

Online Safety and Social media Guidance

Updated October 2025



- 1. Introduction
- 2. Aim
- 3. Online Safety
- 4. Keeping Athletes Safe
- 5. Definition of Social Media
- 6. Staff and Volunteer Responsibilities
- 7. Social Media in Your Personal Life
- 8. Personal Online Relationships
- 9. Reporting Concerns

1. Introduction

At Special Olympics GB (SOGB) we recognise that the online world provides many opportunities to those who use it; however, it can also present risks and challenges and we have a duty to ensure that all Athletes involved in SOGB are provided, where appropriate, with the right knowledge and tools to protect themselves from potential harm online. We have a responsibility to ensure Athletes are kept safe from online risks and harm while in attendance at all SOGB activity including but not limited to; club activity, events, competitions, SOGB Social events, media events and any SOGB online activities, where access is in our control.

SOGB will endeavor to make the best use of all available technology and innovation to improve the way we operate. This includes using all reasonable and cost-effective means to improve the way we communicate and interact with our athletes, volunteers and families, corporate partners as well as the general public.

Online communication tools such as emails, the <u>SOGB website</u> and social media platforms offer SOGB a great opportunity to connect with many of our members and interested parties.

These tools and platforms open up many new and exciting opportunities. However, the practical application of such technology by SOGB is continually developing and there are many potential issues to consider – both as individual employees and as an organisation.

To mitigate risk that may result in reputational, legal and ethical issues, and/or the misuse or abuse of online communication tools, it is important that we **manage** any potential risks through a commonsense approach and framework as well as proactively monitoring the development of such applications.

2. Aim

The aim of this guidance document is to provide SOGB Staff, Volunteers, Athletes and Families with information concerning online risks which include but are not limited to online abuse, exploitation and other forms of harm that may occur online. In addition, this guidance outlines the appropriate use of, or the development of any social media application or online communication tools in order for members to get the best out of the tools available whilst maintaining a safe professional environment and endeavouring to protecting all involved at SOGB.

3. Online Safety

It is important to understand what constitutes online safety risks, so you are able to spot concerns and act quickly to safeguarding Athletes and/or yourselves. Below are some common online risks to familiarise yourselves with.

Grooming

How it works: Is a process that involves building a relationship with a child or vulnerable adult, gaining their trust and a position of power over them in preparation for abuse.

Tactics used: Flattery, affection, gifts, or threats to manipulate and isolate victims, asking victims to keep secrets, with the intention to exploit them in some way (sexually/financially/criminally).

Staying safe: Where appropriate, monitor online activity and educate Athletes about online predators. Teach them to never share personal information with strangers online, use appropriate privacy settings, block certain software, talk openly about grooming.

Learn more: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/

Catfishing

How it works: Someone creates a fake online identity in order to build emotional or romantic relationships with unsuspecting victims.

Tactics used: Emotional manipulation, gaining trust over time, and exploiting vulnerabilities (e.g., loneliness or desire for connection).

Staying safe: Verify the identity of people you meet online by checking multiple sources or using reverse image searches and look for any inconsistencies. Do not share personal information with strangers.

Phishing Scams

How it works: Attackers trick people into revealing sensitive or personal information (passwords, credit card numbers, etc.) by pretending to be trustworthy entities like banks, employers, or social networks.

Tactics used: Urgency, fear, or fake authority (e.g., "Your account has been compromised, click here to verify").

Staying safe: Use two-factor authentication (2FA) and be cautious about clicking links in unknown emails or texts, verify the URL's and avoid opening attachments from unknown sources.

Imposter Scams

How it works: Scammers pose as trusted figures, like family members, friends, representatives from legitimate businesses or officials, to gain money, information, or access to account information.

Tactics used: Creating scenarios where victims feel compelled to act quickly, such as pretending to be a relative in need.

Staying safe: Be wary of anyone asking for money or personal information, especially in emergency situations. Contact the person directly if you're unsure – scammers may use technology to make it appear that they are calling from a legitimate number.

Online Extortion and Sextortion

How it works: Manipulators coerce victims into sending compromising material, then threaten to release it unless the victim pays or provides them with something else such as sexual acts.

Tactics used: Blackmail, leveraging shame or fear of public exposure.

Staying safe: Avoid sharing compromising materials, and report sextortion attempts immediately to the appropriate authorities.

Cyberbullying and Harassment

How it works: Perpetrators use psychological manipulation to degrade, humiliate, or coerce individuals, this can be one-to-one or in group settings.

Tactics used: Name calling, sending hurtful private messages, public shaming, threats, removal from social groups, or intimidation that impacts a person's emotions negatively.

Staying safe: Document incidents of cyberbullying and report them to the platform and/or authorities. Use privacy settings to block offenders. Speak to a member of the SOGB Safeguarding Team.

Learn more: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/

Online Radicalisation

How it works: Online radicalisation is the process in which someone comes to adopt extreme beliefs and, in some cases, starts to support or even plan acts of violence driven by ideology. Radical content ranges from overt calls to violence to subtle messaging underpinned by an "us versus them" mentality. It might normalise conspiracy theories, fuel resentment or frame certain groups as threats, gradually shaping how someone sees the world.

Tactics used: This often happens through digital channels such as social media, forums or private messaging apps. Online radicalisation tends to be more isolated, often happening privately and out of sight, sometimes behind encrypted apps or anonymous platforms, but sometimes in public forums and more generalised posts.

Staying safe: Create a safe space to discuss concerns openly and positively so you can challenge the narrative, making efforts not to "shut it down" but to listen and provide alternative points of view. Report any concerns to the SOGB Safeguarding Team for advice, and support. If you have concerns that the person poses a risk or has developed extremist views, you must report this to the relevant authorities (The Police Prevent Teams), information, support and guidance from the Police can be found HERE.

All of the above can take place on various online platforms including social media, websites, via emails, texts, messaging apps, forums and in online gaming platforms.

4. Keeping Athletes Safe

SOGB will seek to keep Athletes safe by:

- Ensuring that our Safeguarding Lead has the appropriate knowledge and training to respond to any online safety concerns effectively.
- Providing clear and specific directions to Athletes, Staff and Volunteers on how to behave online through this guidance, our Codes of Conduct and additional relevant policies and procedures.
- Providing support and training as appropriate for all Athletes, Staff and Volunteers on dealing
 with all forms of abuse, including online safety risks, bullying/cyberbullying, emotional abuse,
 sexting, sexual abuse and sexual exploitation.
- Supporting and encouraging Athletes to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Developing online safety resources for Athletes and families and signposting Athletes and families to already existing online safety resources, information and support.
- Developing and communicating clear and robust procedures to enable SOGB to respond appropriately to any incidents of inappropriate online behaviour, that involves an Athlete, Family Member, Volunteer or Member of Staff.
- Working in partnership with Athletes, their families and other agencies to promote Athlete welfare and to support Athletes to be responsible in their approach to online safety.

5. Definition of Social Media

'Social media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online. As the name

implies, social media involves the building of online communities or networks to encourage participation and engagement.

For the purposes of these guidelines, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes email, online social forums, blogs, video and image-sharing websites and similar facilities. (This may include platforms such as YouTube, X, TikTok, Snapchat, Facebook and Instagram).

SOGB Staff and Volunteers should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. SOGB Staff and Volunteers should follow these guidelines in relation to any social media that they use.

6. Staff and Volunteer Responsibilities

SOGB encourages Staff and Volunteers to make reasonable and appropriate use of social media and online communication tools to promote SOGB's work and to communicate with SOGB Members and other interested parties. It is recognised that it is an important part of how SOGB communicates with its audience and allows communication and networking between Staff, Volunteers, Athletes, Families and Partners.

Staff and Volunteers must be aware at all times that, while contributing to SOGB's online presence, promotion of events and/or organisational awareness and information sharing, they are representing SOGB.

Staff and Volunteers who use social media as a way of communicating SOGB activities, events, updates and information outwardly to Members, Athletes and the Public should adhere to the following guidance when doing so:

- Ensure that the communication has a purpose and/or is of benefit to SOGB and/or its Members (Volunteers and Athletes).
- Use the same safeguards as they would with any other type of communication about SOGB that is in the public domain.
- Ensure that all communication is respectful.
- Ensure that all communication is in line with ethos and values of SOGB

Any communications that Staff and Volunteers make in a professional capacity through online communication must not:

- Reveal confidential or intellectual property or information about SOGB.
- Include any confidential information about an individual (such as a Staff Member, Volunteer or Athlete) or other organisation (such as a partner).
- Discuss SOGB's internal workings (such as agreements that it is reaching with clients/customers or its future business plans that have not yet been communicated to the public).
- Make offensive, untrue or derogatory comments especially relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.
- Use social media to bully another individual or group or make any comments which could constitute unlawful discrimination or harassment.
- Post content that is illegal, discriminatory or inappropriate or links to any such content.
- Attribute personal statements, opinions or beliefs to SOGB or when expressing personal beliefs
 or opinions, not expressly or implicitly represent themselves as an employee of SOGB.

Staff and Volunteers using online communication must take care not act in a way that is detrimental to or that may bring SOGB, or its Staff, Volunteers or Athletes into disrepute, for example by:

Criticising or arguing with Staff members, Athletes, Families, Partners or members of the public.

- Making defamatory comments about individuals, SOGB or other organisations or groups.
- Posting content that is illegal, inappropriate or links to inappropriate content.
- Impersonating someone else.

Staff and Volunteers using online communication must also take care not to breach copyright, for example by:

- Using someone else's content or intellectual property without permission.
- Failing to give acknowledgement where permission has been given to reproduce something.

7. Social Media in Your Personal Life

SOGB recognises that Staff and Volunteers may use social media in a personal capacity. While they are not acting on behalf of SOGB, Staff and Volunteers must be aware that there is a potential for them to damage the reputation of SOGB if they are recognised as being one of our employees and post something that is not in line with SOGB ethos and values.

Staff and Volunteers are permitted to say that they work or volunteer for SOGB in online communications. SOGB recognises that it is natural for its Staff and Volunteers to sometimes want to discuss their work on social media. The employee's online profile (for example, the name of a blog or a Twitter name) may contain SOGB's name, but should be focused to the area in which the Staff Member or Volunteer operates within.

If Staff or Volunteers do discuss their work on social media (for example, giving opinions on their specialism or the sector in which SOGB operates), they should include a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of SOGB."

Any communications that employees make in a personal capacity through social media must not:

- Reveal confidential intellectual property or information owned by SOGB.
- Give away confidential information about an individual (such as a Staff Member, Volunteer or Athlete) or organisation (such as a partner).
- Discuss SOGB's internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public).

Staff and Volunteers posting in a personal capacity must be mindful not to communicate anything that could be considered discriminatory against, or bullying or harassment of, any individual, or groups for example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.
- Using social media to bully or harass another individual (SOGB Staff Member, Volunteer, Athlete or member of the public).
- Posting images that are illegal, discriminatory or inappropriate or links to such content.

Staff and Volunteers posting in a personal capacity must be mindful not to bring the Organisation into disrepute, for example by:

- Criticising or arguing with Staff members, Athletes, Families, Partners or members of the public.
- Making defamatory comments about individuals or other organisations or groups.
- Posting content that is illegal, discriminatory and/or inappropriate or links to such content
- Posting or communicating defamatory comments or content in relation to SOGB.

8. Personal Online Relationships

It is likely that through SOGB activity, Staff, Volunteers and Athletes will build connections and networks that may lead to online connections, such as on those social media platforms. It is vital that these connections are safe and remain appropriate at all times. When communicating with staff, volunteers and athletes online and via social media this should be done with transparency and be in line with SOGB's codes of conduct.

Staff and Volunteers should not privately message or befriend athletes online unless there is an already established family or close family friend connection. If you receive private message requests or friend requests from Athletes you are not already closely connected to, politely decline these and explain that communicating privately is not in line with SOGB online safety guidance.

9. Reporting Concerns

Reporting online safety concerns is vital in ensuring Athletes, Volunteers and Staff can be protected from online abuse, harm and risk. Reporting concerns means that action can be taken to mitigate any risk or exposure to risk that may be present.

If you have any concerns regarding online safety risks, you should inform your Club Safeguarding and Welfare Officer (SWO) as quickly as possible. If your Club SWO is unavailable, you should contact the SOGB Safeguarding Team on 07383 389663 during the hours 9 - 5 Monday to Friday. Alternatively you can email safeguarding@sogb.org.uk

For more information on how to report a concern at SOGB, go to Report a Concern page on our website HERE

If an athlete is in immediate danger contact the emergency services by calling 999.

You can also contact your Local Authority Safeguarding Services which can be found using the below links:

England

Children: https://www.gov.uk/report-child-abuse-to-local-council Adults: https://www.gov.uk/report-abuse-of-older-person

Scotland

Children: https://www.mygov.scot/report-child-abuse/

Adults: https://www.actagainstharm.org/getting-help/find-your-local-contact

Wales

Children: https://gov.wales/reporting-suspected-abuse-harm-or-neglect-safeguarding Adults: https://www.cysur.wales/contacts-and-useful-links/reporting-concerns-adult/

Online Safety advice and guidance links:

Keeping children safe online | NSPCC

https://www.anncrafttrust.org/safer-online-lives-internet-use-and-safety-for-adults-with-intellectual-disabilities/