

Online Safety

Safeguarding children and young people online can involve a range of issues e.g. online bullying, pressure to look 'right' and get 'likes', fake news, violence, extremist behaviour, grooming, child sexual & criminal exploitation and sexting.

This highlights the need to educate children, young people, their parents, carers and practitioners about the benefits and risks and provide safeguards and awareness for users to safely control their online experiences.

All settings should have an Online Policy that reflects the setting's approach and operates alongside other policies including:

- Use of cameras and mobile devices
- Social media
- Acceptable ICT Use for practitioners and young people
- Practitioners' and young people's behaviour
- Bullying
- Online safety and the curriculum
- Data protection
- Information sharing and security
- Filtering and monitoring

Online safeguarding depends on effective practice at a number of levels:

- A safe and secure network/broadband connection
- Appropriate and ongoing levels of ICT security at the setting, e.g. firewalls, access restrictions
- Up to date online safety policies that are understood, implemented and regularly reviewed by practitioners, children and young people, parents and carers
- Safe and responsible ICT use by all practitioners, children and young people, parents and carers
- Attending regular training on online safety on the KRSCP website

Assessing and managing risk - the setting should:

- take reasonable precautions to prevent access by practitioners, children and young people to inappropriate material
- maintain an audit of all ICT and social media use
- ensure children and young people are aware of strategies for safe and responsible use of the internet and what to do when things go wrong
- safety-check all sites and links before using with children and young people
- have clear reporting process to deal with problems with all practitioners, children and young people aware of it
- ensure that the Acceptable Use and Online Safety Policies cover all aspects of technology and online environments used in the setting

Communicating with children and young people, practitioners, parents and carers:

- Rules for online safety and internet access should be make clear to everyone.
- Attention should be drawn to online safety in the setting's newsletters, brochures and website

Children, young people, practitioners, parents and carers should:

- Have a thorough understanding and an ageappropriate copy of your Online Safety and Acceptable Use Policies
- Be informed that all internet use may be monitored and traced to the individual user, and therefore appropriate conduct is essential

Images of children and young people and other identifying information should be carefully managed.

Written consent should **always** be obtained from the child/young person and their parents or carers before it is used, and the image should be removed as soon as the child/young person has left the setting.

What is online bullying?

Online bullying can leave children and young people feeling scared, upset, isolated and very vulnerable, particularly as the bullying can happen in their own home.

There are a number of different methods of online bullying, but the main ones are:

- online communication such as messages, texts, emails, photographs, video-messaging, sexting via mobile phones, computers, smartphones, tablets, gaming devices etc. to individuals or groups
- making humiliating and abusive phone calls on mobiles or land lines
- sending inappropriate communication that can be shared with others through social networking and gaming sites
- communicating with friends of the victim and other people to try to make them become part of the bullying
- setting up fake profiles on social networking sites to make fun of a child or young person
- creating a false identity to impersonate someone and send inappropriate communications in their name
- using chat rooms and gaming sites to abuse other players, threaten them, lock victims out of games, and/or spread false rumours
- Sending viruses or hacking programs that can destroy the victim's games, device or delete/harvest personal information from their device
- posting intimate, sensitive and personal information about someone without their permission or knowledge

The communication is threatening, upsetting and/or offensive and may include racist, sexist, or homophobic content.

Some of the above methods can also be used by

Youth gambling:

- In 2019, 11% of 11-16 year olds in Britain reported spending their own money on one or more gambling activities. This equates to approximately 350,000 11-16 year olds (Young People and Gambling Survey 2019 A research study among 11-16 year olds in Britain October 2019)
- It is easier to target children and young people online (advertising, apps, influencers, gaming)
- Build resistance to gambling via

Key points:

- The internet is an important, useful and necessary tool for learning
- Children and young people need to learn how to evaluate internet information and to take care of their own safety and security

Useful web links/resources:

- Child Exploitation & Online Protection Centre (CEOP): Thinkuknow
- Childline Bullying
- Kidscape
- Preventing Bullying, DfE
- UK Safer Internet Centre
- NSPCC NetAware
- YGAM

adults to 'groom' vulnerable children and young people to exploit or radicalise them. They may pretend to be someone else online to:

- befriend a child or young person
- find out sensitive information
- obtain intimate photographs of them
- threaten to expose this information to their family or friends if the child/young person does not do as they say.

Assessing risks and problems – what to do:

Experience of child or young person:		
Universal	Universal plus/partnership plus	Targeted/acute/specialist
 Has a range of IT skills and understands how the internet works and its global audience Safely enjoys the benefits of the internet and is able to communicate safely with friends and family Maintains personal security when using chat rooms, gaming etc. Does not disclose personal details of friends to unknown parties Family aware of use and understand safe use principles Child shares interest with parents 	 Some IT skills but doesn't really understand how the internet works Uses the internet carelessly, visiting unregulated sites Visits adult sites and views explicitly sexual or violent material Is the victim or perpetrator of occasional low level cyber-bullying Has IT skills but using them to access unsuitable areas of the internet Uses the internet to establish contact with unknown others and discloses contact details Transmits pictures/video of self or others which could be used by internet predator or for cyber bullying Discloses address and phone details Agrees to meet stranger 	 Visits illegal sites or sites designed for adults and develops an interest which may lead to criminal or exploitative actions Exposes friends to risk by disclosing details to strangers Posts explicitly violent material photos/video of self or others Discloses stranger abuse resulting from contact Is the victim or perpetrator of sustained and/or serious cyber- bullying that includes disclosure of personal and identifying information Agrees to meet a stranger alone
with peer(s) Action from practitioners:		
 Child is benefiting from parental guidance Continue discussion about online safety 	 Parents, carers and setting provide advice and consider steps which need to be taken Parents and carers are given advice as needed Age appropriate access controls put in place Discuss with DSL Consider action plan 	 Inform DSL Notify police Inform parents/carers if safe to do so Notify other parents/ carers if appropriate
All children and young people should be taught to evaluate the content of online information, e.g.		

All children and young people should be taught to evaluate the content of online information, e.g.

- Are representations of body image photo-shopped or air-brushed?
 - How other people portray their lives online
 - How to spot fake news
 - How to disengage and control their internet use

Safeguarding Assessment

The media often raise concerns about 'unsafe' websites and material online, which can cause panic and result in advice not to use the site in question.

Do not specify the sites that you are concerned about to other practitioners, children and young people and their families as this encourages them to access the site and potentially harmful material on it.

Unsafe sites are often taken down or moved quickly once they are discussed in the media and children and young people instead then access an associated image shared by numerous media outlets or a copycat.

There are three areas of concern for using the internet:

- Content are children and young people accessing harmful material e.g. racist, pornographic, bullying, sexual, homophobic or damaging ideas?
- Contact who else is the child/young person interacting with online and are they encouraging the child/young person to do something harmful?
- Conduct is the child/young person's online behaviour causing concern e.g. making, sending, receiving explicit images, online bullying, racism

Most issues can be resolved through good quality regular education and targeted training in the setting.

What action to take:

- Never publicise 'unsafe' sites as it encourages people to look for it and implies that other sites are 'safe'
- Teach staff, children and young people, parents and carers to act safely in all internet use
- If your concern is low level, discuss with parents or carers & agree a plan
- Assess their needs with an Early Help Assessment (EHP)
- If any child or young person is at risk of significant harm refer them immediately to the Single Point of Access (SPA), tel. 020 8547 5008
- If you think the parents or carers are part of the risk to the child/young person or if a crime may have been committed, do not inform them before you have talked to the SPA team
- Ensure other involved practitioners are aware of your online safety concerns and incorporate this into the support they are providing

Consider:

- What has happened?
- How did it make them feel?
- What did they do?
- Have they posted personal information about themselves or someone else on the internet?
- Is someone they don't know well offline offering e.g. gifts or money for actions or behaviour?
- Have they agreed to meet someone in person that they met through the internet?
- What level of supervision do they have while using the internet?
- Do parents/carers know what sites/material they are accessing?
- Are the parents/carers able to protect the child/young person?
- Are they being shown harmful material by someone they know?
- Does the child/young person understand the risks and if so what reason do they give for taking them?
- Are you concerned that the child/young person is at risk of or suffering significant harm & if so refer immediately – details below)

If you have concerns about the internet use of a specific child/young person you need to assess their safeguarding needs in the same way as you assess other safeguarding needs that children and young people may have. You can ask:

- what they have seen or done
- any impact it has had on them
- what their support needs are