ONLINE SAFETY POLICY

The purpose of this policy is to ensure that all members of our community use technology proactively, productively, responsibly and safely in order to advance their education, effectiveness and personal wellbeing.

We aim to develop an understanding of:

- how technology is changing
- the nature of children and young people's online world
- risk factors and protective factors when going online
- what we can do as individuals and organisations
- good practice guidelines
- where to go for help and support

Rationale

Children and young people have been brought up with the internet and most use technology intuitively, often showing their parents how to use it. Being online enables children and young people to socialise, learn and experience many things in a variety of different ways. Children are becoming very familiar with technology at a younger age and there has been a substantial increase in the use of smartphones.

It is unrealistic to expect all those working with children and young people to know and keep up to date with all the apps and games children access. However, understanding the basic concepts of social media and gaming and how young people access them will help to understand the potential risks. It is also important to know how risks can run across multiple platforms and experiences, and how to minimise them.

A young person's online activity can influence their life 24 hours a day, seven days a week. Many children and young people report feeling 'disconnected' from the world if they can't go online, but they can often be unaware that what they do online can affect them offline. It is important to recognise that young people don't tend to differentiate between life online or offline; it is all part of their life. In a recent UNICEF report it was found that children and young people make up an estimated one in three internet users around the world.

Potential risk factors

Due to lack of life experience and emotional resilience children can be unaware of the risks, and their perception of risk can be different to that of adults. A child may perceive risk as an immediate threat, whereas adults tend to think a few steps ahead and sometimes arrive at the worst-case scenario.

Whilst the internet has entertaining, engaging and educational content, it also has illegal and inappropriate content which all has the potential to be viewed by a young person. This not only has safeguarding implications but can also have a negative impact on a young person's wellbeing and mental health.

It is important that children and young people are supported to understand the motives behind why different people contact them online and know how to report any concerns. This is not always easy as motives may not be clear or it could involve multiple motives. It is important for children to use their critical thinking skills and seek help if they are unsure what someone is messaging them, something sounds too good to be true, a new contact comes out of the blue or a conversation suddenly changes direction.

Online safety risks can be categorised into three areas - Content, Contact and Conduct.

AREA 1: CONTENT - What are children and young people able to access and experience online?

Social networking

Social networking sites and apps such as TikTok, WhatsApp, Instagram and Snapchat are extremely popular with young people. Photos, videos, thoughts and feelings are often shared, either publicly or privately. The age at which a young person can have an account varies with each site and country where it is being accessed. It is important that all members of the community understand the rules for the country where we live. Students, staff and parents should always follow the laws of the UAE

Children can be at risk of:

- viewing inappropriate material or hearing inappropriate language
- oversharing information
- unwanted contact, including abuse and bullying.

Safety tools often include:

- blocking tool
- reporting tool
- privacy settings
- safety information centre.

Privacy settings

Where some sites ask for a child's age, giving their correct age can ensure that additional protections are put in place. Social media sites often have additional layers of protection for users aged between 13 and 18, including who can view their profiles and send friend requests etc.

Children should be supported to access, implement and manage the privacy settings on different social media sites. By having privacy settings in place, an individual can control how much information is shared on a profile and who can view it.

Further information

As someone who works with young people, it is important you manage your own settings in order to protect and safeguard your own professional reputation.

If you use social media in your personal life you should consider:

- making your account private
- using a different name or variation of your name
- keeping your location private, particularly if you are on residential trips with young people
- not accepting friendship requests from the young people with whom you work or have worked.
- If you use social media in a professional capacity:
- the account can be public or private
- appropriate images should be used
- do not send private messages to children or young people.

Gaming

As we have seen from the statistics, gaming is extremely popular with children and young people. Games are easily accessible and can be played on various devices. Advances in augmented and virtual reality means that games can appear extremely realistic.

But with the increase in free gaming apps and live streaming, keeping children safe has become increasingly challenging.

Gaming concerns and risks are:

- viewing inappropriate material/hearing inappropriate language
- game play and chat offline with people they don't know
- unwanted contact, including abuse and bullying
- oversharing through the voice and video technology used within games, including webcams and headphones or voice chat.

Details of the media regulation by the UAE government can be found here:
https://u.ae/en/media/media-in-the-uae/media-regulation

Live streaming

Live streaming is a way of broadcasting or receiving live videos offered by most online services. This has become a popular way for celebrities to communicate with their fans. It is also a popular trend with vloggers. Young people can be at risk of being exposed to inappropriate or adult content. They

also need to think carefully about the content which they broadcast themselves, i.e. who can view the live content and what personal information might they be able to see.

Ephemeral or expiring content

This is any type of online content that has an expiry date, after which it is seen to 'disappear'. Ephemeral content began with Snapchat and is now a common feature on most social media platforms. The feature normally allows users to add throughout the day, building up a story. It is very popular with young people as it allows content to be created and viewed quickly and easily. Whilst this content is seen to 'disappear' it can be recorded or screenshot by other users, allowing them to keep a copy.

Video chat and webcams

Most tablets, games consoles and smartphones allow the user to take photos and videos. A growing number of social media sites allow live 'chats' for groups or individuals. If there is internet access, then these can be accessed at anytime and anywhere. When security is set to private, a young person might think that what they are sharing online is private, but it could be captured in a screenshot or recording and potentially shared with others making it public content. Young people should always be careful about who they are chatting to and what they are sharing online.

Downloading

There is music, films and more which can be easily accessed and downloaded on the internet. Children and young people should be made aware that there can be legal consequences for illegally downloading content although they are more likely to use online streaming services.

Adult content

Pornography

Pornography can often portray misleading attitudes around consent, gender roles and what sex is.
Pornography can be viewed intentionally, for example, out of natural curiosity, or by accident. Some pornography is illegal for anyone to view; for example, indecent images of children. If found online, this should be reported directly to your national hotline, see www.inhope.org, or the organisations in the support section at the end of the course.

Gambling

There is growing concern about the amount of young people gambling, particularly when gaming. Skin gambling is where gamers exchange virtual goods that they have won or purchased with virtual gaming chips. These can then be sold and turned into real money.

Graphic violence

Children and young people of all ages are at risk of seeing content that is for over 18's, including graphic violence.

Violent and extreme content

What causes upset online is broad and variable depending upon both gender and age of respondents. In general, upset is most commonly caused by:

- abusive comments from peers and others they interact with online
- stories in the news and media that can be upsetting (for example, terrorist incidents, child suffering, and natural disasters)
- animal abuse – videos that show animal cruelty, images of harm to animals or upsetting stories related to animals
- upsetting content, such as shocking videos produced by YouTubers, content showing people being hurt, acts of self-harm.

Younger children are more likely to be affected by things such as:

- swearing
- abuse from peers.

Older children are more likely to be affected by content such as:

- news and media
- animal abuse
- the behaviour of peers.

Inaccurate information

One of the biggest online problems is being able to recognise the reliability of information. The internet is a mine of information, including fake news and online scams. Some young people will trust online content more if the website looks professionally built or official terms are used. They may also think that the first result displayed by a search engine is the most trustworthy, accurate site, which is not necessarily the case. A key skill young people must develop is the ability to think critically about what they see or the contact they receive online.

Further information

Clickbait is online content, such as headlines, whose main purpose is to attract attention and encourage visitors to click on a link to a particular web page. Once the post has been liked or shared that group will be able to reach a wider network of people.

AREA 2: CONTACT - How do children and young people behave and interact with other people online?

Technology is an integral part of children and young people's way of building and maintaining friendships. How many likes and followers they have can influence how they are feeling.
Online contacts may or may not be who they say they are. Some may have ill intent; for example, sexual predators who attempt to groom children with the aim of meeting them offline. They may also be people who threaten, intimidate or bully others.
Education about online contact needs to reflect the risks of meeting up with someone you only know online as well as communicating with them online. Some strangers may exploit children through the internet with no intention of meeting up with them. Instead they may wish to obtain indecent images or videos so they can continue to exploit a child.

It is important to develop an understanding of how contact is made with others online and the risks that this involves.

Cyberbullying
Online platforms can be a tool for individuals or groups to bully or intimidate others directly or indirectly. Cyberbullying is a form of bullying, and as such, targets of cyberbullying can be upset, hurt, humiliated, afraid, and in some cases, may lead to a greater risk of self-harm and suicidal behaviours.

Geolocation
Geolocation refers to the geographical location of a user or device such as a phone. Some services allow the geolocation information to be shared with other people; this could be with anyone the user is connected with online, allowing others to become familiar with where a person lives and their lifestyle patterns. Geolocation can be turned off per app via a device's privacy settings.

AREA 3: CONDUCT
Children and young people should be aware that their online activity can have an impact on themselves and others.They need to be educated about how to manage their online behaviour, look after others and report any concerns.

Online reputation
What you create, post and share online is called your digital footprint and this is what shapes your online reputation. What others say and share about you also adds to your online reputation.
A digital footprint can be negative or positive and can affect how people see an individual in the future.

Personal information
Young people can be unaware that they are sharing personal information online, either by photos (an identifying school uniform, a road or shop sign may be shown) or by a direct conversation online. For

example, when you add a picture to WhatsApp, the picture, name and phone number can be visible to the rest of the people in the group.

Personal information can include:

- name
- address
- name of their school or college
- phone number
- location, including live location.

Young people should be taught that they should keep their information, and that of others, safe.

Sexting/sending nudes

Sexting is when someone shares sexual, semi-naked or naked photos or videos of themselves or others. It can also be the sharing of messages with sexual content. Once the message or image has been sent the person has no control of what happens to it. Young people can be pressurised into taking images and then blackmailed with them. Sexting is often referred to by young people as sending nudes. By sending this content on to another person, they have distributed an indecent image of a child. By receiving content of this kind from another young person, they are then in possession of an indecent image of a child.

Further information

If you become aware of an incident of sexting you should report it to the safeguarding lead in your organisation immediately. For a school this is the designated safeguarding lead. Guidance is available in the Resources section for schools and colleges to support them in handling sexting incidents.

Online sexual harassment

This is unwanted sexual conduct on any digital platform. Online sexual harassment can make a person feel exploited, upset, threatened, discriminated against and humiliated. This behaviour happens directly between and amongst young people and by witnessing it online.

In the UK 10% of 13 to 17-year-olds have received sexual threats online from people their age in the last year. 29% have witnessed this happening.

Sharing information is a great way for young people to stay in touch with others. But what is shared and said and to whom it is said should be thought about carefully. Anyone who goes online and shares information should think before posting.

Children and young people should be educated to understand the three C's of risk – Content, Contact and Conduct. The three C's are unlikely to occur in isolation and many of the risks will run across

more than one C. The three C's come into play at different stages of a child's life and so vulnerability is not a static issue.

Document	Online Safety Policy
Date written	April 2010
Last reviewed	July 2023
Next Review	August 2024
Version	Working Document