GOV.UK

Department
for Education

Guidance

Teaching online safety in schools

Updated 12 January 2023

Applies to England

Contents

Introduction
Curriculum context
Underpinning knowledge and behaviours
Teaching about harms and risks
Vulnerable pupils
Use of external resources
Use of external visitors
Safeguarding
Whole school approach
Further sources of information

This publication is available at https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

This non-statutory guidance outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

It complements existing subjects including:

- relationships education
- relationships and sex education
- health education
- citizenship
- computing

There are no additional teaching requirements.

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

Independent schools and non-maintained special schools may also find this guidance helpful as they are required to teach relationships education, relationships and sex education, and health education.

Introduction

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.

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.

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.

Refer to the education for a connected world framework (https://www.gov.uk/government/publications/education-for-a-connected-world) for age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

Curriculum context

As part of the statutory relationships and health education (https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education/relationships-education-primary) in primary schools and relationships, sex and health education (https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education/relationships-and-sex-education-rse-secondary) in

secondary schools, pupils are taught about online safety and harms. This includes being taught:

- what positive, healthy and respectful online relationships look like
- the effects of their online actions on others
- 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.

This complements the computing curriculum (https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study), 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
- where to go for help and support when they have concerns about content or contact on the internet or other online technologies

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example, citizenship education (https://www.gov.uk/government/publications/national-curriculum-in-england-citizenship-programmes-of-study) explores:

- freedom of speech
- the role and responsibility of the media in informing and shaping public opinion
- the concept of democracy, freedom, rights, and responsibilities

Educate Against Hate has a full teaching pack dedicated to fundamental British values (https://educateagainsthate.com/resources/lets-discuss-british-values/) that includes class tasks, a class presentation, films and teaching guidance.

You should consider what you are already delivering through the curriculum, and build in additional teaching as required to make sure pupils know how to stay safe and how to behave online.

Underpinning knowledge and behaviours

The online world develops and changes at a 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.

It is 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
- covered using school-wide approaches

Teaching must always be age and developmentally appropriate.

How to evaluate what they see online

Covering this content will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

You can help pupils to consider:

- whether a website, URL or email is fake
- what cookies do and what information they are sharing
- if a person or organisation is who they say they are
- why a person wants them to see, send or believe something
- why a person wants their personal information
- the reason why something has been posted
- whether something they see online is fact or opinion

How to recognise techniques used for persuasion

Covering this content will enable pupils to recognise the techniques that are often used to persuade or manipulate others.

You can help pupils to recognise:

- online content which tries to make people believe something false is true or mislead (misinformation and disinformation)
- techniques that companies use to persuade people to buy something
- ways in which criminals may try to defraud people online
- ways in which games and social media companies try to keep users online longer (persuasive or sticky design)
- grooming and manipulation techniques used by criminals
- ways to protect themselves from a range of cyber crimes

Online behaviour

Covering this content will enable pupils to understand what acceptable and unacceptable online behaviour look like. You should teach pupils:

- that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others
- to recognise unacceptable behaviour in others

You 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[footnote 1]
- looking at the key principles behind a constructive discussion, including a willingness to listen to other opinions and a readiness to be educated on a topic
- considering how to demonstrate empathy towards others (on and offline)
- 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
- considering unacceptable online behaviours often passed off as so-called social norms or just banter, for example, negative language being used as part of online gaming but would never be tolerated offline

How to identify online risks

Covering this content 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.

You can help pupils to identify and manage risk by discussing:

- the ways in which someone may put themselves at risk online
- risks posed by another person's online behaviour
- when risk taking can be positive and negative
- online reputation and the positive and negative aspects of an online digital footprint
- sharing information online and how to make a judgement about when and how to share and who to share with
- the risks of cyber crime, online fraud and identity theft

How and when to seek support

Covering this content will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

You can help pupils by explaining how to:

- identify who trusted adults are
- access support from the school, police, the National Crime Agency's Click CEOP reporting service (https://www.ceop.police.uk/CEOP-Reporting/) for children and 3rd sector organisations such as Childline (https://www.childline.org.uk/) and Internet Watch Foundation (https://www.iwf.org.uk/)

- report cyber crime, fraud and suspicious online activity, through organisations such as Action Fraud (https://www.actionfraud.police.uk/) and the Advertising Standards Authority (https://www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html)
- report inappropriate contact or content for various platforms and apps

You should link this to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff. Refer to keeping children safe in education (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) for more information.

Online media literacy strategy

The online media literacy strategy (https://www.gov.uk/government/publications/online-media-literacy-strategy) sets out that the government will give internet users the knowledge and skills they need to make informed and safe choices online.

It sets out 5 principles to underpin delivery of media literacy education. These include understanding:

- the risks of sharing personal data and how to protect their privacy
- how the online environment operates
- how online content is generated and to critically analyse the content they consume
- that online actions can have offline consequences, and use this understanding in their online interactions
- how to participate positively in online engagement, while understanding the risks of engaging with others

A list of media literacy resources for teachers and parents (https://www.gov.uk/guidance/online-media-literacy-resources) is available.

Teaching about harms and risks

Understanding and applying knowledge and behaviours will provide pupils with a solid foundation to navigate the online world in an effective and safe way. By understanding the risks that exist online, you can tailor your teaching and support to the specific needs of your pupils.

This section will help you understand some of the issues your pupils may be facing and where these could be covered within the curriculum. You 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.

How to navigate the internet and manage information

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

Age-specific advice on these potential harms and risks can be found in the following sections of the education for a connected world (https://www.gov.uk/government/publications/education-for-a-connected-world) framework:

- managing online information
- copyright and ownership
- privacy and security

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:

- explaining 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
- explaining 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
- explaining what the age of digital consent means - 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

You could cover this content in the following curriculum areas:

- health education (all stages) - internet safety and harms topic
- computing (all key stages) – you may want to discuss age restrictions as part of e-safety

How content 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
- the risk of identity theft or targeted approach from fraudsters using information shared online

- ensuring pupils understand what is illegal online, for example:
  - youth-produced sexual imagery (sexting)
  - sharing illegal content such as extreme pornography or terrorist content
  - the illegality of possession, creating or sharing any explicit images of a child even if created by a child

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- relationships and sex education core content (secondary) – online and media topic
- health education core content (all stages) – internet safety and harms topic
- computing (all key stages)

Disinformation, misinformation, malinformation 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
- malinformation and understanding that some genuine information can be published with the deliberate intent to harm, for example releasing private information or photographs (including revenge porn)
- 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

You could cover this content in the following curriculum areas:

- relationships education (all stages)
- relationships and sex education (secondary)
- health education (all stages)
- computing (key stages 2 and above)
- citizenship (key stages 3 and 4)

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 another gain.

Teaching could include:

- 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 or 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
- explaining the risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist

You could cover this content in the following curriculum areas:

- relationships education (all stages)
- relationships and sex education (secondary)
- health education (all stages)
- computing (all key stages)

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
- explaining that online fraud can be highly sophisticated and that anyone can be a victim
- how to protect yourself and others against different types of online fraud
- how to identify 'money mule' schemes and recruiters
- the risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal
- the risk of sharing personal information that could be used by fraudsters
- explaining that children are sometimes targeted to access adults' data, for example, passing on their parent or carer's bank details, date of birth or national insurance number
- 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
- how to report fraud, phishing attempts, suspicious websites and adverts

You could cover this content in the following curriculum areas:

- relationships education core content – online relationships topic
- computing (all key stages)

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 safe and that others may try to trick you to reveal them
- explaining how to recognise phishing scams, for example, those that try to get login credentials and passwords
- the importance of online security to protect against viruses (such as keylogging) that are designed to access, steal or copy passwords
- what to do when a password is compromised or thought to be compromised

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) - online relationships topic
- computing (all key stages)

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 and 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

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- relationships and sex education core content (secondary) – online relationships topic

- computing (all key stages)

Persuasive design

Many devices, apps and 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 notifications to pull users back online

You could cover this content in the following curriculum areas:

- health education core content (all stages) – internet safety and harms topic
- computing (all key stages)

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

You could cover this content in the following curriculum areas:

- relationships education core content – online relationships topic
- computing (all key stages)

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.

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) 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

You could cover this content in the following curriculum areas:

- health education core content (all stages) - internet safety and harms topic
- computing (all key stages)

How to stay safe online

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

Age-specific advice on these potential harms and risks can be found in the following sections of the education for a connected world framework (https://www.gov.uk/government/publications/education-for-a-connected-world):

- online relationships
- privacy and security
- online reputation
- online bullying

Abuse (online)

Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal.

Teaching could include:

- explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation
- explaining 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 the implications for victims
- being clear about what good online behaviours do and don't look like

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- health education core content (all stages) – internet safety and harms topic
- computing (all key stages)
- citizenship (key stage 4)

Online radicalisation

Children, young people and adult learners are at risk of accessing inappropriate and harmful extremist content online. This could include downloading or sharing terrorist material, which could be a criminal act.

The internet and social media make spreading divisive and hateful narratives easier. Extremist and terrorist groups and organisations use social media (for example, apps, forums, blogs, chat rooms) to identify and target vulnerable individuals.

Teaching could include:

- how to recognise extremist behaviour and content online
- understanding actions which could be identified as criminal activity
- exploring techniques used for persuasion
- knowing how to access support from trusted individuals and organisations

All education settings have a responsibility under the Prevent duty. This includes building your students' resilience to extremism and ensuring staff are adequately trained to spot the signs of radicalisation.

Guidance, teaching resources and tools to help you teach young people about extremism, radicalisation and staying safe online are available on Educate Against Hate (http://www.educateagainsthate.com/).

Challenges

Online challenges acquire mass followings and encourage others to take part in what they suggest.

Teaching could include:

- 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)

You could cover this content in the following curriculum areas:

- relationships education (all stages)
- relationships and sex education (secondary)
- health education core content (all stages)

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

You could cover this content in the following curriculum areas:

- relationships education (all stages)
- relationships and sex education (secondary)
- health education (all stages)

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 are not (such as 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, for example:
  - profile pictures that don't like right, for example, of a celebrity or object
  - accounts with no followers or thousands of followers
  - a public figure who doesn't have a verified account

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- computing (all key stages)

Grooming

Knowing about the different types of grooming and motivations for it, for example:

- radicalisation
- child sexual abuse and exploitation
- gangs (county lines)
- financial exploitation (money mules)

Teaching could include:

- boundaries in friendships with peers, families and with others
- the 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

See the National Crime Agency's think u know (https://www.thinkuknow.co.uk/) 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.

You could cover this content in the following curriculum areas:

- relationships education (all stages)
- relationships and sex education (secondary)

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 live streaming such as the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent
- that 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
- 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

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- health education core content (secondary) – internet safety and harms topic

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, such as revenge porn or people trafficked into sex work

You could cover this content as part of the relationships and sex education core content (secondary), online and media topic.

Unsafe communication

Knowing different strategies for staying safe when communicating with others, especially people they do not know or 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

You could cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- relationships education core content (all stages) – respectful relationships topic
- relationships and sex education core content (secondary)
- computing (all key stages)

Wellbeing

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

Age-specific advice on these potential harms and risks can be found in the following sections of the education for a connected world framework (https://www.gov.uk/government/publications/education-for-a-connected-world):

- self-image and identity
- online reputation
- online bullying
- health, wellbeing and lifestyle

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
- understanding that 'easy money' lifestyles and offers may be too good to be true
- looking at photo manipulation including discussions about why people do it and how to look out for it

You could cover this content as part of the health education core content (secondary), internet safety and harms topic.

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)
- helping pupils to consider quality versus quantity of online activity
- explaining that pupils need to consider if they are actually enjoying being 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

You could cover this content as part of the health education core content (secondary), internet safety and harms topic.

Online versus 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 lead to pressure

- discussing how and why people are unkind or hurtful online, when they would not necessarily be unkind to someone face to face

You could cover this content as part of the relationships education core content (all stages), online relationships topic.

Reputational damage

What users post can affect future career opportunities and relationships – both positively and negatively.

Teaching could include:

- looking at strategies for positive use
- how to build a professional online profile

You could cover this content as part of the relationships and sex education core content (secondary), online and media topic.

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 (https://pshe-association.org.uk/guidance/ks1-4/mental-health-guidance) provides useful support for teachers in handling this material.

Vulnerable pupils

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. You should consider how you tailor your offer to make sure these pupils receive the information and support they need.

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

- vulnerable children in a digital world (https://www.internetmatters.org/about-us/vulnerable-children-in-a-digital-world-report/) - a report from Internet Matters
- children's online activities, risks and safety (https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group) - a literature review by the UK Council for Internet Safety's evidence group

Use of external resources

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.

Before using any resource, you should check:

- where the organisation gets their information from
- what their evidence base is
- if they have been externally quality assured
- the background of the organisation
- if the resources are age appropriate for pupils
- if the resources are appropriate for the developmental stage of pupils

Use of external visitors

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.

Guidance for schools on using external visitors to support online safety education (https://www.gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings) is available.

Safeguarding

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.

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 or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

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 planning any safeguarding related lessons or activities (including online). 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.

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 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 (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) your reporting mechanisms should be child friendly and operate with the best interests of the pupil at their heart.

Whole school approach

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
- partnerships with families and the community

We recommend that schools embed teaching about online safety and harms within a whole school approach.

Incorporating the principles of online safety across all elements of school life

You should reflect the principles of online safety in the school's policies and practice where appropriate, and communicate this with staff, pupils and parents. This could include, for example:

- having clear processes for reporting incidents or concerns in the child protection policy
- reflecting online behaviours in the school's behaviour and bullying policies

Keeping children safe in education (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) provides advice for schools on embedding online safety into their broader safeguarding and child protection approach.

Pupils should be just as clear about what is expected of them online as offline.

Engaging staff, pupils, parents and carers

Proactively engage staff, pupils, parents and carers in school activities that promote the agreed principles of online safety. This could include, for example:

- co-designing programmes to reflect any emerging issues parents and pupils are hearing about or facing online
- peer-to-peer support - 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 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

Reinforce 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
- 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.

Further sources of information

This list provides links to relevant government guidance and a range of national organisations who can offer support to schools.

Related guidance is available on:

- relationships and sex education (RSE) and health education (https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education)
- national curriculum in England computing programmes of study (https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study)

- national curriculum in England citizenship programmes of study (https://www.gov.uk/government/publications/national-curriculum-in-england-citizenship-programmes-of-study)
- keeping children safe in education (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)
- behaviour in schools (https://www.gov.uk/government/publications/behaviour-in-schools--2)
- searching, screening and confiscation at school (https://www.gov.uk/government/publications/searching-screening-and-confiscation)

Support and resources are also available from:

- the CEOP Thinkuknow Programme (https://www.thinkuknow.co.uk/professionals/)
- the NCA's Click CEOP (https://www.ceop.police.uk/safety-centre/)
- National Centre for Computing Education (NCCE) (https://teachcomputing.org/)
- UK Council for Internet Safety (https://www.gov.uk/government/organisations/uk-council-for-internet-safety)
- Education for a Connected World (https://www.gov.uk/government/publications/education-for-a-connected-world)

Schools can also get advice from national organisations such as:

- The Anti-Bullying Alliance (https://www.anti-bullyingalliance.org.uk/)
- Childnet (http://www.childnet.com)
- The Diana Award (http://www.antibullyingpro.com/resources)
- DotCom Charity (https://dotcomcharity.co.uk/)
- Hopes and Streams (https://www.lgfl.net/online-safety/hopesandstreams)
- Internet Matters (https://www.internetmatters.org/schools-esafety/)
- Internet Watch Foundation (https://www.iwf.org.uk/)
- NSPCC learning (https://learning.nspcc.org.uk/)
- Parent Zone's school resources (https://parentzone.org.uk/beinternetlegends/schools)
- PSHE Association (https://www.pshe-association.org.uk/)
- SWGfL (https://swgfl.org.uk/resources/)
- UK Safer Internet Centre (https://www.saferinternet.org.uk/)

You can refer parents to the following national organisations for support:

- NSPCC (https://www.nspcc.org.uk/)
- Parent Zone (https://parentzone.org.uk)

You can refer pupils to the following national organisations for support:

- BBC Own It (https://www.bbc.com/ownit)
- Childline (https://www.childline.org.uk/)

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

↑ Back to top