

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

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

Safeguarding children & young people online can involve a range of issues e.g. cyberbullying, pressure to look 'right' & 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 & staff about the benefits & risks of using this environment & provide safeguards & awareness for users to safely control their online experiences.

All settings should have an [Online Safety Coordinator](#) and an Online Safety Policy that reflects the setting's whole-school approach and operates alongside other policies including:

- Use of cameras & mobile devices
- Social media
- Acceptable ICT Use for staff & pupils
- Pupil/student and staff behaviour
- Bullying
- Online safety & the curriculum
- Data protection
- Information sharing and security
- Filtering and monitoring

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

- Safe & secure network/broadband connection
- Appropriate & ongoing levels of Information & Communication Technology (ICT) security at the setting, e.g. firewalls, access restrictions
- Up to date online-safety policies that are understood, implemented & regularly reviewed by staff, pupils/students, parents & carers
- Safe & responsible ICT use by all staff, pupils/students, parents & carers
- Education & training **including a progressive & age appropriate online safety curriculum**

Assessing and managing risk - the setting should:

- Take reasonable precautions to prevent access by pupils/students and staff to inappropriate material
- Maintain an audit of all ICT & social media use
- Make pupils/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 pupils/students
- '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 pupils/students made aware of it
- Ensure that your Acceptable Use and Online Safety Policies cover all aspects of technology and online environments used in the setting

Communicating with pupils/students, staff, parents and carers:

- Rules for online safety and internet access should be posted in all classrooms
- Attention should be drawn to online safety in the setting's newsletters, brochures and website
- Pupils/students, staff, parents and carers should:
 - Have a thorough understanding and an age-appropriate 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 students and other identifying information should be carefully managed.

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



What is cyber-bullying?

Cyber-bullying can leave children & young people feeling scared, upset, isolated & 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:

- Online communication such as messages, texts, emails, photographs, video-messaging, sexting via mobile phones, computers, smart-phones, tablets, gaming devices etc. to individuals or groups
- The communication is threatening, upsetting and/or offensive and may include racist, sexist, or homophobic content
- 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

Some of the above methods can also be used by adults to 'groom' vulnerable children and young people in order to exploit or radicalise them. They may pretend to be someone else online in order 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.

Youth gambling:

- Around 17% of under 16 year olds have spent own money on gambling activity in last 7 days
- It is easier to target children & young people online (advertising, apps, influencers, gaming)
- Build resistance to gambling via curriculum

All education settings **must** have an Online-Safety Coordinator who is trained about online safety and safeguarding and is part of the safeguarding children team.

For more information go to: [Safeguarding Sheffield Children website: Online Safety Coordinators](#)

Key points:

- **The internet is an important, useful and necessary tool for learning**
- **Pupils/students need to learn how to evaluate internet information and to take care of their own safety and security**
- **Online safety is part of the statutory computing curriculum**

Related documents in the [Education Policies, Procedures & Guidance section](#) of the **Safeguarding Sheffield Children website:**

- **Mobile devices**
- **Photographs, videos and other images**
- **Child Sexual Exploitation**
- **Peer Abuse**
- **Abuse of Trust**

Useful web links/resources:

- [Safeguarding Sheffield Children website: Online Safety](#)
- [SCSP Procedures - Online Safety](#)
- [Child Exploitation & Online Protection Centre \(CEOP\): Thinkuknow](#)
- [Childline - Bullying](#)
- [Kidscape](#)
- [Preventing Bullying, DfE](#)
- [UK Safer Internet Centre](#)
- [NSPCC NetAware](#)
- [YGAM](#)



Assessing risks and problems – what to do:

Experience of child or young person:		
Universal	Universal plus/partnership plus	Targeted/acute/specialist
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • 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:		
<ul style="list-style-type: none"> • Child is benefiting from parental guidance and curriculum activity • Continue discussion about online safety in curriculum 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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

Safeguarding Assessment

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

Education settings need to support students to access material safely. The SSCB [Safeguarding Sheffield Children](#) website contains some useful information including:

- [Online Safety and the Curriculum](#)
- [Online Safety Policy](#)
- [Online Safeguarding, Sept 19](#)

Do not specify the sites that you are concerned about to staff, students and their families as this encourages them to access the site & potentially harmful material on it.

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

[Online-Safety Coordinators](#) are responsible for:

- Undertaking training from the SCSP
- Safeguarding student's online
- Supporting & educating staff and parents online
- Working with the safeguarding team to assess the needs of students who may be at risk.

There are 3 areas of concern for using the internet:

- **Content** – are students accessing harmful material e.g. racist, pornographic, bullying, sexual, homophobic, or damaging ideas?
- **Contact** – who else is the student in interacting with online and are they encouraging the student to do something harmful?
- **Conduct** – is the student'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 & targeted training in the setting.

If you have concerns about the internet use of a specific student you need to assess their safeguarding needs in the same way as you assess other safeguarding needs that children & young people may have.

You can ask what:

- **They have seen or done**
- **Impact it has had on them**
- **Their support needs are**

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 whilst using the internet?
- Do parents or carers know what sites/material they are accessing?
- Are the parents/carers able to protect the student?
- Are they being shown harmful material by someone they know?
- Does the student understand the risks & if so what reason do they give for taking them?
- Are you concerned that the student is at risk of or suffering significant harm & if so refer immediately – details below)

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, students, parents & 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 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 their current social worker**
- If you think the parents or carers are part of the risk to the student or if a crime may have been committed, **do not inform them before** you have talked to The Hub
- Ensure other involved practitioners are aware of your online safety concerns and incorporate this into the support they are providing