Online Safety Policy

Overview

All ICON staff, host family members, and students should understand the importance of adopting good online safety practices, reporting misuse, abuse, or access to inappropriate materials, and knowing how to report these concerns.

An effective approach to online safety can protect and educate children in their use of technology and offers the ability to identify, intervene in, and escalate any incident where appropriate. Education for our students about maintaining a healthy and safe online presence is key. This policy should be read in conjunction with our Safeguarding Policy.

This policy has been written using guidance from 'Keeping Children Safe in Education' (September 2024) and NSPCC advice on 'Online Safety'. The policy will be reviewed annually by the Designated Safeguarding Lead (DSL) and Head of Compliance.

Categories of Online Safety Risks

Online safety risks can be broadly categorized into three areas:

- **Content:** Exposure to illegal, inappropriate, or harmful material, such as web pages containing indecent images of children or pro-eating disorder or self-harm websites.
- **Contact:** Harmful online interaction with others, including cyberbullying or grooming.
- **Conduct:** Personal online behavior that increases the likelihood of harm.

What is Online Abuse?

The NSPCC defines online abuse as any type of abuse that happens on the internet, whether through social networks, playing online games, or using mobile phones. Children and young people may experience:

- Cyberbullying **(bullying via technology, including social media, gaming sites, and mobile phones)**
- Grooming **(building an emotional connection with a child to exploit them)**
- Sexual abuse **(including sexting or youth-produced imagery)**
- Sexual exploitation
- Emotional abuse

Cyberbullying

Cyberbullying can happen at any time and is often difficult to trace. It includes:

- Sending threatening or abusive messages
- Creating and sharing embarrassing images or videos
- 'Trolling' (sending upsetting messages online)
- Excluding children from online activities or groups

- Setting up hate sites
- Encouraging self-harm
- Creating fake accounts to impersonate or embarrass someone
- Pressuring children into sending explicit messages or engaging in sexual conversations

Grooming

Grooming involves building a relationship with a child online to abuse them. This can include:

- Using social media, games, and chatrooms to contact children
- Creating multiple fake identities to trick children
- Learning personal information from posts to target vulnerable children
- Persuading children to chat privately and later exploit them

The ultimate goal of grooming is to sexually abuse a child, either online or in person. It is crucial that students understand how to report any concerns and avoid meeting people they have only interacted with online.

Signs of Online Abuse

Potential indicators of online abuse include:

- Being upset after using the internet or mobile phone
- Secretive online behaviour
- Increased or decreased time spent online
- Receiving messages from unknown contacts
- Avoiding school or social situations
- Difficulty sleeping or low self-esteem

Parental Controls and Privacy Settings

Host families are encouraged to use privacy settings, parental controls, and built-in safety features from internet service providers. Resources for parental controls can be found at:

- www.saferinternet.org.uk/parental-controls/
- www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Social Network Sites

Students should understand how to report concerns on social media platforms. They should be aware of:

- Blocking features
- Privacy settings
- The importance of managing their digital footprint

Further guidance can be found at: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/taking-care-your-digital-footprint/

Procedure for Dealing with an Online Incident

If an online safety concern is reported by a student, parent, or staff member, the following steps must be taken:

- Record the disclosure using the designated form.
- Report the incident verbally as soon as possible to the Designated Safeguarding Lead (DSL) or Deputy DSL (Ben Hughes in her absence).
- Submit a written record of the disclosure to the DSL
- The DSL will report the incident to the student's school DSL and ensure an action plan is implemented.
- If required, the school will contact parents or carers unless doing so would put the student at risk.
- If a child is at immediate risk of harm, the incident should be reported to the police by dialling 999.

When to Involve the Police

Police involvement is necessary if:

- The incident involves an adult
- There is evidence of coercion, blackmail, or grooming
- The content includes unusual or violent sexual acts
- The imagery involves children under 13
- A child is at immediate risk of harm (e.g., suicidal thoughts)

If a staff member views youth-produced sexual imagery, they must report it immediately and seek emotional support if required.

Support for Students and Staff

ICON will work with schools to support affected students. We will also ensure that staff members who encounter distressing content receive appropriate support.

For further information on online safety, please visit:

- NSPCC: www.nspcc.org.uk/keeping-children-safe/online-safety
- Think U Know: www.thinkuknow.co.uk/parents/articles/reporting-to-social-media-sites/

This policy will be reviewed annually to ensure it remains aligned with best practices and legal requirements.

This policy reviewed on 3rd April 2025, next review date is 2nd April 2026.