Online Safety

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

Settings need to educate pupils, parents, carers & staff about the benefits and risks of using this environment and provide safeguards and awareness for users to safely control their online experiences.

Online safeguarding good practice:

- Safe & secure network & broadband connection
- Compliant Information Communication Technology (ICT) security e.g. firewalls, access restrictions
- Up-to-date online-safety policies are understood, implemented & regularly reviewed by staff, pupils, parents & carers
- Staff, pupils, parents/carers responsible ICT use
- Education & training includes progressive & age appropriate online safety curriculum

All settings should have:

- A trained Online-Safety Coordinator who is also a trained Designated Safeguarding Lead/Deputy
- An Online-Safety Policy that reflects your whole-school approach alongside other policies including:
  - Use of cameras, mobile devices, social media
  - Acceptable ICT Use for staff & pupils
  - Pupil and staff behaviour including bullying
  - Online safety & the curriculum
  - Data protection, information sharing & security
  - Filtering and monitoring

The Online-Safety Coordinator is responsible for:

- Undertaking SCSP training
- Safeguarding students online & assessing the needs of students who may be at risk
- Supporting & educating staff, parents & carers

Communication with pupils, staff, parents, carers should include:

- Rules for online safety & internet access in all areas of the setting
- Articles about online-safety in setting newsletters, publicity, website etc.

Pupils, staff, parents, carers should be able to:

- Access & fully understand your age-appropriate Online Safety & Acceptable Use Policies
- Use the internet appropriately & know their use can be monitored & traced to individual users

Assessing & managing risk - settings should:

- Take reasonable precautions to prevent pupil & staff access to inappropriate sites or material
- Maintain an audit of all ICT & social media use
- Teach pupils about responsible & safe use of the internet and what to do when things go wrong
- Ensure staff check sites & links before pupil usage
- Ensure all online platforms used to communicate with pupils & their families (e.g. learning online at home) are fully risk-assessed & monitored
- Ensure all staff & pupils are aware of & can access a clear reporting process for online-safety issues
- Ensure their Acceptable Use & Online Safety Policies considers how all technology, online environments & mobile devices communicate one; access social networks, music, videos & gaming sites; take photographs & record videos
- Carefully manage images & other identifying information about students; obtain their written consent before use; remove/delete image when student has left the setting

Cyber-bullying can make children feel scared, upset, isolated & vulnerable, particularly as it can happen whilst alone and/or in their own home.

The main methods of cyber-bullying are:

- Messages, texts, emails, photographs, video's, sexting, to individuals or groups
- Communicating threats, upset, offense &/or includes racist, sexist, or homophobic content
- Humiliating/abusive phone calls
- Inappropriate communication shared through social networking & gaming sites
- Encouraging other people to bully the victim
- Setting up fake profiles to make fun of someone
- Creating a false identity to send inappropriate communications in someone else's name
- Using chat rooms & gaming sites to threaten, abuse, lock out, &/or spread rumours
- Send viruses or hacking programs to harvest information or destroy someone's game/device
- Post intimate, sensitive & personal information without someone's permission or knowledge

An adult may use the above methods to pretend to be someone online to befriend, obtain sensitive information/materials & threaten to expose information to their family or friends if they do not do as they say.

Online Safety

It is a crime to:

- Harass or bully via text, email or phone call
- Create, possess, distribute indecent images of child even with consent or if self-generated
- For an adult to have sexual communication with a child under 16 years

The age of criminal responsibility is 10 years.

Other issues:

- Taking a photograph without consent is an invasion of privacy & may be distressing
- Once photos are sent to a device, network or website they are impossible to fully track or delete
- Giving out any personal information (including photos) could put someone at risk of harm
- Location tracking services allow any individual to identify the location of people & devices

Head Teachers & staff have powers to search pupils & their possessions, see:

- 'Reasonable force, searching & screening, Sept 20A' in **education policies, procedures & guidance**, Safeguarding Sheffield Children website.

3 key concerns when using the internet:

- **Content** – harmful material or ideas e.g. racist, pornographic, bullying, sexual, homophobic
- **Contact** – who interacting with online, are they encouraging student to do something harmful?
- **Conduct** –online behaviour e.g. making, sending, receiving explicit images, bullying, gambling
- Most issues can be resolved through regular education and targeted training.

Consider whether the student was:

- Posting inappropriately on the internet?
- Offered e.g. gifts or money for something?
- Meeting someone through the internet?
- Supervised whilst using the internet?
- Supported/protected by parents/carers?
- Being shown harmful material?
- Able to understand & give reasons for risk-taking?
- At risk of or suffering significant harm?

Youth gambling:

- 17% of under 16's gambled online in last 7 days
- Targeted through adverts, apps, influencers, gaming, etc.
- Teach about gambling issues via the curriculum

Top tips:

- **Never publicise 'unsafe' sites**: it encourages people to look & implies other sites are 'safe'
- Teach staff, students, parents & carers to act safely in all internet use
- If your concern is low level, discuss with parents or carers & agree a plan
- Where appropriate, assess child and families needs with an FCAF
- **If any child or young person is at risk of significant harm refer them immediately to The Sheffield Safeguarding Hub, tel. 0114 2734855 or to their current social worker**
- If you think parents/carers are part of the risk] or if a crime may have been committed, **do not inform them before** you discuss with The Hub
- Ensure other involved practitioners are aware of your online safety concerns and incorporate this into the support they are providing

Useful links:

- Safeguarding Sheffield Children website: Online Safety
- Sheffield Children Safeguarding Partnership Procedures - Online Safety
- UK Safer Internet Centre
- Screening, Searching & Confiscation: advice for schools, DfE 2018
- Safeguarding and remote education
- NSPCC NetAware
- Preventing Bullying, DfE
- NSPCC: Sexting
- Thinkuknow
- YGAM

Assessing risks and problems

Child or young person's level of need:

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 with peer(s)	• 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 sexual/ violent material including photos/ video of self or others • Discloses stranger abuse resulting from internet contact • Is the victim or perpetrator of sustained and/or serious cyber-bullying that includes disclosure of personal and identifying information • Agrees to meet stranger alone

Action from practitioners:

• Child is benefiting from parental guidance and curriculum activity • Continue discussion about online safety in curriculum	• Parents, carers and school 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/D in school • Consider action plan	• Inform DSL/D • Notify police • Inform parents/carers if safe to do so • Notify other parents/carers if appropriate

All pupils/students 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**