E-Safeguarding

All education settings should be safe environments for children and young people to learn.

The purpose of internet use in educational settings is to raise educational standards and promote achievement, support the professional work of staff & enhance the settings' management of information, communication and administration systems between staff, pupils and parents or carers.

Therefore safeguarding children and young people online can involve a range of potential issues such as cyberbullying, extremist behaviour, grooming, child sexual exploitation and sexting.

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

All settings should have an E-Safety policy that reflects the settings whole-school approach and should operate alongside other policies including:

- Student and staff behaviour
- Bullying
- Curriculum
- Data protection
- Information sharing and security

E-safeguarding depends on effective practice at a number of levels:

- Safe and secure network and broadband connection from the Yorkshire and Humberside Grid for Learning or your Internet Service Provider
- Appropriate and ongoing levels of ICT security at the setting, e.g. firewalls, access restrictions etc
- Up to date E-Safety policies that are understood, implemented and regularly reviewed by staff, pupils and parents
- Safe and responsible Information & Communication Technology (ICT) use by all staff, pupils and their parents & carers
- Education and training including a progressive and age appropriate e-safety curriculum

Top Tips:

- **E-safety is part of the statutory computing curriculum**
- **The internet is a necessary tool for learning – encourage safe use**
- **Access to the internet is an entitlement for students who show a responsible and mature approach to its use**
- **Students 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 (CEOPS): Thinkuknow
- Childline - Bullying
- Kidscape
- Preventing and Tackling Bullying, Department for Education
- UK Safer Internet Centre

Related documents in the Education Policies & Procedures section of website:

- **Mobile devices, Sept 15**
- **Photographs, videos and other images, Sept 15**
- **Bullying and abuse by children and young people, Sept 15**
- **Child Sexual Exploitation, Sept 15**

If any Sheffield practitioner needs advice and support, they can contact:

Safeguarding Children Advisory Service

Mon-Fri, 9-4.30pm, tel 205 3535

What is cyber-bullying?

Cyber-bullying happens 'online' through electronic information technology with a widespread audience and numerous devices to communicate through.

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

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

- Electronic communication such as messages, texts, emails, photographs, video-messaging, sexting via mobile phones, computers, smart-phones, tablets etc to individuals or groups
- Communication is threatening, upsetting or offensive and may include racist, sexist, or homophobic content
- Making humiliating and abusive phone calls on mobiles or land lines
- Sending innappropriate 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 'profiles' on social networking sites to make fun of a child or young person
- Creating a false identity to impersonate someone and send innappropriate communications in their name
- Use chat rooms and gaming sites to abuse other players, use threats, lock victims out of games, spread false rumours
- Sending viruses or hacking programs that can destroy the victim's computer or delete personal information from their hard drive
- Posting intimate, senstitive and personal information, about someone without their permission or knowledge

The above methods can also be used by adults to 'groom' vulnerable children and young people in order to sexually exploit them.

These people pretend to be someone else online in order to be-friend a child or young person, find out sensitive information or obtain intimate photographs of them, and then threaten to expose this information to their family of friends.

Assessing and managing risk - the setting should:

- Take reasonable precautions to prevent access by students and staff to inappropriate material
- Maintain an audit of all Information and Communication Technology use at the setting
- Make students aware of strategies for safe and responsible use of the internet and what to do when things go wrong
- Staff should safety-check all sites and links before using with students
- The use of social media should be risk-assessed and carefully controlled within the setting
- 'Managed' Learning Environments' (MLE) must be thoroughly risk assessed and monitored
- A clear reporting process should be in place to deal with problems and all staff and students made aware of it
- Ensure that your 'Acceptable Use' and 'E-safety' policies cover all aspects of technology and online environments used in the setting.

Images of students and other identifying information should be carefully managed; written consent should be obtained from the student and their parents or carers before it is used, and the image should be removed as soon as the student has left the setting.

Communicating with pupils, staff, parents and carers:

- Rules for e-safety and internet access should be posted in all classrooms
- Pupils, staff, mothers, fathers and carers should:
  - Have a thorough understanding and an age-appropriate copy of your 'E-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
- Attention should be drawn to the 'E-safety' policy in newsletters, brochures and on the website for the educational setting

Assessing risks and problems – what to do:

Experience of child or young person:		
Universal	**Universal plus/targeted**	**Acute/specialist**
• Has a range of IT skills and understands how the internet works and it's 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	• 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 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 e-safety in curriculum	• Mothers, fathers, carers and school provide advice and consider steps which need to be taken • Access control needed • Discuss with DSL in school • Consider action plan	• Inform DSL • Seek advice from Safeguarding Children Advisory Service • Notify police • Inform parents if safe to do so • Notify other parents if appropriate