



*This policy is adapted from the Online Safety Policy developed by the **English Bridge Union (EBU)** and **English Bridge Education & Development (EBED)**. The World Bridge Federation gratefully acknowledges both organisations for permission to adapt this material.*

Online Safety Policy

This policy provides guidance on the procedures that support and govern the use of online bridge platforms social media, and other digital services within the WBF. It is essential that all staff, volunteers, coaches, officials/TDs, board/trustee members, and anyone working on behalf of the organisation are aware of and agree to the terms outlined in this policy.

Aims

- To protect young people when playing bridge online.
- To safeguard young people who use technology (such as mobile phones, games consoles, handheld devices, and the internet) while under the care of the WBF.
- To provide staff and volunteers with clear information about online safety policies and procedures.
- To ensure that the WBF operates in line with its values and complies with relevant laws regarding the use of information technology.

Part 1: Online Bridge

Particular care must be taken when young people play or learn bridge online. Parents should be advised to check the safety controls provided by any online bridge platform before allowing their children to use it. Young players participating in open games are advised not to identify themselves as minors in their profiles or usernames.

Each platform has different safety features and arrangements. Any communication from coaches or adults to young people via online chat must always be polite, supportive, professional, and strictly limited to bridge-related topics.

RealBridge

RealBridge is an online bridge platform that includes integrated video and audio features. It is normally considered a safer environment than many other platforms because access is restricted via a private link shared with a limited group of participants, who are usually known to the event organiser. This platform is the one recommended for playing, teaching and training young people.

The director or lead teacher of a RealBridge event involving young people must hold a valid background check and have completed safeguarding training provided by the WBF. Other teachers involved should also undergo background checks if they engage in regulated activity online with young people (i.e., more than three sessions in a 30-day period).

If a RealBridge event involves the use of screens, parents must be informed that their child may be online alone with adult participants. It is recommended that a parent or guardian be present in the room while the child is playing.

Bridge Base Online (BBO), Bridge Club Live, FunBridge, and IntoBridge

These sites have open membership and public chat facilities. They require greater parental supervision. Young people should use a nickname and avoid using a personal photo to prevent being identified as minors.

BBO is deemed to be a site for players aged 18 and over. However, young people may safely access BBO's tools that do not engage with other people and do not require logging in, such as: *Mini-Bridge, Bridge Master, Just Declare, Just Play Bridge, Bridge 4, Matchpoints, and IMPs.*

Cuebids

Cuebids is a bidding teaching tool. Only teachers who have a valid background check or equivalent safeguarding clearance should use it with young people. Any chat or teaching should be businesslike and bridge related.

Part 2: General Online Safety

1. Principles of Online Safety

All members of WBF, teachers and volunteers are expected to:

- Understand and uphold the principles of online safety, including what constitutes acceptable and unacceptable behaviour when using digital technologies such as social media, apps, gaming consoles, and the internet.
- Use technology respectfully and responsibly, ensuring that all communication and online interactions reflect the values and safeguarding standards of the organisation.
- Take personal responsibility for managing privacy settings and maintaining professionalism online.

2. Compliance and Legal Responsibilities

WBF will:

- Ensure that all online activity complies with relevant legislation, including data protection and safeguarding laws, and aligns with good practice guidance.
- Confirm that any social media or digital service providers used by the organisation (e.g., Facebook, Instagram) comply with relevant safety and privacy standards.

3. Policy Review and Oversight

- Safeguarding policies and procedures relating to online activity will be reviewed **annually** or following any incident or change in legislation.
-

Procedures will cover:

- Reporting online concerns about possible abuse.
- Reporting breaches of conduct, confidentiality, or data protection.
- The WBF Safeguarding Officer will oversee compliance and ensure prompt action is taken in response to concerns.

4. Management of Webpages and Social Media

WBF will ensure that:

- All official webpages and social media profiles are authorised, managed, and regularly reviewed by trained staff or volunteers.
- Parental consent is obtained and verified before using photos or videos of young people for publicity.
 - Additional consent will be required if names are to be published alongside images.
- All interactive content (e.g., forums, comment sections, social media groups) will be moderated by someone trained in safeguarding awareness.
- The WBF Safeguarding Officer will be involved in oversight of all online content and publicity activities.

5. Online Communication and Conduct

- Staff, volunteers, coaches, and teachers must maintain a clear distinction between personal and professional online profiles.
- Personal social media connections (“friending” or “following”) between (unrelated) adults and young people are not permitted.

Online communication with young people must:

- Be professional, transparent, and related to bridge activities. Parents should be copied in to emails.
- Preferably take place in group settings or include another adult (e.g., a parent or co-coach).
- Avoid private or one-to-one messaging.
- Messaging apps such as WhatsApp may be used only for bridge-related communication and should remain businesslike in tone and content.

6. Privacy, Security, and Data Protection

- Personal data, including images and videos of young people, will be stored securely. Images should be deleted from personal devices once processed. Care must be taken to verify parental consent for the photos that are stored.
- Staff and volunteers will receive guidance on recognising phishing, scams, and other online threats.
- Breaches of data security must be reported immediately to the WBF Safeguarding Officer and/or the Data Protection Officer.

7. Reporting and Responding to Online Concerns

- Concerns about online behaviour, suspected abuse, or breaches of conduct must be reported to the WBF Safeguarding Officer without delay.

The organisation will ensure:

- Clear and accessible reporting mechanisms, including anonymous options where appropriate.
- Prompt acknowledgement and action within defined timeframes.
- Accurate record-keeping of all online safeguarding incidents for review and learning.
- Serious concerns or allegations will be managed according to the organisation's **Safeguarding Procedures**.

8. Governance and Continuous Improvement

- This policy will be reviewed annually, or sooner if significant incidents occur or new risks emerge.
- Feedback will be sought from young people, parents, staff, and volunteers to inform updates.
- Regular audits of online platforms and practices will be undertaken to ensure ongoing compliance and safety.

World Bridge Federation • Bridge for Peace

Policy updated: March 2026