Online Safety (E -Safety Policy) and Guidance.

This policy links to the SOGA Safeguarding and Child Protection Policies and outlines how we ensure that we maximize the safety of our students who use the internet and related communication technologies.

The good practice in the policy content is aligned to the requirements of Keeping Children Safe in Education 2023. Policy: This document is based on guidance from the Home Office 'Keeping Children Safe in Education' (September 2024), and NSPCC advice on 'Online Safety'.
National Society for the Prevention of Cruelty to Children.

The guidance for students and host families has been tailored from the policy and included within the Student Handbook and Host Family Handbook.

We share by email information to Host families to ensure that there is an awareness of how to minimize the risks attached to digital and video images of students.

Host Families
Host families play a crucial role in ensuring that the students who stay with them use the internet and mobile devices in accordance with the guidance contained within the Host Family Manual.

SOGA will take every opportunity to help host families understand the issues through website links to the NSPCC updates containing online safety news and advice.

SOGA proactively raises awareness of high-profile events including Safer Internet Day through the website and email information.

Students
Students are responsible for using the internet and mobile devices in accordance with the guidance in the Student Handbook. Students must know the importance of adopting good online safety practice and reporting misuse, abuse or access to inappropriate materials and know how to report these concerns.

SOGA further supports students in raising their awareness of how to stay safe online through our, policies, and website

Online Safety –

An effective approach to online safety empowers a school, college, guardian or host family to protect and educate children in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable but can be categorized into three areas of risk:

Content:

Being exposed to illegal, inappropriate, or harmful material, for example web pages, indecent images of children or pro-eating disorder or self-harm websites

Contact:

Being subjected to harmful online interaction with other users, for example cyberbullying or grooming.

Conduct:

Personal online behavior that increases the likelihood of, or causes, harm. What is online abuse?
The NSPCC defines online abuse as any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones.

Commerce:

Risks such as online gambling, inappropriate advertising, phishing and or financial scams
Any person at risk, please report to Anti-Phishing Working Group https://apwg.org

Children and young people may experience cyberbullying (*bullying that takes place using technology including social media sites, mobile phones, gaming sites*), grooming (*building an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation, or trafficking*), sexual abuse, 'sexting' or youth produced imagery, sexual exploitation, county lines gang recruitment, radicalisation or emotional abuse from people they know as well as from strangers.

SOGA Guardianship clearly has a role to play in reporting signs of possible online abuse early so that prompt action can be taken to protect any children who are found to be at risk.

Possible signs of online abuse:

The NSPCC list possible signs of a child experiencing abuse online if they demonstrate a change in behavior or unusual behavior:

Being upset after using the internet or their mobile phone
.
Unwilling to talk or be secretive about their online activities and mobile phone

use. Spending much more or much less time texting, gaming, or using social

media.

Many new phone numbers, texts or email addresses show up on their mobile phone, laptop, or tablet.

After texting or being online they may seem withdrawn, upset, or outraged.

Not wanting to go to school and/or avoiding meeting friends and school

mates. Avoiding formerly enjoyable social situations.

Difficulty sleeping.

Low self-esteem

The possible signs of abuse could be seen through reports from students or schools, incident reporting by staff, and/or Host families reports.
.

SOGA would encourage Soga members and host family members to set an appropriate agreement with students in order to supervise internet access and set boundaries about what they can and cannot do online.

If a child breaks the rules!!

We would ask the host family to restrict internet access for an agreed period. Below is some suggested advice for talking to children about online safety:

https://www.thinkuknow.co.uk/parents/articles/having-a-conversation-with-your-child https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online

We would ask the host families to use privacy settings, parental controls and built-in internet safety features provided by the major internet service providers.

The UK Safer Internet Centre has guides for parental controls (host families) https://www.saferinternet.org.uk

Parents and carers (host families) experiencing any internet safety issues with their children, O2 and the NSPCC have set up a helpline: 0808 800 5002 Filters and monitoring

SOGA asks host families to be doing all that they reasonably can to limit children's exposure to the above risks from the IT systems at the home. As part of this process, host families should ensure appropriate filters and monitoring systems are in place.

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, host families should consider the age range of their pupils, the number of pupils, and how often they access the IT system.
The NSPCC website 'Online Safety' outlines controls that host families can implement to filter and monitor what a child in their house can see, including checking that parents know how to use privacy settings and reporting tools:
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

The NSPCC provide advice for host families on parental controls which allow a number of different things to happen including filtering and blocking content, setting different profiles so that each family member can access age appropriate content and restricting information that can be shared:
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online safety/parental-controls/

Staying safe on mobiles

Smartphones and tablets The NSPCC advice for tracking children's online activity via devices includes:
Location tracking,
Taking and sending pictures, setting up parental controls, public Wi-Fi, parent protection apps

Full details can be found on the website: https://www.nspcc.org.uk/preventing abuse/keeping-children-safe/online-safety

Social network sites Children and young people connect online with friends, make new

friends, and browse the internet for information, chat with others and play games. This may include using search engines, sharing images, watching videos, using social network sites, playing games, and chatting with people through online gaming.

Host families are advised to ensure that their own children and/or SOGA students know where the reporting functions are on each of the sites they use, how to block someone and how to keep information private.

The NSPCC encourage talking to children about social networks using 'Net Aware' to stay up to date with the social network sites and what you need to know about for example reporting and privacy settings: https://www.net-aware.org.uk Safety (E-Safety) Policy - SOGA Policies – www.scottishoverseasguardianship.co.uk

The NSPCC encourage talking to children about online privacy and being 'Share Aware': https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware Further reading: NSPCC Online Safety: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

Child Exploitation and Online Protection Centre: CEOP: Child Exploitation & Online Protection Centre – internet safety CEOP: Thinkuknow: https://www.thinkuknow.co.uk

UK Safer Internet Centre
https://www.saferinternet.org.uk

Disrespect Nobody
find out about healthy relationships and respecting each other:
https://www.disrespectnobody.co.uk

Internet matters
Helping parents keep their children safe online:
https://www.internetmatters.org

How social media,
Is used to encourage travel to Syria and Iraq: A briefing note
https://www.gov.uk/government/publications/the-use-of-social-media-for-online radicalisation

Procedure for dealing with an incident which involves online services:

A SOGA member receives the report of suspected online abuse from a student, parent or other source by face-to-face disclosure, email, or telephone call.

A SOGA member adheres to the Child Protection Policy including listening and recording the disclosure in the most appropriate format (using the 'Tell Explain Describe' model open ended questions, if the information is being given by a student).

The record of the disclosure is reported verbally as soon as practicable to the Designated Safeguarding Lead (DSL), Mrs Pamela Keracher 07762791805.

The SOGA member must submit a written record of the disclosure on the Student Record and email the report to pamkerachersoga@hotmail.co.uk

The DSL will hold an emergency strategy meeting to discuss the incident, assess the alleged threat and risk to the child (including any relevant facts about the child which may affect their vulnerability including age and ability), implement an action plan and continue to review the situation until a resolution has been achieved.

The meeting will be recorded with timed and dated entries within a Student Record – Incident Record to record all actions and updates.

The DSL will arrange for the young person to be helped and supported in recognition of the pressures (and possible vulnerabilities) they may have been under as a result of the suspected abuse.

This could include helping them to understand how to recognise the early signs of online abuse, the wider issues and motivations of online abuse and making available relevant information and material.

This help and support could be provided through talking to a member of the SOGA team or from accredited organisations such as the school, National Society for the Prevention of Cruelty to Children (NSPCC), ChildLine and National Crime Agency (NCA) – Child Exploitation and Online Protection Centre (CEOP) websites and helpline.

The DSL will ensure that viewing of the images or other content is only made where there are good and clear reasons to do so (unless unavoidable because the student has willingly shown a member of staff), basing incident decisions on what the DSL has been told about the content of the imagery or other content.

The DSL will ensure that SOGA members do not search through devices and delete imagery unless there is a good and clear reason to do so.

The DSL will consider the need to ask for the student to produce the device as evidence. The viewing of any images, other content or seizing of any devices will be recorded including those present, date and time to meet SOGA standards set out for recording incidents

The DSL will consider the need to contact another school, college, setting or individual and whether to contact the parents or carers of the children involved. In most cases parents should be involved unless there is good reason to believe that involving these parties would put the young person at risk of harm.

The incident will be referred to a statutory agency (Children's Services on the Local Authority telephone number or the police by dialing 101) immediately if there is a concern a young person has been harmed or is at immediate risk of harm (telephone the police by dialing 999). This would include information coming to light if at the initial

stage

The incident involves an adult
There is reason to believe that a young person has been coerced, blackmailed, or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
What you know about the imagery or other content suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

The imagery or other content involves sexual acts and any pupil in the imagery is under 13

You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self harming Where the material or activities found or suspected are illegal and there is no immediate risk to the child, The Child and Exploitation Online Paedophile Unit should be informed. If none of the above apply, the DSL may decide (with input from key stakeholders if appropriate) to respond to the incident without involving the police or children's social care.

The DSL can choose to escalate the incident at any time if further information/concerns come to light. The decision should be recorded in line with the Safeguarding Policy and Child Protection Policy, found on the website www.scottishoverseasguardianship.co.uk and regularly reviewed throughout the process of responding to the incident. The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved, and the risks can be managed within the SOGA support framework and network for the child.

The DSL will advise the young person to delete imagery or other content, and to confirm they have deleted the imagery. Young people should be given a deadline for deletion across all devices, online storage, or social media sites on the basis that possession of youth produced sexual imagery is illegal. Where a young person refuses or is later discovered to have not deleted the images or other content, they are committing a criminal offence and the police may become involved. A record will be made of these decisions as per the Safeguarding Policy including decisions, times, dates, and reasons. SOGA may wish to invoke their own measures to discourage young people sharing, creating or receiving images in line with behaviour policies.

. Where the DSL is aware that youth produced sexual imagery or other content has been unavoidably viewed by a member of staff, the DSL should ensure that the staff member has appropriate support. Viewing youth produced sexual imagery or other content can

be distressing for both young people and adults and appropriate emotional support may be required.

Where police action has been instigated for an incident involving a member of SOGA internal procedures will take place at the conclusion of the police action.

A suspension will likely take place before the internal procedures begin. .

Issued July 2024