Online Safety and Social Media Policy

Introduction

This policy provides guidance on how Surrey Clubs for Young People (SCYP) and our Youth Clubs use the internet and social media and the procedures for doing so. It also outlines how we expect the staff and volunteers who work for us, and the children and young people who are members of our organisation, to behave on-line.

Young people will be known as members for the purposes of this document.

Aims

The aims of our online safety policy are:

- To protect all members involved with our organisation and who make use of technology (such as mobile phones, games consoles and the internet) whilst in our care.
- To provide staff and volunteers with policy and procedure information regarding online safety and to inform them how to respond to incidents.
- To ensure our organisation is operating in line with our values and within the law regarding how we behave online.

Understanding the online world

As part of using the internet and social media, our organisation will:

- Understand the safety aspects, including what is acceptable and unacceptable behaviour for staff, volunteers and young people, when using websites, social media, apps and other forms of digital communication.
- Be aware that it doesn't 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, Twitter, and Instagram) ensure that we adhere to relevant legislation and good practice guidelines[2].
- Regularly review existing safeguarding policies and procedures to ensure that online safeguarding policies are fully intergraded, including:
    - Making sure concerns of abuse or disclosures that take place online are written into our reporting procedures.
    - Incorporating online bullying (cyberbullying) in our anti-bullying policy.
- Provide training for the person responsible for managing our organisation's online presence.

Managing our online presence

Our online presence through our website and social media platforms will adhere to the following guidelines:

- All social media accounts will be password protected, and at least three members of the clubs 'team' (one must be a trustees and/or senior youth worker) will have access to each account and password.
- The accounts will be monitored by a designated person, who will be appointed by the club's trustees.
- The designated person managing our online presence will seek advice from our designated safeguarding lead to advise on safeguarding requirements.
- A designated supervisor will remove inappropriate posts by members, staff and volunteers, explaining why, and informing anyone who may be affected (as well as the parents/guardians of any members involved).
- Account, page and event settings will be set to private so that only club members can see their content.
- Identifying details such as a young person's home address, school name or contact details should not be posted on social media.
- Identifying details such as a / volunteer / staff members home address or contact details should not be posted on social media.
- Any posts or correspondents will be consistent with our aims.
- We will make sure that our members are aware of who manages our social media accounts and who to contact if they have any concerns about the running of the account.
- Parents/guardians will be asked to give their approval for us to communicate with their children through social media, or by any other means of communication. [1]
- Parents/guardians will need to give permission for photographs or videos of their child to be posted on social media. [4]
- All of our accounts and email addresses will be appropriate and fit for purpose.

What we expect of staff and volunteers

- Staff/volunteers should be aware of this policy and behave in accordance with it.
- Staff/volunteers should seek the advice of the designated safeguarding lead if they have any concerned about the use of the internet or social media.
- Staff/volunteers should communicate any messages they wish to send members to the designated person responsible for the organisations online presence.
- Staff/volunteers should not 'friend or follow' members from their personal accounts on social media.
- Staff/volunteers should make sure any content posted on their own personal accounts is accurate and appropriate, as young people can 'follow' them on social media.
- Staff (Youth Workers) may wish to use a variation of their own name when using their personal account so that members cannot seek them out.
- Rather than communicating with parents through personal social media accounts, staff/volunteers should choose a more formal means of communication, such as face-face, in an email or in writing, or use organisational account, profile, website.
- At least one other member of staff/volunteer should be copied into any emails sent to members.
- Staff/volunteers should avoid communicating with members via email outside of normal office hours. If staff/volunteers only have the opportunity to email during evening club time, this is acceptable but should be completed as early on in the club hours as is possible and no later than 7.00pm.
- Emails should be signed off in a professional manner. Avoid the use of emoji's or symbols such as 'kisses' (xx).
- 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.
- Smartphone users should respect the private lives of others and not take or distribute pictures of other people if it could invade their privacy.
- Staff/volunteers and members must not engage in 'sexting' or send private pictures to anyone that are obscene, indecent or menacing.

What we expect of your members (young people)

- Members should be aware of this online safety policy and agree to its terms.
- We expect member's behaviour online to be consistent with the guidelines set out in our acceptable use statement. [3]
- Members should follow the guidelines in our acceptable use statement on all digital devices, including smart phones, tablets and consoles. [3]

Using mobile phones or other digital technology to communicate

When using mobile phones (or other devices) to communicate by voice, video or text (including texting, email and instant messaging), we will take the following precautions to ensure young people's safety.

- Staff/volunteers will avoid having members personal mobile number and will instead seek contact through a parent or guardian.
- We'll seek parental permission on each occasion we need to contact members directly and the purpose for each contact will be clearly identified and agreed upon.
- A method of accountability will be arranged; such as copies of texts also being sent to the club's lead welfare officer (or equivalent) or to parents/guardians.
- Staff/volunteers should have a separate phone from their personal one for any contact with parents or members. This should be a club asset and recorded on the club's asset list.
- Texts will be used for communication information, such as reminders about upcoming events or to bring items to the club only. Text should not be used to engage in conversation.
- If a member misinterprets such communication and tries to engage staff/volunteers in conversation, the staff member /volunteer will take the following steps:
    - End the conversation and stop replying.
    - Suggest discussing the matter further at the next club night.
    - If concerned about the member, provide contact details for the club's welfare officer (or equivalent staff member/volunteer) or appropriate agencies.

Using mobile phones during club night and activities

So that all members can enjoy and actively take part in activities, we discourage the use of mobile phones during club activities. As part of this policy we will:

- Make members aware of how and who to contact if there is an emergency or a change to previously agreed arrangements with the club.
- Inform parents/guardians of appropriate times that they can contact members who are away at camps or away trips and discourage them from making contact outside of these times.
- Advise parents that is may not be possible to contact members during activities and provide a contact within the club or organisation who will be reachable should there be an emergency.
- Explain to members how using a mobile phone during activities has an impact on their safe awareness of their environment, and their level of participation and achievement.

Use of other digital devices and programmes

The principles in this policy apply no matter which current or future technology is used including, computers, laptops, tablet, web-enabled games consoles and smart TVs and whether an app programme or website is used.

If any digital devise is used as part of activities within the club:

- We expect members to adhere to the guidelines surrounding online use and behaviour set out in our acceptable use document. [3]
- We will establish appropriate restrictions (parental controls) on any device provided to prevent misuse or harm.

[1] Request for consent form which is available from SCYP

[2] https://thecpsu.org.uk/help-advice/topics/online-safety/

[3] Acceptable Use statement for internet and social media use available from SCYP

[4] Permission is part of the SCYP membership form which is available from SCYP

Supporting Information

In England and Wales, the Defamation Act 2013 makes the website host responsible for removing defamatory material posted to a site.

Section 103 of the Digital Economy Act 2017 requires social media platforms across the UK to follow a code of practice which sets out the actions they must take to protect individuals from bullying, intimidation and insulating behaviour online.

In April 2019 the Department for Digital, Culture, Media and Sport (DCMS) and the Home Office opened a public consultation on their Online Harms White Paper. This sets out the measures the government intends to take to keep UK users safe online, including a new regulatory framework for online platforms (DCMS, 2019).

The Information Commissioner's Office's (ICO) Age appropriate design: code of practice for online services sets out 15 standards that providers of online products or services likely to be accessed by children should comply with. The code explains how providers can design services that appropriately safeguard children's personal data and comply with data protection and privacy laws. The code is expected to come into force by autumn 2021, following Parliamentary approval (Information Commissioner's Office, 2020).

Key guidance

Across the UK, statutory guidance highlights the responsibility of those in the education, community and care sectors to safeguard children from all forms of abuse and neglect including online abuse:

- Child protection legislation and guidance in England
- Child protection legislation and guidance in Northern Ireland
- Child protection legislation and guidance in Scotland
- Child protection legislation and guidance in Wales
- Key guidance for schools in the UK

There is also more specific guidance for people who work with children about safeguarding children from online abuse.

Keeping children safe from online abuse

The UK Home Office has published guidance aimed at tech firms, the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse. The guidance is comprised of 11 actions that online companies should take to tackle online sexual exploitation, including on tackling child sexual abuse material, online grooming and livestreaming of child sexual abuse. The guidance was developed in collaboration with the Governments of Australia, Canada, New Zealand and the USA (Home Office, 2020).

The UK Council for Internet Safety (UKCIS) has produced a framework (PDF) for people who work with children across the UK that highlights the digital skills and knowledge children need to stay safe online. It includes discussion around:

- online relationships
- online reputation
- online bullying (UKCIS, 2018).

UKCIS also provides guidance about online safeguarding in early years settings for managers and practitioners (UKCIS, 2019).

In England, the Department for Education (DfE) has published non-statutory guidance on teaching online safety in school (PDF). (DfE, 2019)

The Home Office has developed an Online abuse and bullying prevention guide (PDF) for those who work with young people in England and Wales. This aims to help them understand the types of online abuse, its consequences and where to go for help. Topics covered include:

- threatening behaviour
- cyberbullying
- online grooming (Home Office, 2015).

The Department of Education Northern Ireland provides Internet and WiFi guidance which includes a range of advice on how internet technology can be used safely in schools. Topics covered include:

- online safety
- mobile and digital devices
- guidance on using the internet safely (Department of Education, 2018).

Key policy

The government's Online Harms white paper sets out the measures the government intends to take to keep UK users safe online, including:

- establishing a new statutory duty of care and regulatory framework to ensure online platforms take responsibility for the safety of their users
- a new independent regulator to implement, oversee and enforce the regulatory framework and raise awareness about online safety (DCMS, 2019).