]	Description	Curriculum area this could be covered in
	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. Teaching could include: • 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.	Health education core content (all stages) – internet safety and harms. "about the benefits of rationing time spent online, the risks of excessive internet time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing" Health education (secondary) core content – internet safety and harms "the risks related to online gambling including the accumulation of debt." Computing curriculum (all key stages) – "use technology safely, respectfully and responsibly"
Privacy settings	Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared. Teaching could include: • 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.	Relationships education core content – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them." Computing curriculum (all key stages) – "understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy"
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.	Health education – core content (all stages) - internet safety and harms. "how to be a discerning consumer of information online including understanding that

The potential harm or risk[2]	Description	Curriculum area this could be covered in
	Teaching could include: • 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.	information, including that from search engines, is ranked, selected and targeted" Computing curriculum (all key stages) – "use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content"

How to stay safe online

27. This section covers elements of online activity that could adversely affect a pupil's personal safety or the personal safety of others online.

28. Age specific advice on these potential harms and risks can be found in the following sections of the Education for a Connected World framework

- Online relationships
- Privacy and Security
- Online reputation
- Online bullying

The potential harms or risk	Description	Curriculum area this could be covered in
Abuse (online)	Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal. Teaching could include	Relationships education core content (all stages) – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact,

The potential harms or risk	Description	Curriculum area this could be covered in
	• 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.	and how to report them." Relationships Education core content (all stages) – online relationships. "about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help." Relationships education, relationships and sex education and health education – the law "Pupils should be made aware of the relevant legal provisions when relevant topics are being taught" Health education core content (all stages) – internet safety and harms. "that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health" Computing curriculum (all key stages) – "recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact." Citizenship : Key Stage 4 – Pupils should be taught about diverse national, regional, religious and ethnic identities in the United Kingdom and the need for mutual respect and understanding
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching could include: • explaining what an online challenge	Relationships education (all stages) and relationships and sex education (secondary) – "about online risks, including that any material someone provides to another has the

The potential harms or risk	Description	Curriculum area this could be covered in
	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).	potential to be shared online." Health Education core content (all stages) – "how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private", "how to be a discerning consumer of information online" and "where and how to report concerns and get support with issues online."
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching could include: • 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.	Relationships education (all stages), relationships and sex education (secondary) and health education (all stages) – the law "Pupils should be made aware of the relevant legal provisions when relevant topics are being taught".

Fake profiles	Not everyone online is who they say they are.
	
	Teaching could include:
	
	• 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
		Relationships education core content (all stages) – online relationships. "that people sometimes behave differently online, including by pretending to be someone they are not."
		
		Computing curriculum (all stages) – "identify a range of ways to report concerns about content and contact."

The potential harms or risk	Description	Curriculum area this could be covered in
	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). Teaching could include: • 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; and • 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. See the NCA-CEOP Thinkuknow website for further information on keeping children safe from sexual abuse and exploitation. At all stages it will be important to balance teaching children about making sensible decisions to stay safe whilst being clear it is never the fault of a child who is abused and why victim blaming is always wrong.	Relationships Education (all stages) and Relationships and Sex Education (secondary) – "the characteristics of positive and healthy friendships (in all contexts, including online)". Relationships and Sex Education (secondary) includes, for example, "the concepts of, and laws relating to, sexual consent, sexual exploitation, abuse, grooming, coercion … and how these can affect current and future relationships" and "how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)."
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. Teaching could include: • explaining the risks of carrying out	Relationships education core content (all stages) – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them" Health education (secondary)

The potential harms or risk	Description	Curriculum area this could be covered in
	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 - see above for more on grooming.	core content – internet safety and harms. "the impact of viewing harmful content"
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching could include: • that pornography is not an accurate portrayal of adult sexual relationships, • viewing pornography can lead to skewed beliefs about sex and in some circumstances can normalise violent sexual behaviour, • that not all people featured in pornographic material are doing so willingly, i.e revenge porn or people trafficked into sex work.	RSE (secondary) core content – online and media. "that specifically sexually explicit material e.g. pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners."

The potential harms or risk	Description	Curriculum area this could be covered in
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know/have never met. Teaching could include: • 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.	Relationships education core content (all stages) – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them." and "how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met." Relationships Education core content (all stages) – respectful relationships. "the importance of permission-seeking and giving in relationships with friends, peers and adults" RSE (secondary) core content – "the characteristics of positive and healthy friendships (in all contexts, including online) including: trust, respect, honesty, kindness, generosity, boundaries, privacy, consent and the management of conflict, reconciliation and ending relationships. This includes different (non-sexual) types of relationship" Computing curriculum (all key stages) – "identify a range of ways to report concerns about content and contact."

Wellbeing

29. This section covers the elements of online activity that can adversely affect a pupil's wellbeing.

30. Age specific advice on these potential harms and risks can be found in the following sections of the Education for a Connected World framework:

- Self-image and identity
- Online reputation
- Online bullying
- Health, wellbeing and lifestyle

The potential harm or threat	Description	Curriculum area this could be covered in
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching could include • exploring the use of image filters and digital enhancement, • exploring the role of social media influencers, including that they are paid to influence the behaviour (particularly shopping habits) of their followers, • looking at photo manipulation including discussions about why people do it and how to look out for it.	Health education (secondary) core content – 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 and how people may curate a specific image of their life online)."
Impact on quality of life, physical and mental health and relationships.	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent on and offline. Teaching could include: • helping pupils to evaluate critically what they are doing online, why they are doing it, and for how long (screen time). This could include reference to technologies that help them to manage their time online, monitoring usage of different apps etc, • helping pupils to consider quality vs quantity of online activity, • explaining that pupils need to consider if they are actually enjoying being	Health Education core content (all stages) – internet safety and harms. "about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing."

The potential harm or threat	Description	Curriculum area this could be covered in
	online or just doing it out of habit, due to peer pressure or the fear of missing out, • helping pupils to understand that time spent online gives users less time to do other activities. This can lead to some users becoming physically inactive, • exploring the impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues, • explaining that isolation and loneliness can affect pupils and that it is very important for pupils to discuss their feeling with an adult and seek support, • where to get help.	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching could include • how and why people can often portray an exaggerated picture of their lives (especially online) and how that can that can lead to perfect/curated lives pressures, • discussing how and why people are unkind or hurtful online, when they would not necessarily be unkind to someone face to face.	Relationships Education core content (all stages) – online relationships. “that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous”
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively Teaching could include • looking at strategies for	RSE core content (secondary) – online and media. “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

The potential harm or threat	Description	Curriculum area this could be covered in
	positive use, • how to build a professional online profile	online."
Suicide, self-harm and eating disorders.	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using emotive language, videos or images. Guidance on teaching about mental health and emotional wellbeing provides useful support for teachers in handling this material.	

Additional considerations for schools

31. When planning their curriculum, and how online safety fits within it, we suggest schools consider carefully the following.

Vulnerable pupils

32. Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Schools should consider how they tailor their offer to ensure these pupils receive the information and support they need.

33. The following resources can help schools consider how best to support their most vulnerable pupils stay safe online:

- Vulnerable Children in a Digital World - Internet Matters
- Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group section 11
- STAR SEN Toolkit - Childnet

Use of external resources

34. Schools are best placed to make their own decisions about which resources are educationally appropriate for their pupils. This includes reviewing resources, even when from a trusted source, as some will be more appropriate to their cohort of pupils than others. Schools could should ask themselves:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are the resources age appropriate for our pupils?
- Are the resources appropriate for the developmental stage of our pupils?

Use of external visitors

35. Online safety can be a difficult and complex topic which changes very quickly. Therefore, schools may want to seek external support who have expertise, up to date knowledge and information. The right external visitors can provide a useful and engaging approach to deliver online safety messages, but this should enhance a school's offer rather than be delivered in isolation.

36. The UK Council for Internet Safety developed guidance for educational settings seeking support from external visitors to help explore issues such as cyberbullying, online pornography, 'sexting' and staying safe online. Schools can use this document to guide their process of selecting suitable visitors and sessions.

Teaching about online harms and risks in a safe way

37. As with any safeguarding lessons or activities, it is important that schools consider the topic they are covering and the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way.

38. It is important to create a safe environment in which pupils feel comfortable to say what they feel. If a pupil thinks they will get into trouble and/or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

39. Where schools are already aware of a child who is being abused or harmed online they should carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. It is good practice to include the Designated Safeguarding Lead (or a deputy) when considering and planning any safeguarding related lessons or activities (including online) as they will be best placed to reflect and advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

40. In some cases, a pupil will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the pupils to realise they are being abused or harmed and/or give them the confidence to say something. This is why it is essential all pupils are clear what the school's reporting mechanisms are. As per "Keeping Children Safe in Education" those mechanisms should be child friendly and operate with the best interests of the pupil at their heart.

Whole school approach

41. Whole-school approaches are likely to make teaching more effective than lessons alone. A whole school approach is one that goes beyond teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community.

42. We recommend that schools embed teaching about online safety and harms within a whole school approach. In practice, this means:

- **Creating a culture that incorporates the principles of online safety across all elements of school life.** The principles should be reflected in the school's policies and practice where appropriate, and should be communicated with staff, pupils and parents. This will include, for example, in the child protection policy clear processes for reporting incidents or concerns. Keeping Children Safe in Education provides advice for schools on embedding online safety into their broader safeguarding and child protection approach. It will also include reflecting online behaviours in the school's behaviour and bullying policies. Pupils should be just as clear about what is expected of them online as offline.

- **Proactively engaging staff, pupils and parents/carers** in school activities that promote the agreed principles of online safety. This could for example involve the co-design of programmes to ensure the school captures information from parents and pupils about their experience of emerging issues they are hearing about or facing online.

  It could also include peer-to-peer support**.** Experts have told us that pupils like to hear from other pupils when learning about staying safe online. Schools could consider implementing a scheme which supports pupils to help their peers stay safe online.

- **Reviewing and maintaining the online safety principles.** This includes making sure that school staff have access to up to date appropriate training/CPD and resources, so that they are confident in covering the required content in a way that is relevant to their pupils' lives. It could also include using information available to the school to review practices and ensure the issues facing their pupils are covered in a timely manner.

- **Embedding the online safety principles:**
  - When teaching curriculum subjects and other teaching opportunities
  - Reinforcing what is taught in lessons by taking appropriate and consistent action when a pupil makes a report of unacceptable online behaviours from another pupil, including cyberbullying, or shares a concern about something they have seen online.

- **Modelling the online safety principles consistently.** This includes expecting the same standards of behaviour whenever a pupil is online at school - be it in class, logged on at the library or using their own device in the playground. Schools should also ensure they **extend support to parents**, so they are able to incorporate the same principles of online safety at home. The further sources of information section includes information about organisations who can either support schools engage with parents or support parents directly.

Further sources of information

43. Here we signpost to relevant government guidance and a range of national organisations who can offer support to schools. This is not an exhaustive list and we are not mandating that schools use resources from these organisations, we are aware that there will be many other organisations offering quality support.

Government guidance and support:

- Relationship Education, Relationships and Sex Education and Health Education Statutory Guidance

- National curriculum in England: computing programmes of study - Statutory guidance on computing programmes of study.

- National curriculum in England: citizenship programmes of study – Statutory programmes of study and attainment targets for citizenship at key stages 3 and 4.

- Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.

- Behaviour and discipline in schools - Guidance for school leaders and staff on developing a school behaviour policy, and a checklist of actions to take to encourage good behaviour.

- Searching, screening and confiscation at school - Guidance explaining the powers schools have to screen and search pupils, and to confiscate items they find.

- CEOP Thinkuknow Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18, expert and support and professional development for the children's workforce. Signposts to the NCA's Click CEOP service for children to report concerns related to sexual abuse.

- National Centre for Computing Education (NCCE) has been set up to support the teaching of computing education throughout schools and colleges in England, giving teachers the subject knowledge and skills to establish computing as a core part of the curriculum. To help primary and secondary schools teach the safety and security aspects of the National Curriculum Computing Programme of Study, the National Centre for Computing Education's resource repository and professional development courses cover objectives from the Education for a

Connected World framework. The resource repository's lesson plans will include links to the framework, as well as specific activities for non-specialist teachers.

- UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms. The website has useful resources for schools and parents to help keep children safe online including:
    - Education for a Connected World – a framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.
- UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use, published February 2019.

National organisations:

For schools

- The Anti-Bullying Alliance - A coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn. Their website includes a range of tools and resources to support schools prevent and tackle cyberbullying.
- Childnet - a children's charity and has a wide range of practical resources freely available, covering all online safety issues, and which are available for teachers working with children of all ages, including children with SEN.
- The Diana Award – a charity running a number of different projects aimed at reducing bullying in schools. Their resource section has information to help schools tackle cyberbullying along with resources from their Be Strong Online Ambassador programme – a peer-led initiative which aims to empower young people to increase the digital resilience of their peers.
- DotCom Digital - a free resource for schools, created by children with Essex Police and the National Police Chief Council Lead for Internet Intelligence and Investigations, to be launched October 2019. The resource aims to prevent young people becoming victims of online grooming, radicalisation, exploitation and bullying by giving them the confidence to recognise warning signs and reach out to an adult for help.

- The Hopes and Streams report by LGfL has themed chapters that include links to online resources and ideas for tackling the issues raised.

- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with parents about online safety.

- Internet Watch Foundation – an internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images online.

- NSPCC learning – includes a range of safeguarding and child protection teaching resources, advice and training for schools and colleges.

- Parent Zone's dedicated school zone - includes a range of resources to support teachers educate their pupils on how to stay safe online, what to do if they find themselves in an uncomfortable situation and how to build their digital resilience.

- PSHE Association - the national body for Personal, Social, Health and Economic (PSHE) education. Their programme of study for PSHE education aims to develop skills and attributes such as resilience, self-esteem, risk-management, team working and critical thinking. They also have many guides about how to teach specific topics.

- SWGfL – a charity dedicated to empowering the safe and secure use of technology. Their website includes a range of free resources for schools covering a range of online safety issues, including digital literacy / critical thinking and consequences of sharing and publishing images.

- UK Safer Internet Centre –a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people. Their website includes a range of practical resources and support for schools including:
    - 360 degree safe - a free to use self-review tool for schools to assess their wider online safety policy and practice.
    - A Helpline – This helpline was established to support those working with children across the UK with online safety issues. Operated by SWGfL, it can be contacted at 0344 381 4772 and helpline@saferinternet.org.uk
    - Safer Internet Day - The UK Safer Internet Centre organise Safer Internet Day for the UK and each year develops a range of materials from

assemblies to lesson plans, posters to quizzes, for each Key Stage, to address a key online safety issue.

For parents and carers

- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world. Their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, Vlogging & livestreaming, online gaming and cyberbullying.

- NSPCC - includes a range of resources to help parents keep children safe when they're using the internet, social networks, apps, games and more.

- Parent Info - from CEOP and Parent Zone, Parent Info is a website for parents covering all of the issues amplified by the internet. It is a free service which helps schools engage parents with expert safety advice, endorsed by the National Crime Agency's CEOP command. This website provides expert information across a range of online harms.

- Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms.

For pupils

- BBC Own It – Support for young people to take control of their online life, including help and advice, skills and inspiration on topics such as friendships and bullying, safety and self-esteem.

- Childline – includes information for pupils on sexting, gaming, grooming, bullying, porn, relationships.

Department for Education

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DfE-00128-2019

Follow us on Twitter: @educationgovuk

Like us on Facebook: facebook.com/educationgovuk