Online Safety Policy

Online safety is an integral part of safeguarding and requires an approach and collaboration between all parties involved. This policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), and NSPSS guidance. It designed to sit alongside or be integrated into SE Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the SE safeguarding and child protection procedures.

The KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract.) These are known as the 4 Cs of online safety:

- Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, radicalisation and extremism.

- Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

- Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

- Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

KCSIE makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection. DSL responsibilities:

- Promotes an awareness and commitment to online safeguarding throughout the SE community
- To ensure that all SE staff and Homestays are aware of the procedures that need to be followed in the event of an online safety incident
- To ensure that an online safety incident log is kept up to date
- Facilitates training and advice for all SE staff
- Liaises with the Local Authorities and relevant organisations

- Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from:
    1. sharing of personal data
    2. access to illegal / inappropriate materials
    3. inappropriate online contact with adults / strangers
    4. potential or actual incidents of grooming
    5. online bullying and use of social media

Homestays Responsibilities:

- To make sure students in their care use the internet and mobile devices according to the guidance in Homestay Handbook
- To support SE in promoting online safety
- To consult with the SE Staff if they have any concerns about their children's use of technology

SE Staff responsibilities:

- To read, understand and help promote the Online Safety Policy
- To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices
- To report any suspected misuse or problem to DSL
- To maintain an awareness of current online safety issues and guidance
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with pupils and parents should be on a professional level
- To maintain confidentiality at all times and never share any images or content regarding students on any social media platform

Online Abuse

The following information about abuse online is taken from the NSPCC website:

https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/

Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones. Children and young people may experience cyberbullying, grooming, sexual abuse, sexual exploitation or emotional abuse.

Children can be at risk of online abuse from people they know, as well as from strangers. Online abuse may be part of abuse that is taking place in the real world (for example bullying or grooming). Or it may be that the abuse only happens online (for example persuading children to take part in sexual activity online).

Children can feel like there is no escape from online abuse – abusers can contact them at any time of the day or night, the abuse can come into safe places like their bedrooms, and images and videos can be stored and shared with other people.

Internet Policy

It is our policy to make sure that all our Guardian Homestays are well informed about the types of online abuse and the signs and symptoms to look out for. This information is shared through sources such as this handbook and in our workshops. We also seek to ensure that all our Guardian Homestays

know how to respond with regard to recording information, not guaranteeing confidentiality and informing the appropriate persons.

Bullying Online or Cyberbullying

Cyberbullying is an increasingly common form of bullying behaviour which happens on social networks, games and mobile phones. Cyberbullying can include spreading rumours about someone, or posting nasty or embarrassing messages, images or videos.

Children may know who's bullying them online – it may be an extension of offline peer bullying - or they may be targeted by someone using a fake or anonymous account. It's easy to be anonymous online and this may increase the likelihood of engaging in bullying behaviour.

Cyberbullying includes:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations.

Online Grooming

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking.

- Children and young people can be groomed online or face-to-face, by a stranger or by someone they know - for example a family member, friend or professional.
- Groomers may be male or female and could be any age. Many children and young people don't understand that they have been groomed or that what has happened is abuse.
- Groomers can use social media sites, instant messaging apps including teen dating apps, or online gaming platforms to connect with a young person or child. They can spend time learning about a young person's interests from their online profiles and then use this knowledge to help them build up a relationship.
- It's easy for groomers to hide their identity online - they may pretend to be a child and then chat and become 'friends' with children they are targeting.
- Groomers may look for: usernames or comments that are flirtatious or have a sexual meaning public comments that suggest a child has low self-esteem or is vulnerable.
- Groomers don't always target a particular child. Sometimes they will send messages to hundreds of young people and wait to see who responds.
- Groomers no longer need to meet children in real life to abuse them. Increasingly, groomers are sexually exploiting their victims by persuading them to take part in online sexual activity.

Sexual Abuse Online

When sexual exploitation happens online, young people may be persuaded, or forced, to:

- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone
- have sexual conversations by text or online

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in other sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

How to spot Abuse, signs and symptoms

The signs of child abuse aren't always obvious, and a child might not tell anyone what's happening to them.

Children might be scared that the abuser will find out, and worried that the abuse will get worse. Or they might think that there's no-one they can tell or that they won't be believed.

Sometimes, children don't even realise that what's happening is abuse. Below is list of things to look out for:

- Becomes secretive and reluctant to share information.
- Reluctant to go to school/home to parents/home to guardian homestay host
- Unwilling to bring friends home or reluctant for professionals to visit the family home/homestay home or school
- Poor school attendance and punctuality
- Parents show little interest in child's performance and behaviour at school.
- Parents are dismissive and non-responsive to professional concerns.
- Is reluctant to get changed for sports etc.
- Wets or soils the bed.
- Drinks alcohol regularly from an early age, experiments with drugs such as marijuana
- Is concerned for younger siblings without explaining why.
- Becomes secretive and reluctant to share information.
- Talks of running away.
- Shows challenging/disruptive behaviour at school or in the homestay • Is reluctant to get changed for sports etc.

Lines of communication

Allegations of abuse made by a child should be reported as follows:

- A child should speak to a member of the SE personnel
- If the alleged abuser is the SE staff the child should initially report it to another member of SE's personnel. This individual should then report the matter to a senior member of staff, or to the Social Services Department, whichever is appropriate.
- A child should speak to one of the adults of the homestay about any abuse that is taking place if appropriate

Any person responsible for the welfare of a child has a duty under English law to report any suspicions of abuse to the relevant authority.

Reporting and recording action

Sutherland Education is extremely diligent in keeping detailed and accurate records (mostly electronically) of communications and situations regarding each student, and of actions taken. Please use the opportunity freely to email us about your student, in all aspects of his or her life in your home. We are particularly interested in the level of commitment to study and personal development.

Digital images and video:

SE gain parental permission for use of digital photographs or video involving their child as part of the guardianship. SE do not identify students in online photographic materials or include the full names of pupils in the credits of any produced marketing material.

There is the rapid rise of generative AI, thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI "girlfriends," unregulated therapy bots, and even chatbots that encourage self-harm or suicide—tools many students can access freely at home or school. Chatbots can also blur reality, offer harmful advice or engage in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation.
When used for generating text, GenAI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content.
AI create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. Alarming reports also show children using nudifying apps to create illegal content of peers.

According to Ofcom's *'Children and parents: media use and attitudes report 2025'* has shown that YouTube remains the most used site or app among all under 18s, followed by WhatsApp, TikTok, Snapchat and Instagram.
https://www.ofcom.org.uk

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Any suspected online risk or infringement should be reported to the Designated Safeguarding Lead as soon as possible on the same day.

Any concern/allegation about staff misuse is always (similar to any safeguarding allegation) referred directly to the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

SE will actively seek support from other organisation as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

SE will inform parents of online safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

Nudes – sharing nudes and semi-nudes

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area.

DSL is to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL**.

DSL and Prevent Staff: Andrew Sutherland, mob. 07774646886

DDSL and Prevent Staff: Wioletta Laszyn. tel. 02038083800

Policy date: **17th October 2025**
Responsibility for Policy Review: **Wioletta Laszyn**

Useful links:

https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

https://www.ofcom.org.uk