



Online Safety CPD

Staff update, 2020-21



This document has been created to support the near ten thousand school staff in UK schools who completed the OSA's accredited CPD course last year. It updates staff on important developments relating to online safety and the use of technology in schools.



A substantially updated version of the course for the 2020-21 academic year is now available for free from the website of the Online Safety Alliance. We recommend staff who did not complete the training last year should undertake the course rather than rely on this update.

New statutory requirements from September 2020: Relationships Education

From September 2020, schools must provide education on Relationships Education (primary settings) and Relationships and Sex Education (secondary settings). These requirements aim to ensure that children and young people know how to be safe and healthy, and how to manage their academic, personal and social lives in a positive way.

Given the amount of time children and young people spend online and how the Internet impacts on all aspects of life, much of these statutory requirements focus on schools ensuring pupils have firm knowledge of how to protect themselves and others online.



Primary Settings

To meet requirements for Relationships Education your online safety provision must ensure that pupils understand:

- that people sometimes behave differently online, including by pretending to be someone they are not.
- 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.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.
- what sorts of boundaries are appropriate in friendships with peers and others.
- about the concept of privacy; including that it is not always right to keep secrets.
- how to respond safely and appropriately to adults they may encounter (including online).
- how to recognise and report feelings of being unsafe.

Secondary Settings

To meet requirements for Relationships and Sex Education your online safety provision must ensure that pupils understand:

- the characteristics of positive and healthy friendships and relationships (including online).
- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how to get help.
- that the same expectations of behaviour apply in all contexts, including online.
- about online risks.
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- where to get support to manage issues online.
- the impact of viewing harmful and sexually explicit content.
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence.
- how information and data is generated, collected, shared and used online.
- the concepts of, and laws relating to topics including, sexual consent, sexual exploitation, abuse, grooming, coercion and harassment.

Please note, the bullet points detailed above are meant to highlight the new requirements which relate specifically to online safety issues. There are other requirements not relating to online issues which we have not referenced and relevant staff will need to ensure they are aware of these requirements. Please see DFE documentation for full guidance.

The need to develop awareness of TikTok

It is important that staff in schools develop an awareness of the general guidelines which apply to the safe use of all social media rather than focus on the specifics of lots of individual platforms. However, given the rapid rise in popularity of TikTok and the very specific concerns it raises, developing an understanding of the features and risks of TikTok is good practice for staff working with children.

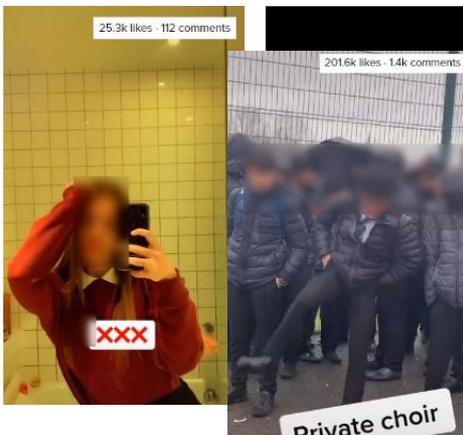


What is TikTok?

TikTok is a social media platform which over the past year has gained massive popularity with tweens and younger teenagers despite a minimum age limit of 13. TikTok is branded as a platform for sharing short videos of 15 seconds. The content of the videos commonly includes lip-syncing to music, dance routines, gaming clips, makeup and fashion and reactions of people to events/pranks.

An OSA survey of Key Stage 3 pupils in 2019-2020 found that 61% of them used TikTok, putting it at similar usage levels to SnapChat and Instagram.

Concerns about TikTok



>> School-based content

Many of the videos trending on TikTok involve children in British school uniforms and often seem to have been filmed on school premises. Wearing school uniform in videos can enable others to identify the location of a child.

>> Privacy settings

The default privacy settings on TikTok are a concern given they include new accounts being public, with anybody able to view videos the user posts and to comment upon them.

>> Security concerns

TikTok has been banned in India and a number of countries around the world are considering following suit. Reasons cited for this include the platform requires access to more personal data than should be needed and requests to access user location, audio and camera recordings, and contacts.

>> Nature of the content

Children using TikTok will be quickly exposed to content including offensive language and sexualised dancing. Viewing such content can normalise such behaviours and lead to children producing their own video content which is no age-appropriate.

Tips for safe use

As with all social media platforms, encourage pupils to stick to the stated minimum age limits (13 in the case of TikTok).

Encourage pupils to check their privacy settings are appropriately set and to think carefully about possible impacts before posting anything online.

Parents should be made aware of how the role they can play in the safe use of social media. TikTok has launched a "Family Safety Mode," designed to let parents set screen-time limits, limits on direct messages and a restricted mode that limits the appearance of inappropriate content.



The OSA Certificate of Online Safety courses for KS3, KS4, KS5 and parents can help ensure that your pupils and their parents/carers have a strong understanding of the risks associated with social media use and how these risks can be managed. Please see our website for details

Online risks to children: updates

Youth-produced sexual imagery

A December 2019 report published in the Guardian found there had been 6,499 cases where children under 14 had been investigated by police for sexting offences in the preceding three years, including more than 300 relating to primary school children.

Only 30 of these cases resulted in a charge, caution or summons for the child. The vast majority of investigations were dropped because the police decided it would not be in the public interest to take formal action.

A report by the Internet Watch Foundation (IWF) took action on 37,000 'sexual selfies' last year. Of these, 80% were of girls aged between 11 and 13. They also stated that 'of all web pages featuring images of child sexual abuse, a third consisted of self-generated images, mostly by girls in a domestic setting'.



Gaming

During the school closures

of 2020, online gaming undoubtedly provided opportunities for many children to stay in touch with friends and enjoy shared experiences. However, gaming brings some associated risks:



- In May 2019 the World Health Organisation officially classified gaming addiction as a disease.

- In October 2019 the Children's Commissioner for England released a report which indicated that some monetisation within games 'looks more like gambling' than play. Children can spend large amounts of money on 'loot boxes' in different games, often not knowing what they will get from them.

- Online communication in games can lead to children encountering bullying and abuse. In some cases, it has been used as an opportunity for grooming.

Misinformation

The June 2019 government guidance 'Teaching Online Safety in Schools' states that pupils should be taught about disinformation, misinformation and hoaxes. With 'fake news' being such a common topic in national and global news, there should be lots of opportunities to have topical discussions with pupils on this topic.

Recent high profile examples (at the time of writing) include Donald Trump tweets about postal voting being flagged as 'potentially misleading' and Madonna's Instagram post about Coronavirus being taken down for misinformation.



In September 2020, Researchers at Cornell University found that Donald Trump was "the single largest driver of misinformation around Covid". He was linked to 38% of the overall "misinformation conversation"

Grooming has continued to be a serious risk to children over the past

Grooming

year, a situation exacerbated by lockdown. The small selection of case studies shown below highlight some of the techniques currently being employed by groomers and the fact that often children do not report such issues.



In June 2020, a 31-year-old man was sentenced to thirteen years in prison for grooming and exploiting sixteen girls, with the youngest two being twelve years old. He approached them as 'Sarah' using a fake social media account, offering them work with a model agency. He told them to install the messaging app 'Kik' so that the manager of the (fake) agency could talk to them. They were then aggressively coerced into sending sexually explicit videos and images. He threatened to come to their homes and sue their families for 'time-wasting' if they refused.



In July 2020, a law firm worker was jailed after police discovered he had sent 59,000 messages and indecent images to children, trying to entice them into sexual acts over a period of six years. The youngest known victim was twelve years old.

The case serves as an example of how few children raise the alarm when they receive such contact as this individual was only identified by the police during an investigation into another individual.



In January 2020, a 21-year-old woman was jailed for eight years after pleading guilty to sexually assaulting teenage girls she had met online. She pretended to be a 15-year-old boy named Jake and liked the profiles of potential victims on Instagram and Snapchat. She shared flattering messages and intimate photographs before traveling to meet up with her victims (in disguise as 'Jake') where assaults took place. The youngest victim was 13 and police believe there could have been as many as 50 victims in total.

Please ensure your pupils are aware of the role of CEOP in tackling concerns about online grooming.

Staff use of digital technology

Each year our CPD course examines ways in which staff use of digital technology has caused problems, with a particular focus on cases which led to reviews by the Teaching Regulation Agency. A selection of the cases from this year is shown below.

Consider how you use school technology for personal reasons

In July 2019, the headteacher of two primary schools was banned from teaching, with the option of being able to apply to teach again in eight years.

Among the allegations against him which were found to be proven, he had sent images of naked and part-naked adult females from his school email address to his personal email, sent emails including inappropriate language and sent emails relating to online gaming during school hours.

Don't damage your school's reputation through social media

In August 2019 the TRA found that a teacher had threatened to release photographs of other members of staff on social media, which he suggested would tarnish the school's reputation unless the school agreed to the terms of his offer to leave their employ. This followed an investigation into inappropriate behaviour at the school prom.

The teacher was banned from teaching indefinitely (available for review after two years).

Communications with pupils must remain professional

In March 2020 the Teaching Regulation Agency banned a teacher for unacceptable professional conduct and failure to follow safeguarding procedures. In communications with a pupil she included words such as "sweetie" and/or "love", used 'x' to indicate a kiss/kisses and referred to her own personal family issues. She also sent messages undermining the school Designated Safeguarding Lead who had instructed her to avoid emailing the pupil.

Managing remote learning

The closure of schools in March 2020 due to Covid-19 resulted in a move to remote learning, with schools providing education through a range of online platforms such as Microsoft Teams, Google Classroom and Virtual Learning Environments. A key challenge for staff has been to meet these new expectations while continuing to protect students and themselves online.

Staff should be aware of the Department for Education's 'Safeguarding and remote education during coronavirus' guidance (updated May 2020), key elements of which are shown below:

Communicating with pupils and parents

- communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)*
- communicate through the school channels approved by the leadership team
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- teachers should not share personal information

Virtual lessons and live streaming

- Teachers should try to find a quiet or private room or area to talk to parents or carers.
- When broadcasting a lesson or making a recording, consider what can be seen in the background.

"Remote education may need to be an essential component in the delivery of the school curriculum for some pupils, alongside classroom teaching, or in the case of a local lockdown."

DFE, July 2020



*: In the 2019-2020 CPD course we detailed a case study of an individual banned from teaching after sending inappropriate emails between 9pm and 2am. In September 2019 a teacher was banned from teaching indefinitely after sending emails of a personal nature 'late at night' to a student. The latest emails sent were just before 9pm. Staff should reflect on when they send communications and feedback to pupils given the views taken by the TRA in this case and the DFE guidance above.