Online activities with children – safety and social media policy

This policy applies to all staff, volunteers, children and young people and anyone involved in SGI-UK’s activities. It provides guidance on how SGI-UK uses the internet and social media and the procedures for doing so, in particular relation to its activities for people under the age of 18. It also outlines how we expect the staff and volunteers who work for us, and the children or young people who take part in activities within our organisation, to behave online.

This policy should be read alongside SGI-UK’s policies, procedures and guidelines on child protection and safeguarding.

SGI-UK provides Future Division activities nationally and locally for young people between the ages of 7 and 18. Due to the ages of the Future Division members, we need to take extra steps to safeguard against potential abuse in line with our statutory obligations under law. We have drawn up this policy in line with guidance from the Charity Commission and the NSPCC.

This policy seeks to:

- To protect all children and young people involved in our organisation who make use of technology (such as mobile phones, games consoles, and the internet) while engaging in our activities.
- To provide staff and volunteers with policy and procedure information regarding online safety and inform them on how to respond to incidents.
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we behave online.

Legal framework
This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England, Scotland, Wales and Northern Ireland. Summaries of key legislation and guidance are available from the NSPCC: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

We believe that:
Children and young people should never experience abuse of any kind. Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

Understanding the online world
As part of using the internet and social media, SGI-UK will:
• Understand the safety aspects – including what is acceptable and unacceptable behaviour for staff and children – when using websites, social media, apps and other forms of digital communication.
• Be aware that it does not matter what device is being used for digital interaction, but that the same safety aspects apply whether it is a computer, mobile phone or game console.
• When using social media platforms (including Facebook, Instagram, snapchat and Twitter) ensure we adhere to relevant legislation and good practice guidelines.

Managing our online presence
• All social media accounts will be password protected, and the Safeguarding team and SGI-UK staff responsible for social media will have access to each account and password.
• All accounts will be monitored by SGI-UK staff responsible for social media who will report to the Safeguarding team in SGI-UK, seeking advice from them with regards to safeguarding requirements.
• SGI-UK staff responsible for social media will remove inappropriate posts by children, staff or members, and work with the Safeguarding team to inform anyone who may be affected, including the parents of any children involved.
• SGI-UK makes every effort to ensure that we do not use images of children on official social media channels.
• SGI-UK staff responsible for social media will be clear that personal information such as home addresses and contact details should never be posted on social media platforms.
• We will make sure children and young people know who to contact if they have concerns about the running of an account or platform they are using.
• It is highly unlikely that it would be appropriate for anyone to communicate with a child through social media, but if this happens, parental permission will be sought first.
• Parental permission must be given before any image or video of a child is posted on our social media channels.
• All of our accounts and email addresses shall be appropriate and fit for purpose.
• Under-18s will not be included in any online meetings (except Indigo Group meetings, for young people aged 15-18) without a parent or guardian present.
• In Indigo Group meetings (for young people aged 15-18), online meetings must include at least two Safeguarding supervisors of volunteers present in each online room as best practice. In-person and online future division meetings must include at least two safeguarding supervisors of volunteers present in each room as best practice.
• While we are working towards appointing more safeguarding supervisors of volunteers, at least one safeguarding supervisor of volunteers and one supporter who has an enhanced DBS check through SGI-UK must be present in each room. This is so that no adult (aside from parents or guardians) is alone with a child in an activity.

We will seek to keep children and young people safe by:
• Providing clear directions to staff and volunteers on how to behave online.
• Encouraging young people to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
• Supporting and encouraging parents and carers to do what they can to keep their children safe online.
• Responding appropriately to any incidents of inappropriate online behaviour.
• Reviewing and updating the security of our information systems regularly.
• Ensuring that user-names, logins, email accounts and passwords are used effectively ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
• Ensuring that images of children, young people and families are not circulated online or posted on social media by SGI-UK
• Raising awareness among staff and volunteers about online safety.
• Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

What we expect from our staff and volunteers
• Staff, members and volunteers should be aware of this policy and behave in accordance with it.
• Staff, members and volunteers should seek the advice of the Safeguarding team if they have any concerns about the use of the internet or social media.
• Staff, members and volunteers should not ‘friend’, ‘follow’ or communicate with children or young people using social media. They should not contact under-18s for any reason apart from SGI-UK Future Division activities. For guidance on how to contact under-18s regarding SGI-UK activities, see below.
• Communication regarding Young Eagles, Mimosa or Rising Phoenix activities (for children aged 7-14) should always be directed through a parent or guardian. Staff, members and volunteers must not engage personally by email, text or online with children about these activities.
• Communication regarding Indigo Group activities (for young people aged 15-18) can be made directly with the young people concerned with prior written parental consent only, and then by email only, always cc’ing the parents and the national Indigo Group leaders.
• Apart from information about Indigo Group activities, staff, members and volunteers must not engage personally by email, text or online with anyone under 18. All communication should be made with the parents or guardians face to face, on the phone, by text or message, in an email or in writing.
• Emails and communications should be signed off in a professional manner, avoiding the use of emojis or symbols such as ‘kisses’ (‘X’).
• Any disclosures of abuse reported through social media should be dealt with in the same way as a face-to-face disclosure, according to our reporting procedures.
• Notice should be given when images are taken at SGI-UK activities. Smartphone users should take care to not take or distribute pictures of others on social media.
• Staff, members and volunteers will avoid having children’s or young people’s personal mobile numbers and instead seek contact through a parent or guardian.
• Staff, members and volunteers must not engage in sexting, or send pictures or messages to anyone that are obscene, indecent or menacing.
• If a child or young person misinterprets communications from adults and tries to engage in social conversation, the adult will take the following steps:
  o End the conversation or stop replying.
  o Suggest discussing the subject further at the next activity.
  o If concerned about a child or young person’s welfare, pass this on to the Safeguarding team.

What we expect of children and young people
• Children and young people should be made aware of this policy.
• Children and young people should sign an online activities agreement before engaging in online activities with SGI-UK.

Using mobile phones and devices during Future Division activities
So that children can enjoy and actively take part in Future Division activities, SGI-UK discourages the use of mobile phones by staff, members and volunteers while they are supporting the activity. However, communication is vital and staff, members and volunteers will therefore:

• Make parents and Indigo Group members aware of who to contact in the case of an emergency or a change in arrangements.
• Inform parents and carers of the appropriate times they can contact their children, when they are staying at an overnight activity and discourage them from making contact outside of those times.
• Provide parents and carers with an emergency contact should they need to immediately reach their child.
• Explain to children and young people that that SGI-UK activities are on the whole, ‘off-line’ activities, and that mobile phone usage can detract from their experience of the activity.
• Remind children and young people about safe online and mobile phone behaviour.

Use of other digital devices and programmes
The principles in this policy apply no matter which current or future technology is used – including laptops, computers, tablets, web-enabled games consoles and smart TVs – and whether an app, programme or website is used. SGI-UK will establish the appropriate restrictions, i.e. ‘parental controls’ on any device owned and used within SGI-UK’s online network to prevent misuse or harm.

Ratified: May 2023
Review by Trustees due: May 2024