



ONLINE SAFETY AND SOCIAL MEDIA POLICY

TABLE OF CONTENTS

<i>Our online safety statement</i>	2
<i>Purpose and scope</i>	2
<i>Understanding online risks</i>	2
<i>Responsibilities</i>	3
<i>Choosing digital platforms</i>	3
<i>Managing our online presence</i>	3
<i>Communicating with children and young people</i>	4
<i>Expectations of adults</i>	4
<i>Expectations of children and young people</i>	4
<i>Expectations of parents and carers</i>	5
<i>Online coaching and video conferencing</i>	5
<i>Photography, filming and livestreaming</i>	5
<i>Mobile phones and devices during sessions</i>	5
<i>Responding to online concerns</i>	6
<i>Information handling</i>	6
<i>Breaches of this policy</i>	6
<i>Appendix 1</i>	7
Acceptable use of IT and Social Media agreement	7
<i>Sources and further guidance</i>	8
<i>Change log</i>	8

OUR ONLINE SAFETY STATEMENT

Safeguarding continues into the online world. Aikido Alliance is committed to providing safe, respectful digital environments and to responding promptly to online behaviour that may place a child at risk or affect the welfare of children involved in Alliance activities.

Online communication can support participation, administration and a sense of community, but it must never weaken the professional boundaries and safeguarding standards expected in person.

PURPOSE AND SCOPE

This policy applies to Aikido Alliance, affiliated associations and clubs, and to instructors, coaches, assistants, helpers, committee members, welfare officers, administrators and other adults acting on their behalf. It also sets expectations for children, young people, parents and carers when using digital technology in connection with Alliance or club activity.

It covers websites, social media, messaging and membership applications, email, mobile phones, video conferencing, livestreaming, online coaching and any other digital service used for Alliance or club purposes. It does not seek to regulate a family's private use of technology except where online conduct creates a safeguarding concern or is directly connected with Alliance activity.

For this policy, a child is anyone under 18 years of age.

POLICY AIMS

- protect children and young people from online abuse, exploitation, bullying and other harm
- set clear professional boundaries for adults who communicate with children
- ensure that digital platforms are selected, configured and used safely
- explain how online concerns must be reported and managed
- protect personal information and use it lawfully and proportionately
- support children and parents to understand safe and acceptable online behaviour

APPLICATION ACROSS THE UNITED KINGDOM

Aikido Alliance applies the same safeguarding principles throughout England, Wales, Scotland and Northern Ireland. Each association and club must also follow the legislation, terminology, statutory guidance and reporting arrangements that apply in the country where the activity takes place or the child is located. Advice should be sought from the Alliance Lead Safeguarding Officer where the correct route is uncertain or a concern crosses national boundaries.

UNDERSTANDING ONLINE RISKS

Online harm may happen entirely online or may form part of abuse occurring offline. Risks relevant to sport include:

- grooming, sexual exploitation, sexual harassment and inappropriate adult-child relationships
- requests for, creation of, or sharing of nude or sexual images, including AI-generated or manipulated images
- online bullying, harassment, threats, discrimination, hate and gender-based abuse
- exposure to pornography, violence, self-harm, eating-disorder content, substance misuse or extremist material
- sharing personal information, location information or images that enable unwanted contact or identification

- fraud, gambling, financial exploitation and pressure to make purchases
- loss of privacy, data breaches, impersonation and misuse of accounts

RESPONSIBILITIES

The Alliance Lead Safeguarding Officer will:

- maintain this policy and advise associations and clubs on significant online safeguarding concerns
- ensure serious, repeated or cross-club concerns are managed under Alliance safeguarding procedures
- review learning from incidents and changes in NSPCC Sport guidance

Club committees and Club Welfare Officers will:

- approve the platforms and accounts used for club business and identify who is authorised to manage them
- ensure adults and families know the communication rules and reporting route
- respond to concerns promptly and refer them in accordance with Alliance procedures
- review access, security and the continuing need for each platform

Everyone covered by this policy is responsible for maintaining professional boundaries, protecting personal information and reporting concerns.

CHOOSING DIGITAL PLATFORMS

Before adopting a social-media channel, messaging service, membership application, livestreaming service or other digital platform, the club must complete and retain a proportionate risk assessment. The assessment should consider:

- the purpose of the platform and whether a less intrusive option would meet the need
- minimum-age rules, privacy controls, moderation, reporting functions and parental controls
- whether one-to-one or encrypted messaging can be disabled or appropriately controlled
- what personal information is collected, where it is stored, who can access it and how long it is retained
- accessibility and the needs of children who may be more vulnerable online
- supplier security, advertising, in-app purchases and the use of children's data for profiling or artificial intelligence

Clubs must not encourage children to open accounts below a platform's minimum age. The NSPCC Sport Digital App Risk Assessment Tool should be used where appropriate.

MANAGING OUR ONLINE PRESENCE

- Public promotional pages must not be used for private communication with children. Private groups must be invitation-only and limited to current, appropriate members.
- At least two trained and authorised adults must have administrative oversight of each account used to engage with children.
- Each administrator should use individual access credentials where the platform permits. Passwords must be strong, stored securely and protected by multi-factor authentication wherever available.
- Access and group membership must be reviewed regularly and removed promptly when a person's role or participation ends.
- Identifying information such as a child's home address, school, telephone number, live location or private travel arrangements must not be posted.

- Content must be accurate, inclusive, professional and consistent with Alliance values and codes of conduct.
- Inappropriate content must be moderated promptly. Relevant safeguarding evidence must first be preserved when it is safe and lawful to do so; suspected child sexual-abuse imagery must never be copied or captured.
- Children, parents and carers must be told who manages the account and how to report a concern.

COMMUNICATING WITH CHILDREN AND YOUNG PEOPLE

- Adults must use only Alliance or club-approved accounts and communication channels for club business.
- Adults must not use personal social-media accounts to contact, “friend” or follow children they know through Alliance activity.
- Routine communication should take place through parents or carers, in an approved group, or on a channel where another authorised adult has oversight.
- Adults must not communicate one-to-one with a child through private or encrypted messaging. Where an operational message must be sent directly to an older child from an approved organisational account, the parent or carer must be informed and another authorised adult must be able to see the communication.
- Messages must be limited to legitimate club matters, written professionally and sent at reasonable, previously agreed times.
- Personal, sexualised, secretive or emotionally dependent communication is prohibited. Adults must not use kisses, sexualised emojis or language that could reasonably blur professional boundaries.
- Club communication must not be moved to disappearing-message functions or accounts that prevent appropriate oversight and record keeping.

If a child contacts an adult through a personal account or begins a private conversation, the adult should respond only as necessary to safeguard the child, move the communication to an approved route and inform the Club Welfare Officer. A disclosure or indication of immediate risk must never be ignored because it arrived through an unapproved channel.

EXPECTATIONS OF ADULTS

- maintain the same professional boundaries online as in person
- use privacy settings but assume that content on a personal public account may be seen by children and families
- never post confidential information or content that could identify a child involved in a safeguarding matter
- complete online-safety training appropriate to the role and understand how to report harmful content
- avoid using a mobile phone while responsible for coaching except for an approved operational, accessibility, health or emergency purpose
- report online concerns in the same way as concerns arising face to face

EXPECTATIONS OF CHILDREN AND YOUNG PEOPLE

Children and young people will be supported to:

- treat others respectfully and follow the club's acceptable-use agreement and codes of conduct
- protect passwords and personal information and use privacy settings
- seek permission before posting images or information about another person
- tell a parent, carer, Club Welfare Officer or another trusted adult if something online causes worry or discomfort
- understand that asking for help will not, by itself, lead to punishment
- use devices during sessions only when permitted or required for an agreed health, disability, communication or emergency need

EXPECTATIONS OF PARENTS AND CARERS

- read and discuss the club's online-safety expectations with their child as required
- keep the club informed of current contact details and any communication or image permissions
- respect the privacy of all children and obtain permission before sharing images that include another child
- avoid posting information that could identify a child's location, routine or private circumstances
- raise concerns with the Club Welfare Officer rather than confronting a child or adult or conducting their own investigation
- support the platform-age requirements and safety arrangements adopted by the club

ONLINE COACHING AND VIDEO CONFERENCING

Before delivering an online activity, the club must assess the safeguarding and physical-safety risks. The following controls apply:

- the platform and session must be approved by the club and invitations sent privately to participants and parents or carers
- sessions must be protected by appropriate security settings; meeting links must not be published openly
- at least two authorised adults must have oversight of a group session and one-to-one online coaching of a child is not permitted
- a parent or carer must know when the child is taking part and should be present or readily available as appropriate to the child's age and needs
- participants and adults should join from a suitable shared or neutral space and wear appropriate clothing
- private chat, screen sharing and recording must be disabled or controlled by the organiser
- a session must not be recorded without prior approval and the permissions required under the AA Photography and Filming Policy
- the organiser must explain how to report a concern and must end the session if safety cannot be maintained

PHOTOGRAPHY, FILMING AND LIVESTREAMING

All photography, filming, recording, publication and livestreaming must comply with the AA Photography and Filming Policy. In particular, only authorised people and approved devices may be used for an agreed purpose; the required consent must be recorded; the wishes of the child must be respected; and images must not be taken in toilets, changing areas or first-aid areas. Children should not normally be named or tagged in public posts.

MOBILE PHONES AND DEVICES DURING SESSIONS

Mobile phones and other devices should not distract from safe coaching or participation. Coaches and other adults must not use them during a session except for an approved operational, accessibility, health or emergency purpose. Any authorised photography or filming must follow the Alliance's separate policy.

- Children and parents must be told how emergency contact can be made while a session is taking place.
- Children should keep devices stored safely unless use has been agreed for a health, disability, communication or emergency need.
- Phones, tablets, cameras and other recording devices must not be used in toilets or changing areas.

RESPONDING TO ONLINE CONCERNS

Online safeguarding concerns must be managed under the AA Responding to Concerns and Allegations guidance. If a child is in immediate danger or a crime is in progress, call 999. Otherwise, report the concern promptly to the Club Welfare Officer, who will seek advice or make referrals through the appropriate national and local safeguarding arrangements.

- Listen, remain calm, take the child seriously and explain that the concern will be shared only with people who need to help.
- Do not investigate, confront the person concerned, make assumptions or ask leading questions.
- Make a factual written record of what was seen, heard or reported, including dates, times, account names, usernames and web addresses where available.
- Preserve relevant messages and posts when it is safe and lawful to do so, but do not circulate them. Harmful public content may be removed after appropriate information has been retained and safeguarding advice obtained.
- Do not ask a child to send or display a nude or sexual image. Do not download, forward, copy, print or screenshot suspected child sexual-abuse material, and do not search the child's device.
- Report sexual exploitation or grooming concerns through safeguarding procedures and, where appropriate, to the police or CEOP. Suspected online child sexual-abuse imagery may also be reported to the Internet Watch Foundation.
- Online bullying must be managed in accordance with the AA Anti-Bullying Policy as well as safeguarding procedures where harm or risk of harm is present.

A child who reports that they have created or shared an image, or who has been pressured or exploited online, must be treated first as a child who may need safeguarding and support. They must not be automatically blamed or sanctioned for seeking help.

INFORMATION HANDLING

Personal information must be handled in accordance with applicable UK data-protection law, including the UK GDPR and Data Protection Act 2018 as amended. Clubs must use an appropriate lawful basis, collect only information that is needed, provide suitable privacy information, restrict access, use secure storage and retain information only for as long as required.

- Safeguarding information must be shared on a need-to-know basis and retained under the Alliance's safeguarding record-retention arrangements.
- Routine messages and account content must not be kept indefinitely. Relevant safeguarding evidence must not be deleted merely to avoid scrutiny.
- Suspected loss, unauthorised disclosure or misuse of personal information must be reported promptly through the applicable data-breach procedure.
- Children's information must not be entered into artificial-intelligence tools or used for profiling without prior organisational approval and an appropriate data-protection and safeguarding assessment.

BREACHES OF THIS POLICY

A breach may result in removal of account access, moderation of content, action under a code of conduct or disciplinary procedure, suspension from duties or participation, referral to statutory agencies, or other proportionate action. Safeguarding needs and immediate safety take priority.

Children should be helped to understand and repair the consequences of inappropriate online behaviour. Disciplinary action must not discourage a child from reporting abuse, coercion, bullying or a mistake that may place them at risk.

APPENDIX 1

ACCEPTABLE USE OF IT AND SOCIAL MEDIA AGREEMENT

This agreement is intended for clubs to adapt to the ages and communication needs of their members. Parents and carers should discuss it with their child.

As a child or young person taking part in this club, I will:

- be respectful and not use digital technology to bully, threaten, humiliate, discriminate against or deliberately upset another person
- use only the club communication channels agreed with my parent or carer
- keep my passwords private and protect personal information such as my address, telephone number, school and live location
- ask permission before taking, posting or sharing an image, recording or personal information about someone else
- not create, request, send or share nude or sexual images or messages
- tell a parent, carer, Club Welfare Officer or another trusted adult if I receive unwanted contact or see something that worries or pressures me
- not arrange to meet someone known only online without telling my parent or carer and putting appropriate safeguards in place
- follow the club's rules about mobile phones and devices during sessions
- understand that conduct connected with the club may be addressed where it affects another member, creates a safeguarding concern or disrupts safe club activity

The club will:

- explain who manages its online accounts and how concerns can be reported
- respond to concerns fairly and under the Alliance's safeguarding and anti-bullying procedures
- support children who ask for help and not automatically punish them for reporting an online concern

SOURCES AND FURTHER GUIDANCE

- [NSPCC Sport Online safety and social media](#)
- [NSPCC Sport Online safety policy template](#)
- [NSPCC Sport Digital App Risk Assessment Tool](#)
- [NSPCC Sport Photography and filming in sports and activities](#)
- [NSPCC Learning Online safety](#)
- [CEOP Safety Centre](#)
- [Internet Watch Foundation Report online child sexual abuse](#)
- [Childline Report Remove](#)
- [Information Commissioner's Office](#)

CHANGE LOG

Date and version	Details
July 2024 V2	Policy renamed from E-Safety and content refreshed using the then-current sector template.
September 2026 V3	Full review against current NSPCC Sport guidance. Updated communication boundaries, platform security, online risk assessment, AI and image risks, response procedures, data protection, UK-wide application and acceptable-use wording. Earlier sector terminology updated to NSPCC Sport.