Bouncing Statistics

Online Safety and Social Media Policy

Lead member of staff:	Ryan Blackwood—Designated Safeguarding Lead
Required on the website:	Yes
Revised Date	08/2025
Next Revision Date	08/2026
Signed by:	R.Blackwood

Key Notes

- The terms ‘child’ or ‘children’ apply to anyone under the age of 18.
- The term ‘parent’ applies to anyone with guardianship or parental responsibility for the child.
- The term ‘staff’ applies to employees and volunteers.

Safety Statement

This policy outlines how Bouncing Statistics uses the internet and social media responsibly and the procedures for doing so. It explains how we expect our staff to behave online and reflects our commitment to keeping children safe when using technology. This policy also ensures we comply with safeguarding, data protection laws (including UK GDPR), and best practice guidelines such as the Children’s Code and Ofcom/NSPCC standards.

Aim of Our Policy

- To protect all children involved with our organisation who use technology (such as mobile phones, game consoles, or the internet) while in our care.
- To provide staff with clear information on online safety procedures and how to respond to concerns.
- To ensure our organisation operates within the law and in line with our values for online behaviour and digital communication.

Understanding the Online World

We will:

- Assess and manage online safety risks — including acceptable and unacceptable behaviour for staff and children on websites, social media (Facebook, TikTok, Instagram, X, Snapchat), apps, and video conferencing platforms (Zoom, Teams, Meet).
- Be mindful of staff’s online activity both inside and outside of our setting.
- Ensure all platforms used have age-appropriate privacy settings, following the Children’s Code.
- Adhere to relevant legislation, including UK GDPR, the Children’s Code, and other best practice guidance.
- Provide annual training for all staff on online safety and privacy matters.
- Regularly review and integrate online safeguarding into our wider safeguarding policies — including cyberbullying, grooming, and harmful content.

Managing Our Online Presence

- Our organisation's digital activity through the website or social media platforms will follow these principles:
- All accounts will be password-protected and monitored by at least two designated staff.
- The Designated Safeguarding Lead (DSL) will advise on any safeguarding or online safety issues.
- We will never post identifying details of a child, such as name, address, or contact information.
- Content shared will align with our tone, mission, and age-appropriateness.
- Parental consent (opt-in) is required for sharing any photos or videos of children.
- Video conferencing must be password protected, and parental approval and supervision are required.
- All platforms used must support high default privacy settings in line with the Children's Code.

Staff Expectations

- Staff must seek advice from the DSL if they have any concerns about internet or social media use.
- Personal social media accounts must not be used to communicate with children.
- Staff should direct any child-related communication through designated organisational accounts.
- Staff must not 'friend', 'follow' or privately message children.
- Public personal profiles should remain professional, as children may see them.
- Staff must use company email or approved communication channels when contacting parents and maintain a professional tone.
- Messages sent to or from organisational accounts should not be deleted.
- Staff must undertake online safety training annually and understand how to report and block harmful content.
- Any concern raised through social media should follow the same procedures as face-to-face safeguarding disclosures.
- A parent, guardian, or teacher must be present during any activity conducted over video conferencing.
- Staff and children must never engage in sexting or share inappropriate images.

Using Mobile Phones and Digital Technology

- Communications (texts, emails, messages) must also be copied to a second staff member for transparency.
- Staff must respect others' privacy and must not take or share photos that could breach personal boundaries.
- Work phones should be used for any parent/guardian contact.
- Digital communication must be factual only, for example, reminders or logistics, not conversational.

If a child/parent misinterprets communication, the staff member will:

- Stop replying.
- Suggest discussing in person.
- Inform the DSL.
- Provide contact details for the DSL or relevant agency and record the concern.

Mobile Phone Use During Sessions

- To ensure safe, focused participation in our sessions for example interventions, tutoring, and sports sessions, we will:
- Explain to children how phones impact awareness, participation, and learning.
- Inform parents of the best times to contact children and discourage unnecessary contact.
- Make staff contact details available during trips or camps.
- Staff must not use personal phones during sessions unless necessary for safety.

Data Protection (UK GDPR & Children's Code)

- We will only collect and process children's data where we have a clear lawful basis (e.g., consent, safeguarding duty).
- Data will be kept secure, used minimally, and deleted when no longer needed.
- Children and parents will be informed about how their data is used and their rights under UK GDPR.
- Platforms must respect child privacy and avoid manipulative design or profiling.
- A named Data Protection Officer (DPO) or equivalent will oversee compliance and respond to any concerns.

Reporting Concerns

- Online incident occurs (e.g., inappropriate message, exposure to harmful content):
- Report immediately to the DSL or designated online safety lead.
- Record the incident in the safeguarding log.
- DSL will assess the case and determine the action required.

If the incident involves illegal material, for example, exploitation or abuse, notify DSL, and then we will contact the police immediately, and do not view or share the content.

DSL will support staff, update policies as needed and liaise with external authorities.

Important Contacts

Ryan Blackwood – Designated Safeguarding Lead

Phone number: 07881 095 259

Email: ryan.blackwood@bouncingstatistics.com