Online Safety Policy
(and Teaching Framework)

September 2019

Overview

At Social Arts for Education, we recognise that it is important to teach pupils about the knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. As a school, we also recognise that we, ourselves, need an understanding of the risks that exist online so that we can tailor our teaching and support to the specific needs of our pupils. This Online Safety Policy is based upon the DfE Guidance, Teaching Online Safety in School.

We 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. We embed teaching about online safety within a whole school approach.

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 to equip our 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.

Curriculum context

From September 2020, Relationships and Sex Education will be compulsory for all secondary aged pupils, including those at Social Arts for Education. We plan to ensure that, through this subject, pupils will be taught about online safety and potential factors for risk and harm. 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. These topics will also be reinforced throughout all curriculum areas. Teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.

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.

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely, for example English 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.
We will constantly evaluate and consider what we are 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

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. 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 is to be built into existing lessons across the curriculum, and covered within specific online safety lessons and school wide approaches. Teaching must always be age and developmentally appropriate.

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.
We 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.

We will 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. We will teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. We will also teach pupils to recognise unacceptable behaviour in others.

We will 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.

We will 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,

- 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.

We will 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

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, we, as a school, also need an understanding of the risks that exist online so that we can tailor our teaching and support to the specific needs of our pupils.

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

The following sections should be read in conjunction with 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

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

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.
- 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.

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,this as part of wider teachings around how information online is stored and used. "protecting their online identity and privacy"
- 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.
- 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."

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.

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 URLs and websites,
- ensuring pupils understand what secure markings on websites are and how to assess the sources of emails,
- explaining the risks of entering information to a website which isn't secure,
- what to do if harmed/targeted/groomed as a result of interacting with a fake website or scam email. Who to go to and the range of support that is available.

Fraud (online)

Fraud can take place online and can have serious consequences for individuals and organisations.

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.

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 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, 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.

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.

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 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”

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.

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,and how to report these
- explanation of when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail,
- how to respond to online abuse including how to access help and support,
- how to respond when the abuse is anonymous,
- discussing the potential implications of online abuse, including implications for victims,
- being clear what good online behaviours do and don't look like.

Challenges

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

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).

Content which incites violence

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 glamourise the possession of weapons and drugs,
- explaining that to intentionally encourage or assist an offence is also a criminal offence,

- ensuring pupils know how and where to get help if worried about involvement in violence.

Fake profiles

Not everyone online is who they say they are.

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 look right, for example of a celebrity or object,
    - accounts with no followers or thousands of followers; and
    - a public figure who doesn't have a verified account.

Grooming

Knowing about the different types of grooming and motivations for it, for example radicalisation, Child Sexual Abuse and Exploitation (CSAE) and gangs (county lines).

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.

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. 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.

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.

Wellbeing

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

Positive Body Image

Knowing that many images online are digitally manipulated, and should not be used as a benchmark to be aspired to.

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.

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 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.

Reputational damage

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

Teaching could include

- looking at strategies for how to build a professional online profile
- discussing the difficulties of removing previously posted material, and how it could already be in the public domain.

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.

Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. 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. Staff at Social Arts for Education must consider how they tailor their teaching to ensure these pupils receive the information and support they need.

Use of external resources

All staff at Social Arts for Education must make sure that resources are thoroughly reviewed to ensure they are educationally appropriate for our pupils, even when that resource comes from a trusted source.

Teachers must 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

Online safety can be a difficult and complex topic which changes very quickly. Therefore, on occasion, Social Arts for Education will seek external support who have expertise, up to date knowledge and information, in order to supplement and enhance the information delivered in class. External visitors will be selected via the UK Council for Internet Safety's guidance document.

Teaching about online harms and risks in a safe way

As with any safeguarding lessons or activities, it is important that we consider the topic to be covered 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 and/or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

Where staff at Social Arts for Education 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. The Designated Safeguarding Lead (or a deputy) should be involved 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.

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.

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 and partnerships with families and the community.

We expect that all staff will embed teaching about online safety and harms within a whole school approach. This will include:

- The creation and maintenance of a culture that incorporates the principles of online safety across all elements of school life, reflecting those principles in Social Arts for Education's policies and practice, and communicating them with staff, students and parents/carers.
- Ensuring pupils are just as certain of the behaviours required of them online as offline.

- Proactively engaging staff, pupils and parents/carers in school activities that promote the agreed principles of online safety.
- Peer-to-peer support.
- Reviewing and maintaining the online safety principles
- 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, and ensuring all staff behave appropriately online.
- Providing support to parents, to enable them to implement a safe online environment at home.

Relevant policies and documents

This policy should be read in conjunction with the following of Social Arts for Education's policies:

- Safeguarding and Child Protection
- ICT Acceptable Use
- Staff Code of Conduct,

It should also be read alongside Keeping Children Safe in Education.

Review

This policy was written on 27th September 2019 and will be reviewed annually, unless significant events, or changes in legislation, force an earlier review.