



International  
Olympic  
Committee

# ONLINE ABUSE AND SPORT

## CONTEXT, DEFINITION, MANIFESTATIONS, IMPACT AND RESPONSE





Developed by the IOC Safe Sport Unit, Health Medicine and Science Dept, IOC.

With special thanks to:

Emma Kavanagh, Reader in Sport Psychology at Loughborough University

Kim Barker, Professor of Law at Lincoln Law School

Daniel Lock, Professor of Sport and Social Identity, Loughborough University London

and Tine Vertommen, Researcher Safeguarding in Sport, Thomas More University of Applied Sciences

For more information please contact [safesport@olympic.org](mailto:safesport@olympic.org)



# EXECUTIVE SUMMARY

**This document highlights key reflections and considerations following the IOC's implementation of measures to prevent, detect and respond to online abuse during the Olympic Games. It frames online abuse as a form of violence that produces real, embodied harm; explains core dynamics (triggers, intersectionality, online-offline spread); summarises Paris 2024 and Milano-Cortina 2026 findings; and sets out recommended practices for sport organisations.**

\*These considerations are intended to support sport organisations in strengthening their safeguarding frameworks. They are general in nature, and any actions or measures taken pursuant to this document should be assessed in light of each organisation's specific circumstances and carried out in accordance with applicable law and regulatory requirements, and relevant internal policies and procedures.

# 01



## KEY RECOMMENDATIONS

Sport organisations are encouraged to adopt a holistic, multidisciplinary safeguarding approach to address online abuse that integrates technology, clear policies, and comprehensive reporting and support mechanisms.

### GENERAL RECOMMENDATIONS

#### Prioritise Digital Literacy

**Mandatory digital safeguarding training** should be provided as part of general safeguarding training, covering how to recognise abuse (such as deepfakes or doxxing), understand and mitigate risks, secure devices, and follow clear reporting protocols.

#### Develop Guidance

Organisations are encouraged to brief participants through guidance **within safeguarding policies**. This can be used to set transparent expectations around online behaviours and integrate online environments into safeguarding processes and disciplinary procedures.

#### Share Learning

Collaborate across the Olympic Movement (IFs, NOCs) to coordinate messaging and **align policies and good practices while ensuring confidentiality**.



## USE OF CYBER MONITORING & PROTECTION SERVICES

### Prevention and Governance

#### Integrated Response

Detection/prevention/response to online abuse should be **embedded into broader safeguarding frameworks** and connected to athlete well-being, not just labelled as a communications problem.

#### Embed Support

Establish a "We're here for you" culture, emphasising that monitoring exists to help support participant safety. Ensure welfare support is available, including **aftercare and short-term monitoring** post event.

### Response and Ethical Technology Use

#### Utilise Automated Monitoring Responsibly

While AI and detection tools are beneficial, organisations should **avoid overreliance** on automated systems. Human review remains **essential** to verify incidents, maintain a critical lens on algorithmic bias, and ensure accurate triage and referral.

#### Ensure Ethical Boundaries

Cyber Protection services should maintain participant trust through use of ethical, transparent monitoring tools with human oversight, bias checks, legal compliance, and clear separation from research use.

### Collaboration

#### Build External Partnerships<sup>1</sup>

Organisations are encouraged to establish early contact and **direct, confidential, reporting lines with social media platforms**.

#### Formalise Liaisons

**Formalise accelerated cooperation mechanisms with relevant law enforcement authorities and security agencies** to enable, where legally permitted, the timely adoption of appropriate measures, as well as the preservation and transmission of evidence (such as screen captures, metadata and account IDs) to competent authorities when applicable criminal thresholds are met.

“Online presence is no longer optional for Olympians, it’s a fundamental part of how we connect with fans, represent our values, and sustain our careers through sponsorships and partnerships. But with that visibility comes vulnerability. Online abuse can have a real emotional and psychological impact, especially during major events when athletes are already under immense pressure.”

**Bruno Fratus**, IOC Mental Health Ambassador



# 02

## BACKGROUND



Safeguarding and the protection of mental health and well-being are foundational commitments of the IOC. Ensuring that sport is a safe, respectful environment for everyone is central to the IOC's approach to safeguarding, which seeks to prevent all forms of interpersonal violence, respond appropriately when concerns arise and to protect the dignity and well-being of all participants.

Digital platforms play an essential role in modern sport, enabling athletes to build their personal image, engage with fans, attract sponsors, and manage their careers. At the same time, these platforms expose individuals and organisations to new and evolving forms of harm. Experience from the Olympic Games Paris 2024 and Milano Cortina 2026 reaffirmed that online abuse is not an isolated or episodic issue, but a persistent and structural risk that is inseparable from modern sport.

Major sporting events can act as trigger moments for online abuse.<sup>2</sup> Heightened visibility, emotional investment, performance scrutiny, and broader societal tensions – relating to nationality, politics, gender, race, or social inequality – can spill into digital spaces. Abuse may target individual athletes, teams, officials, organisations, or entire sporting communities, and can escalate rapidly in scale and intensity.

While legal frameworks and platform moderation mechanisms remain important, they are not sufficient on their own. A significant proportion of harmful online behaviour falls into the category of “lawful but awful”: content that does not meet thresholds for platform removal or other remedies, such as criminal prosecution or related protective measures, yet can cause real and lasting psychological, reputational, and economic harm. This underscores the need for sport-specific understanding, prevention strategies, enhanced education and digital literacy and response mechanisms.

Against this backdrop, strengthening knowledge of online abuse in sport is essential to enhance safeguarding and mental health protections in digital environments. Drawing on expert input and learnings from the Olympic Games Paris 2024 and Milano Cortina 2026, this document intends to support sport organisations to reflect on risk, clarify responsibilities, and develop more effective, coordinated approaches to prevention, protection, and response.

# 03



## UNDERSTANDING ONLINE ABUSE IN SPORT



**“Online abuse adds to the external noise that’s not always conducive to performing at one’s best, taking up energy and emotional bandwidth. It’s hard navigating how to or to not respond, especially competing at the Olympics can be an overwhelming experience at times.”**

**Camille Cheng**, IOC Mental Health Ambassador

Online abuse refers to the use of internet-connected technologies – such as smartphones, computers, and social media platforms – to harm, exploit, intimidate, or threaten individuals or groups. These behaviours may be overt or subtle, isolated or sustained, and can cause psychological, emotional, physical, sexual, reputational, or economic harm.<sup>3,4</sup>

As an overarching concept, online abuse encompasses a wide range of actions, including but not limited to: harassment and bullying; unwanted explicit or sexualised content; stalking or tracking behaviours; coercion or sextortion; doxxing; impersonation; image-based abuse; the creation or distribution of deepfakes; AI and synthetic media; misinformation and disinformation; and coordinated or organised “pile-on” campaigns. Abuse may be perpetrated by individuals or groups, known or unknown to the target, and can occur over short periods or persist for months or years.

Online abuse in sport affects far more than elite or high-profile athletes. It can target anyone within the sporting environment, including coaches, officials, volunteers, staff, fans, and organisations or their representatives. Abuse may occur at individual, collective, or systemic levels, and can intersect with in-person abuse, amplifying its impact and complexity.

Risk and severity are heightened when online abuse intersects with identity-based discrimination, such as gender, race, ethnicity, religion, sexuality, or disability. Individuals with intersecting identities often experience more frequent, targeted, and severe abuse, resulting in compounded harm and longer-lasting effects.<sup>5</sup>

Emerging evidence highlights the scale and evolving nature of the issue. For example, during the FIFA Women’s World Cup 2023, one in five players received targeted discriminatory, abusive, or threatening messages, with a significant proportion classified as sexist, sexual, or homophobic abuse. Other research points to the growing role of digital technologies in facilitating stalking, psychological abuse, cases of sextortion and child sexual exploitation, including a marked rise in elite women athletes reporting stalking with online components.<sup>6</sup>

Although mediated through technology, online abuse does not remain confined to digital spaces. Its impacts extend into athletes’ personal lives, relationships, families, and physical environments, shaping behaviour, well-being, sense of safety, and participation in sport. Understanding these dynamics is critical for developing proportionate, trauma-informed, and effective safeguarding responses.

# TYPES AND EXAMPLES OF ONLINE ABUSE IN SPORT

The following presents a classification of common forms of online abuse in sport, with illustrative examples, to support shared understanding and practical application. While this highlights the breadth of potential harms, it is not exhaustive; abuse types are rapidly evolving and becoming more sophisticated in nature.

## NOTES:

- Types of online abuse are listed alphabetically within thematic groupings and do not indicate relative importance or prevalence.
- Examples are non-exhaustive and provided for illustrative purposes.
- Types of abuse can happen in isolation and/or co-occur, can be multi-modal and be amplified by intersectional identities (or presumed identities).
- Abuse can be perpetrated by those known to recipients and those unknown.
- Abuse is often persistent, repeated, and can involve several types. Digital hostility/teasing and name calling abuse often occurs in volume, without meeting the threshold of other categories of abuse.
- The rapid advancement of artificial intelligence has significantly increased the scale, sophistication, and impact of online abuse in sport. This includes the use of AI-generated synthetic media (such as deepfakes), automated harassment campaigns, and impersonation through fake accounts.
- Not all forms of abuse will be legally actionable, yet this does not reduce their potential harmful effects.



## INTERPERSONAL VIOLENCE

### Body Shaming

Mocking or criticising an individual's body shape, size, or appearance.

#### Example

Negative comments about an athlete's weight after an injury.

### Digital Hostility

Aggressive, non-specific remarks targeting individuals or groups. May be individual or numerous posts.

#### Example

Posting a meme of an athlete's mistake followed by belittling or mocking comments.

### Performance Related

Content that targets a person, group and or event and includes reference to performance.

#### Example

Sending hostile messages to a referee due to a decision made while officiating a performance.

### Cyber-Bullying

Repeated peer-to-peer online harassment or humiliation (often by those known to target).

#### Example

Persistent hostile messages between teammates in a group chat. Can single out individuals as particular targets.

### Online Grooming

Online grooming refers to a pattern of deliberate conduct in which a person uses digital technologies to establish contact, develop a relationship, and cultivate trust, dependency, or influence over another person or group, for the purpose of facilitating manipulation, coercion, exploitation, or control.

#### Example

A coach using technology to groom a minor athlete. Abuse may occur across online and physical settings concurrently.

### Trolling

The act(s) of posting provocative, inflammatory, or offensive content online to intentionally upset or antagonise targets often for one's own amusement or to create conflict, and often as sustained or repeat attacks.

#### Example

Anonymous accounts repeatedly criticising a player to provoke a reaction.

## THREATS, SURVEILLANCE, AND COERCIVE BEHAVIOURS

### Coercive or Controlling Behaviour

Use of technology to monitor, intimidate, or control another person.

#### Example

A coach persistently messages an athlete to exert control; this can extend beyond the athlete's sporting performance to other areas of their life.

### Direct or Indirect Threats

Messages expressing intent to cause physical, psychological or other forms of harm against individuals, groups and/or organisations.

#### Example

An athlete receives death and rape threats after a match. The comment also targeted their family members.

### Pile-Ons/Coordinated Harassment Campaigns

Coordinated online attacks inciting and/or involving many users, or AI for speed and volume across multiple platforms simultaneously.

#### Example

Numerous users repost a video of a foul with abusive captions. Using social media to incite collective abuse of an athlete during a live event.

### Sextortion

Threatening to share an intimate image/video/audio (real or synthetic) of a person, without the consent of the person shown, unless payment is received.

#### Example

An athlete is bribed and threatened that AI generated material (e.g., image, audio, video) of them will be shared unless they pay money to prevent that happening.

### Stalking

Repeated use of technology to follow, communicate, harass or target an individual or team, often with repeated and persistent communications that escalate in frequency.

#### Example

A fan repeatedly messages an athlete and later appears at their events.



## PRIVACY AND IMAGE-BASED OFFENCES

### Cyber-Flashing/Unsolicited Explicit Content

Sending sexually explicit images or videos without consent.

#### Example

Sending an athlete an unsolicited explicit photo.

### Doxxing

Publishing private or identifying information to facilitate harassment.

#### Example

Unauthorised release of a targeted official's home address online, leading to threats of injury or death.

### Synthetic Media e.g., Deepfakes/Voice Cloning

AI-generated or manipulated images, audio or video content that resembles existing persons, objects places, entities or events, such that they would appear, falsely, to a person to be authentic or truthful.

#### Example

Fabricating a video of a coach or athlete making inflammatory remarks. Used to humiliate or deceive, or impersonate.

### Hijacked Communications, Impersonation or Fake Accounts

Unauthorised accounts, fake identities or profiles; impersonation on chats; image impersonations; fake webpages; catfishing; impersonation by AI personas.

#### Example

A false message posted from a hijacked account or fake social media accounts sharing athlete's imagery and content, or false personas that appear to be running genuine accounts through impersonation.

## REPUTATIONAL AND INTEGRITY-RELATED ABUSE

### False Reporting/Misinformation/Disinformation

Spreading false allegations or fabricated information to damage reputation.

#### Example

Circulating a false report accusing an athlete of doping. Fabricated AI-generated footage falsely reporting heightened security threats at a major sporting event as part of a disinformation campaign.

### Integrity-Related Abuse

Accusations undermining an individuals or organisations reputation, honesty and/or sporting integrity including allegations of doping, match-fixing or use of performance enhancing drugs.

#### Example

Posting comments that an athlete “must have cheated.”



## DISCRIMINATORY AND IDENTITY-BASED ABUSE

### Discriminatory/Intersectional Abuse

Abuse based on actual or perceived identity traits such as race, gender, sexuality, religion, nationality, or disability.

See subtypes below.

NB: Where multiple examples occur simultaneously or in combination, they have increased impacts.

#### Ableism

Derogatory or mocking comments about disability.

#### Example

Using slurs referencing disability to insult an athlete. Using ableist language linked to disability to target a non-disabled person.

#### Racism/Xenophobia/ National Identity

Abuse based on (perceived) race, ethnicity, religion, or nationality.

#### Example

An individual is targeted, and messages include racist language.

#### Sexism/Misogyny

Hostile or sexualised comments based on gender.

#### Example

Sexualised abuse targeting women athletes.

#### Transphobia/ Homophobia

Derogatory comments toward LGBTQ+ individuals.

#### Example

Posts using homophobic language to demean a performer or as an intended slur.

# 04

## IMPLEMENTING A CYBER-ABUSE MONITORING SERVICE

**“In snow sports, we are lucky to be part of a community that is generally very supportive and respectful. The vast majority of online interactions with athletes and key stakeholders are positive, but “vast majority” is not enough when it comes to online abuse and intimidation. We have a zero-tolerance policy, which is why FIS is really pleased to support and collaborate with the IOC’s proactive and protective approach, at the Winter Olympics and beyond.”**

Sarah Fussek, FIS Integrity Director

### LEARNINGS FROM THE OLYMPIC GAMES PARIS 2024 AND MILANO CORTINA 2026

The IOC’s **Cyber-Abuse Protection Service (CAPS)** was first deployed at the Olympic Games Paris 2024 and was the largest initiative ever commissioned in sport to *monitor and protect participants* from online abuse. Following its successful deployment at Paris 2024, CAPS was extended to the Olympic Winter Games Milano Cortina 2026.

Its primary goals were to scan social media for abusive content targeting athletes, teams, coaches and officials; categorise and triage incidents by severity; rapidly notify IOC security of any fixated threats; and expedite takedowns of violative content. The system combined AI tools with human analysts to “build a proactive net around athletes,” scanning public posts across X (formerly Twitter), Instagram, Facebook and TikTok.

At Paris 2024, approximately 20,000 social media accounts (over 10,000 athletes and account handles for teams, coaches, officials and IOC stakeholders) were covered. At Milano Cortina 2026, over 6,000 accounts were monitored and language coverage expanded from 45 languages at Paris to 56 at Milano Cortina.

### HOW THE SYSTEM WORKED

CAPS is fully integrated into the IOC’s Games-time Safeguarding Framework. The IOC Safe Sport Unit coordinated the service alongside NOC and IF Safeguarding Officers to ensure timely and trauma informed response to flagged cases. Operations ran 24/7, combining automated AI powered monitoring with human review. Content verified as abusive were reported to platforms, while summaries were shared with the IOC Safe Sport Unit to support affected parties. Those who experienced severe abuse were automatically offered psychological and well-being support in line with the event Mental Health Emergency Action Plan. The provision of the IOC’s Mentally Fit helpline ensured continuous (24/7) access to care. Where content indicated imminent threats, IOC security and host authorities were alerted in real time, and in severe cases forensic tools were used to support referral to law enforcement authorities.

### WHAT WERE THE RESULTS?

Across the two Games, CAPS:

- analysed 4.3 million posts and comments, directed at over 26,000 athletes’ and officials’ social media handles, in real time and in 45 languages at Paris 2024, expanded to 56 at Milano Cortina 2026;
- flagged ~242,000 posts and comments as potentially abusive via AI (152,000 at Paris; ~90,000 at Milano Cortina);
- verified ~24,700 posts and comments as abusive (10,200 at Paris; 14,500 at Milano Cortina), and reported these to the platforms; and
- detected ~18,900 unique accounts sending abusive messages (8,900 at Paris; ~10,000 at Milano Cortina).

**“Over the past Olympic Games I have seen more and more effort from the IOC in demonstrating what systems are in place to protect athletes online, and I hope that this continues to strengthen.”**

Camille Cheng, IOC Mental Health Ambassador

**“Seeing the IOC take such a proactive stance to protect athletes during Paris 2024, sends a powerful message: that we are not alone out there. Knowing there’s a system identifying and holding aggressors accountable not only ensures safety but also makes us feel valued and supported. It’s an example of true teamwork, the kind that extends beyond competition, showing that the Olympic Movement stands with its athletes both on and off the field.”**

Bruno Fratus, IOC Mental Health Ambassador

## WHAT DID WE LEARN?

### Online abuse reflects gender dynamics and intensifies around visibility, emotion and identity

Across both Games, abusive content frequently co-occurred across multiple categories, with overlapping and multi-faceted forms of abuse compounding the experience for those directly targeted. Abuse triggered by an athlete's identity tended to be more sustained than abuse triggered by an athlete's conduct or provocation, which spikes sharply but fades more quickly. Sexist and sexualised comments remained among the most frequent forms, with women disproportionately being the recipients of sexually abusive content. Male athletes received a higher overall volume of abuse, likely reflecting greater visibility and message traffic in men's team sports. General harassment, profanity, and references to violence or threats were widespread. Abuse volumes peaked around high-visibility moments - Opening and Closing Ceremonies, medal events, and high-profile or contested outcomes.

### Exposure is driven by prominence and platform dynamics and “takedown” is no longer the right metric

Targets of abuse were broad, with no sport immune. Athletes and teams in larger-fanbase sports, as well as high-profile individuals with substantial followings, faced disproportionate exposure. Platform differences were pronounced: a single platform (X) dominated abuse volumes at both Games despite holding a minority of monitored accounts, reflecting its role in real-time event commentary. Abuse on image- and video-led platforms was more retrospective. A material shift between the two Games was the move by at least one major platform toward de-amplification rather than removal as the default response to non-illegal abuse. This means takedown rate alone is no longer an adequate measure of platform response – action rate, combining takedowns and visibility limits, better reflects what is actually happening to abusive content. Action rates improved between the two Games, and serious cases continued to see higher removal success on escalation, but enforcement across platforms remains inconsistent.

### Monitoring adds clear value but may be insufficient without human oversight and wider safeguarding measures

CAPS demonstrated clear value across both Games. Its AI-human hybrid model identified tens of thousands of verified abusive posts, generated actionable intelligence, and contributed to hundreds of account suspensions and legal referrals. Centralised reporting removed the burden from athletes, allowing them to focus on performance. However, limitations remain: a high proportion of abusive content stays visible even where action is taken; Legal escalation is also challenging, due to differences in criminal law thresholds and the cross-border nature of online abuse, which complicates jurisdiction and enforcement. Automated systems alone are insufficient, as AI filters can miss context, generate false positives, or reproduce bias. Human review remains essential for accurate triage and culturally informed responses, especially as the language and expression of abusive content is constantly evolving.

Two emerging risks became more visible at Milano Cortina: sextortion attempts targeting younger athletes, and AI-manipulated imagery and impersonation. These point to a current reality where monitoring alone cannot adequately protect athletes and others in their entourage from online threats. Proactive education – particularly for those encountering Olympic-scale audiences for the first time – must be embedded into athlete-facing pathways and into arrival and onboarding moments, with content that addresses synthetic media, sextortion and the realities of de-amplification alongside traditional abuse awareness.

Overall, CAPS validated the importance of embedding monitoring technology within a broader safeguarding and mental health ecosystem. Effective protection from online abuse requires a combined approach that integrates monitoring with education, real-time welfare support, and post-event care, rather than relying on technology in isolation.



# 05

## CORE RECOMMENDATIONS FOR SPORTS ORGANISATIONS



Preventing and responding to online abuse requires holistic, multi-layered action involving sport organisations, athletes, federations, platforms, and authorities. Unilateral or isolated measures are unlikely to be effective and technological and investigative solutions can be costly. Sport organisations should therefore implement integrated safeguarding arrangements that, where applicable uphold duty of care, reduce risk, and provide timely, appropriate support across digital and physical environments.

### 5.1 GOVERNANCE AND POLICY

#### Embed Online Abuse within Safeguarding Frameworks

Online abuse should be explicitly recognised as part of an organisation's broader safeguarding responsibilities and treated as a well-being issue, not a purely technical one. Safeguarding frameworks should include measures to address online harms across policies, risk assessments, reporting routes, and response procedures before, during, and after major sporting events.

#### Develop Clear Guidance for Behaviours Online

Organisations should develop clear guidance for online communication as part of their safeguarding strategies. These should define acceptable online behaviour; set standards for social media use; outline protocols for capturing, sharing, or generating images, video, and synthetic content; and address online communications involving young people.<sup>7</sup> Reliance solely on platform codes of conduct should be avoided, as they are not designed with safeguarding as a priority.

#### Designate Leadership and Accountability

Clear accountability mechanisms should be established, including the designation of safeguarding leads responsible for reporting, escalation, and coordination with internal and external partners.

### 5.2 EDUCATION AND CULTURE

#### Deliver Digital Safeguarding and Literacy Education

Education is a cornerstone of prevention. Organisations should promote age and culturally appropriate, mandatory digital safeguarding and literacy<sup>8</sup> training for athletes, staff, coaches, volunteers, and officials. Training should help participants recognise harmful behaviours, understand rights and responsibilities, and know how to respond to issues such as online hostility, stalking, doxxing, deepfakes, impersonation, sextortion, image-based abuse, deepfakes, and other AI-manipulated content.

Particular attention should be given to participants encountering large-scale public audiences for the first time, who may be unprepared for the volume, speed, and intensity of attention that accompanies high-visibility competition – and to younger participants, where evidence of sextortion attempts and synthetic media targeting is increasing. It should also cover device security, privacy settings, cybersecurity awareness, and the protection of sensitive data.<sup>9</sup> Education should include tools to better support pro-social online interactions and to manage the additional cognitive load of online interactions. In doing so it can help users to leverage the benefits of online interactions and to be aware of and mitigate risks and disbenefits.

## 5.2 EDUCATION AND CULTURE CONTINUED

### Build Awareness of Support Pathways

Education should ensure participants understand reporting routes and know key contacts within teams, organisations, and support networks, enabling early intervention and timely assistance.

### Foster a Positive Digital Culture

A positive digital culture, including pro-social interactions, should be actively encouraged at all levels of sport, including among fans. Digital citizenship initiatives – such as awareness campaigns or athlete-led messaging – can promote empathy, respectful communication, and accountability, reinforcing that online spaces are an extension of the sporting environment.

## 5.3 MONITORING AND RESPONSE SYSTEMS

### Establish Clear Reporting Systems

Organisations should implement and clearly communicate accessible reporting mechanisms (e.g. safeguarding inboxes, hotlines, or online chat functions). Athletes, teams, and other participants should be proactively informed about how monitoring and reporting processes work, what protections are in place, and how to report suspected or experienced online abuse. Reporting pathways should be clearly linked to welfare, security, and safeguarding support.

### Use AI Monitoring and Detection Tools Appropriately

Where feasible, organisations should consider the use of monitoring and threat-detection tools during Major Sporting Events and other high-risk periods. Monitoring should cover public-facing channels comprehensively and, where feasible, offer support for private messages. Any automated or AI-based tools must be paired with human oversight and regularly reviewed for bias, false positives, and contextual limitations. The use of technology should be ethical and transparent compliant with applicable data protection laws, and a defined separation between operational protection and any research or analytical use of data.

Organisations should also recognise that platform responses to abusive content increasingly extend beyond removal to include visibility limits and de-amplification. Effective measurement and reporting should therefore reflect *action rate* – the combined proportion of content that is removed, restricted,

or de-amplified – rather than relying on takedown rate alone, which no longer adequately captures platform response. This is particularly relevant when communicating outcomes to participants, where a narrow focus on takedown can understate the protective effect of platform action.

### Standardise Response Protocols

Responses to online abuse should follow a consistent protocol: verify, document, report, and support. Impacted individuals should be advised on practical steps such as muting or blocking accounts, preserving evidence, and accessing support. Organisations should establish fast-track escalation pathways with internal security teams and law enforcement authorities competent in the relevant jurisdiction where behaviour reaches criminal thresholds or presents imminent risk, recognising that enforcement may be more complicated where the perpetrator is outside that jurisdiction or where laws differ.

### Embed Welfare Support

Welfare is the protection and promotion of a person's safety, health and well-being through care, support and safeguarding measures. Welfare should be embedded throughout monitoring and response systems, reinforcing that these measures exist to protect safety and performance rather than to police behaviour. Organisations should plan for follow-up care and continued monitoring after events, particularly for individuals who have been heavily targeted. Where appropriate, aggregated insights from monitoring can be used to inform targeted education, briefings, and preventive interventions for athletes, teams and staff.

## 5.4 COLLABORATION AND ENFORCEMENT

### Collaborate Across the Sport System

Sport organisations should work closely with federations, professional bodies, and event organisers to coordinate messaging, share good practices, and align policies.

### Engage Social Media Platforms Early

Early engagement with platform representatives ahead of major events can support faster reporting and removal of abusive content. Sharing aggregated findings with platforms can help drive more consistent enforcement of community standards.

### Formalise Law Enforcement and Security Links

Clear protocols and accelerated cooperation mechanisms with relevant law enforcement authorities and security agencies should be established for cases involving imminent threats. This ensures evidence can be rapidly transferred, in accordance with applicable laws, when legal thresholds are met and signals that abuse toward athletes carries real consequences.

# 06

## CONCLUSION & CALL TO ACTION

The digital environment is now an **inseparable part of the sporting environment**, meaning that what happens online directly reinforces, amplifies, or triggers harm offline. Online abuse is unrelenting, affecting all individuals in sport, from elite athletes and officials to volunteers, and substantially increases around major sporting events. The impact of online abuse is profound, that can cause real and lasting physical, psychological, reputational, and economic harm.

While online abuse cannot be fully eliminated, its risks and harms can be meaningfully reduced through proactive strategy. Crucially, sport organisations should recognise that cyber protection systems alone are insufficient. The so-called 'lawful but awful' nature of online abuse means that content may not meet legal thresholds for removal or other remedies, such as criminal prosecution or related protective measures, yet can cause significant psychological and social damage.

Learnings from initiatives like the IOC's Cyber-Abuse Protection Service (CAPS) at the Olympic Games validate that a proactive abuse-monitoring service can **substantially enhance participant safety** when coupled with existing safeguarding and mental health frameworks. Sporting bodies should consider adopting a **multidisciplinary approach** that integrates technology, welfare support, clear policies, and comprehensive cross-sector coordination to protect participants both online and off.





# APPENDICES

## List of Abbreviations

|     |                                 |
|-----|---------------------------------|
| AI  | Artificial Intelligence         |
| IF  | International Federation        |
| IOC | International Olympic Committee |
| MSE | Major Sporting Event            |
| NOC | National Olympic Committee      |

## GLOSSARY OF KEY TERMS

This glossary provides definitions of key terms used throughout the guidance. The aim is to ensure clarity and consistency in how concepts related to online abuse, safeguarding, and digital well-being are understood. The terms are explained in plain language and may differ from formal legal or technical definitions, reflecting their use in the context of safeguarding and major sporting events.

### DEFINITION

#### Artificial Intelligence (AI) Moderation Tools

Technological systems that use machine learning or algorithmic processes to automatically identify and flag potentially harmful online content.

### DEFINITION

#### Community Guidelines

Rules set by organisations or digital platforms outlining acceptable online behaviour and defining what types of content or interactions are not permitted.

### DEFINITION

#### Compounded Harm

Profound and longer-lasting negative impact experienced by individuals targeted by online abuse, particularly when that abuse is rooted in intersectional discrimination and occurs in multiplicity, and/or occurs multi-modally.

### DEFINITION

#### Content Moderation

The process used by social media platforms and organisations to detect, review, and remove harmful or inappropriate content according to their policies or community guidelines.

### DEFINITION

#### Cyber-Abuse Protection Service (CAPS)

The IOC initiative, combining AI tools and human analysts, was commissioned to monitor, detect, and respond to online abuse targeting participants (including athletes, teams, coaches and officials) during the Paris 2024 and Milano Cortina 2026 Games and other Major Sporting Events (MSEs).

### DEFINITION

#### Cyber-Flashing/Unsolicited Explicit Content

The electronic sending of photographs or film of genitals, which is likely a criminal offence in some countries.

### DEFINITION

#### Deepfakes/Voice Cloning

AI-generated synthetic media (video or audio) used to spread misinformation, create embarrassment, or incite conflict.

### DEFINITION

#### Digital Safeguarding

Extending safeguarding principles into online spaces. It includes preventing and responding to online abuse, protecting personal information, and promoting responsible digital engagement among athletes, staff, and fans.

### DEFINITION

#### Doxxing

Sharing private, identifying personal details (such as address, financial records, or phone number) for the purpose of harassment or exploitation.

### DEFINITION

#### Interpersonal Violence

Interpersonal violence involves the intentional use of physical force or power against other persons by an individual or small group of individuals. It can occur online, be perpetrated by different actors and take different forms.

**i** DEFINITION**Intersectional Discrimination/Abuse**

Hateful or abusive language based on multiple characteristics including (but not limited to) gender, race, sexual orientation, religion, or disability. This type of abuse results in an elevated risk of being a target and often produces profound and compounded harm.

**i** DEFINITION**Lawful but Awful**

Refers to online attacks or content that do not meet thresholds for removal or other remedies, such as criminal prosecution in a particular jurisdiction, but which still can cause substantial, real, and lasting harm and impact on those targeted.

**i** DEFINITION**Online Abuse**

The use of internet-connected technologies, such as smartphones, computers, or social media platforms, to harm, exploit, intimidate, or threaten individuals or groups. It encompasses a wide range of communication methods and behaviours that can be aggressive, manipulative, exploitative, or threatening, and may be intended to control others or cause fear, psychological distress, or feelings of inferiority.

**i** DEFINITION**Online Harm**

A broader term that includes both illegal and non-illegal behaviours that negatively affect an individual's well-being, reputation, or sense of safety. Harmful content may not break the law but can still cause real psychological or social damage.

**i** DEFINITION**Platform Action Rate**

The combined proportion of content that is removed, restricted, or de-amplified.

**i** DEFINITION**Protocol**

An agreed set of guidelines or standards that govern how to respond in a particular context.

**i** DEFINITION**Reporting Mechanism**

A process that allows individuals to safely report incidents of abuse or harmful behaviour. Effective reporting systems provide clear procedures, confidentiality, and follow-up support.

**i** DEFINITION**Sextortion**

Threatening to share an intimate image/video without the consent of the person shown unless payment is received.

**i** DEFINITION**Synthetic Media**

AI-generated or manipulated images, audio or video content that resembles existing persons, objects places, entities or events, such that they would appear, falsely, to a person to be authentic or truthful.

**i** DEFINITION**Trigger Event/Trigger Moment**

A moment, such as a major sporting event (MSE), that increases visibility, emotional investment, and online engagement – thereby acting as a catalyst for heightened online hostility and creating conditions where online abuse may intensify or spread rapidly.

**i** DEFINITION**Welfare**

The protection and promotion of a person's safety, health and well-being through care, support and safeguarding measures.

**i** DEFINITION**Well-being**

Refers to a person's overall quality of life and internal state (how they feel and function physically, mentally and emotionally).



## REFERENCES

- 1 Ofcom and Kick It Out, 'Online hate and abuse in sport: A report by Ofcom in partnership with Kick it Out' May 2025 <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/online-abuse/online-hate-and-abuse-in-sport-in-partnership-with-kick-it-out.pdf?v=396829>
- 2 Kilvington, D. (2021). The virtual stages of hate: Using Goffman's work to conceptualise the motivations for online hate. *Media Culture & Society*, 43(2), 256-272
- 3 Kavanagh, E., Jones, I., & Sheppard-Marks, L. (2016). Towards typologies of virtual maltreatment: Sport, digital cultures and dark leisure. *Leisure Studies*, 35, 783-796. doi:10.1080/02614367.2016.1216581
- 4 K Barker, 'Online Violence as a Digital Condition: A New Cultural Habit' *Polemos* (2025) 19(1), 27; 41. <https://doi.org/10.1515/pol-2025-2009>
- 5 K Barker, 'Combatting Technology Facilitated Violence against Women and Girls – Discussion Paper' Council of Europe (September 2024) <https://rm.coe.int/gec-pc-evio-2024-5-gec-cdpcevioidiscussionpaper11sep24-2749-5696-6410-1/1680b1cbf3>
- 6 Kavanagh, E., Mountjoy, M., Teunissen, L. & Constandt, B. (2025). "I'm outside, and I'm going to hurt you": The dark side of stalking in sport. *British Journal of Sports Medicine*
- 7 Differentiation between safeguarding adults and safeguarding children should be a consideration. See e.g.: FA, 'Best Practice and Guidance Notes – The Complete Directory' <https://www.thefa.com/football-rules-governance/safeguarding/section-11-the-complete-downloads-directory>.
- 8 J Fonseca & T Borges-Tiago, (2024). Digital Literacy Education and Cyberbullying Combat: Scope and Perspectives. In: A Kavoura, T Borges-Tiago & F Tiago (eds) *Strategic Innovative Marketing and Tourism. ICSIMAT 2023. Springer Proceedings in Business and Economics*. Springer, Cham. [https://doi.org/10.1007/978-3-031-51038-0\\_18](https://doi.org/10.1007/978-3-031-51038-0_18)
- 9 I Bongiovanni, DM Herold & SJ Wilde, 'Protecting the play: An integrative review of cybersecurity in and for sports events' *Computers & Security* (2024) Vol 146, 104064, 2. <https://doi.org/10.1016/j.cose.2024.104064>.