2.17 E-SAFETY POLICY

Definition of E-Safety

Online safety or E-Safety are generic terms that refer to raising awareness about how children, young people and adults can protect themselves when using digital technology and in the online environment.

'Online abuse' relates to the following areas of abuse;

- abusive images of children, a child or young person being groomed for the purpose of sexual abuse or exposure to pornographic images via the internet
- the use of the internet and in particular social media sites, to engage children in extremist ideologies
- offensive material and websites including those promoting negative lifestyle choices, for example self-harm, suicide and pro-anorexia
- the use of the internet to threaten, harass, bully and humiliate children and young people (e.g. cyber bullying and relationship abuse)

Perpetrators often use social networking sites as an easy way to access children and young people for sexual abuse. In addition, radical and extremist groups may use social networking to attract children and young people into rigid and narrow ideologies that are intolerant of diversity or promote extreme behaviours and justify or attempt to justify political, religious, sexist or racist violence.

Risks to Children

The risks children face online are commonly split into a number of categories:

Content: ***Age-inappropriate or unreliable content being available to children***
For example, content that is pornographic, violent, or extremist, or promotes self/harm suicide or anorexia. It is important that those who care for children consider the reliability of online material and be aware that information may be harmful, misleading and written with a bias.

Conduct: ***Children may be at risk because of their own behaviour, for example, by sharing too much information***
Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. Young people may share too much and take risks such as chatting to strangers or sharing sexual images ('Sexting' or may be led into 'sextortion'), or they may bully or intimidate others.

Youth produced sexual imagery (Sexting) describes the use of technology to generate images or videos that are of a sexual nature and are indecent. The content can vary, from text messages to images of partial nudity to sexual images or video. These images are then shared between young people and adults and with people they may not even know. Young people are not always aware that their actions are illegal and the increasing use of smart phones has made the practice much more common place.

Online Images
Children and young people should be discouraged from taking sexually explicit pictures of themselves and sharing them on the internet or by text.

It is essential that young people understand the legal implications and the risks they are taking. It is illegal to create, possess and distribute an indecent image of a child (under 18).

Children also need to me made aware of the long-term impact of sharing images such as the detrimental impact on future employment prospects or relationships. Sometimes children do not realise that they may be breaking the law when they share photographs of themselves in certain situations.

The initial risk posed by sexting may come from peers, friends and others in their social network who may share the images. Once an image has been sent, it is then out of the child / young person’s control and could be shared with others or posted elsewhere online.

However, whilst it is important to stress to children and young people the implications such activity may have for them, it is also important that a child is not made to feel afraid of telling an adult if they have been subject to online harm.

It is key to remember that the internet can also be a support mechanism for children and young people, where they can contact friends or family and obtain advice.

Working with the child to use the internet / social media safely after an incident will be more beneficial than removing their access or devices, dependent upon the level of risk.

Contact: ***Children can be contacted by bullies or people who groom or seek to abuse them***
Children may be subject to bullying, harassment or intimidation online. Internet abuse may also include cyber-bullying or online bullying. This is when a child is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child or adult using the internet or mobile devices. It is possible for one victim to be bullied by many perpetrators.

Support and intervention should be provided to both the perpetrator and the victim of the bullying.

Commercialism: ***Young people can be unaware of hidden costs and advertising***
This would include advertising, but also ‘hidden costs’ in games and apps.
When communicating via the internet, people tend to become less wary and talk about things far more openly than they might when communicating face to face. Children and young people should be supported to understand that when they use digital technology they should not give out personal information, particularly their name, address or school, mobile phone numbers to anyone they do not know or trust: this particularly includes social networking and online gaming sites. If they have been asked for such information, they should always check with their a member of staff or other trusted adult before providing such details.

What to do if you have concerns about a child being harmed

Children sometimes feel unable to tell an adult about an online concern they have, because they worry that their device or phone will be removed from them, to 'keep them safe'. They also worry that they will get into trouble. The way adults react to the knowledge that a child may be at risk, or have been exposed to concerning material online is therefore very important.

Children should be supported to be familiar with the *Click CEOP* (Child Exploitation and Online Protection Committee) button and know that they can report directly to CEOP if they have concerns and do not feel that they can tell an adult. CEOP will help them to tell their trusted adults.

All concerns must be reported to the child's Social Worker.

If a staff member is concerned that a child may be at risk online, or may have been exposed to inappropriate material, they should:

- stay calm, and not to over-react or get angry or upset
- inform the Registered / on-call Manager immediately
- save any evidence there may be, ideally by removing the device and preserving the information on it. If this is not possible, taking screenshots is advisable for concerns about bullying, intimidation, radicalisation, grooming and so on, but screenshots must not be taken of any inappropriate images of children or adults. In the case of apps such as 'Snapchat' taking screenshots quickly will be the only way to preserve evidence
- access and follow North Lakes Children's Services safeguarding policy, including exploitation, radicalism and extremism etc. as appropriate

Report it

A number of organisations and providers have specific "report it" functionality to tackle on line abuse. Staff should report any concerning activity to the appropriate bodies and providers.

- If you have **concerns about online 'grooming'** or other concerning activity towards a child, then in an emergency, you must call 999, but otherwise report the activity to the child's social worker, and agree who will notify CEOP.
- If you have concerns about **illegal content** (in the UK that includes child sexual abuse images / obscene adult content then this must be reported to *The Internet Watch Foundation (*an independent not-for-profit organisation that works to stop child sexual abuse online) and the Police.
- Online **terrorism activity** must be reported to the police's Counter Terrorism Internet Referral Unit. A Channel referral should also be made as part of the Prevent programme.
- Suspected online terrorist material should be reported through contact with the Police and https://www.gov.uk/report-terrorism.

- Online content, which incites hatred on the grounds of race, religion, disability, sexual orientation or sex, should be reported to the Police. The True Vision (a reporting function for Hate crimes owned by the Police) has a referral function.
- Online scams can be reported to Action Fraud.
- If you have a concern that a member of staff may have acted inappropriately towards a child, or may have accessed material that depicts harm to a child, you must refer to and follow the relevant Safeguarding Procedures e.g. Managing Allegations against staff or the Whistleblowing Procedure as appropriate.

Notification of Serious Events

Any concerns in relation to a child's use or exposure to social media should be considered in line with the Notification Policy.

Risk Assessment

All risk assessments should include the measures taken to enable the child / young person to use social media and the internet safely and to protect the child / young person from on line harm.

The child / young person's risk assessment should be informed by;

- specific technology that the child will have access to
- agreed rules about access and usage of technology and devices (e.g. where in the home they can be used and when)
- agreed use of privacy settings for social networks and online activity
- installation of parental control tools and how to use them
- any known history or current harm, and agreed actions to manage any risk of harm
- the online contact that children may have with their birth family

Risk factors will change as children continue to grow and develop; therefore, it is important that the risk assessment is reviewed regularly.

How to keep children safer online:

It can be difficult to find the balance between allowing children to reap all the benefits that technology offers them, and keeping them safe. We cannot prevent children from ever being exposed to online risks, so we must educate them about risks they may face and how to keep themselves safe and stress the importance of telling somebody if they have any concerns or worries.

It is very important that adults whom care for children know enough about technology and the associated risks, to be able to advise children about their safety online.

General advice to keep children safer on line

- explain the risks of accepting and making friends online. This includes people they have never met in the real world, but also people from their past
- explain that rules that apply in the real world, also apply online and that they are there to keep them safe
- ensure their privacy settings on social media are set to private, so only people they know and trust can see information about them – most sites have advice to help
- ask them to tell you if someone contacts them online who is not meant to (this may include strangers or members of their birth family). Ask them not to respond or accept them as a friend. Reassure them that they will not get into trouble
- whilst parental controls have their place, many children can 'work around' them. It is extremely important to have conversations about the things children may be exposed to online, and how they keep themselves safe
- monitor children's activity online by using the internet history function on computers and other devices

Top Tips for children and young people

- don't post any personal information online, such as your address, email address or mobile number
- think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore
- keep your privacy settings as high as possible
- make sure your apps are not broadcasting your location without you knowing
- never give out your passwords
- don't become friends with people you do not know
- don't meet up with people you've met online. Tell an adult immediately if anybody suggests this to you
- remember that not everyone online is who they say they are
- think carefully about what you say before you post something online
- if you think a friend or another child is being harmed tell someone you trust
- if you see something online, that makes you feel uncomfortable, unsafe or worried: leave the website, and tell a trusted adult immediately.

Advice and guidance about online safety is updated regularly. Staff should access up to date advice online from organisations such as the NSPCC - Online safety or Internet Matters, Child Exploitation and Online Protection Committee CEOP or the Safer Internet Centre UK - Safer

Reviewed 28.04.2022 by Head of Care
Review by 27.04.2023

Internet Centre. Also visit www.net-aware.org.uk/networks for up to date information on popular websites used by children.

Legislation and References

The Serious Crime Act 2015

An offence of sexual communication with a child has been introduced. This applies to an adult who communicates with a child and the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16 years of age.

The Act also amended the Sex Offences Act 2003 so it is now an offence for an adult to arrange to meet with someone under 16 having communicated with them on just one occasion (previously it was on at least two occasions).

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority
- Obtain unauthorised access to a computer
- "Eavesdrop" on a computer
- Make unauthorised use of computer time or facilities
- Maliciously corrupt or erase data or programs
- Deny access to authorised users.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts
- Ascertain compliance with regulatory or self-regulatory practices or procedures

- Demonstrate standards, which are or ought to be achieved by persons using the system
- Investigate or detect unauthorised use of the communications system
- Prevent or detect crime or in the interests of national security
- Ensure the effective operation of the system
- Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal
    - Protect or support help line staff.

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Sexual Offences Act 2003
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least once (previously twice) (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Counter-Terrorism and Security Act 2015
From 1 July 2015 all Independent Fostering Agencies are included as being subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have 'due regard to the need to prevent people from being drawn into terrorism'.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.