**WRITTEN EVIDENCE FROM THE FOOTBALL AUTHORITIES[1] (OSB97)**

**PUBLIC BILL COMMITTEE ON THE ONLINE SAFETY BILL**

## Introduction:

Online discriminatory abuse is a serious problem in football, from the grassroots to the professional game. We all saw last summer how three young England players were subjected to the most sickening online racist abuse after they had stepped up for their country. The football authorities have been in discussions with social media companies for some years now, and while some progress has periodically been made, we agree that legislation is ultimately needed to incentivise, intensify and sustain the systemic changes that are required to significantly enhance online safety for the long term.

The football authorities welcome the Online Safety Bill and we were grateful to have the opportunity to give oral evidence to the Joint Committee on the Draft Online Safety Bill in September 2021. We also submitted written evidence to that Committee, as well as the DCMS Sub-Committee on Online Harms and Disinformation.

We have continued our engagement with the Government and parliamentarians since that point and are pleased that the Government has recently strengthened the Bill in a number of important areas. As highlighted when we provided evidence to the Public Bill Committee in May 2022, we welcome the new provisions on hate crime, anonymity and communications offences.

In addressing the challenges that we see affecting our participants across the game, we believe that there are a few specific areas where the Bill can be strengthened even further. Our proposed changes to the Bill are set out below.

## Online Discriminatory Abuse in Football:

As the nation's number one team sport with 18 million fans, 14 million participants and over 100,000 grassroots teams, football has an incredible power to bring people together, break down barriers and act as a force for good in society.

However, as outlined to the Joint Committee in September 2021, the football authorities have been concerned for some time now about the rising levels of online discriminatory abuse in the game. The victims are not only football players, but also their families, referees, coaches, administrators, pundits, fans and others working in the game. The abuse is not virtual: it is real. It is directed at real people who are real victims. The language used is debasing, and often threatening and illegal. Similarly, emojis and memes are used to spread harmful and discriminatory content. These written and pictorial messages cause distress to the recipients and the vast majority of people who abhor discrimination of any kind.

The football authorities have been in discussions with Twitter, Meta and other social media companies for several years now. Tangible progress has been made very recently, including with tools such as bulk filters. However, there is much more to do. For instance, it is still proving very difficult to ensure

[1] Joint submission supported by Kick It Out, The FA, The Premier League, EFL, Women's Super League, Women's Championship, National League, Isthmian League, Southern League, Northern Premier League, Professional Footballers Association, League Managers' Association, Professional Game Match Officials, and Women in Football.

that social media companies prevent or take down offensive content before it is seen, that online abusers are prevented from deleting and re-registering accounts, or that authorities have sufficient information and evidence to take prosecutions forward. Individuals can abuse others online anonymously, which means that, more often than not, online hate and discriminatory abuse have no real-world consequences for perpetrators or social media companies.

The football authorities have implemented a range of other measures to tackle online discriminatory abuse in the game, for instance:

- The creation of a Football Online Hate Working Group – comprising the main football authorities, the Home Office, Sky, the UK Football Policing Unit, the Crown Prosecution Service and the social media companies;
- Proactive monitoring of social media platforms, alongside investigations and collaboration with law enforcement;
- Education initiatives for players;
- Campaigns for football fans – calling on them to challenge and report discriminatory abuse, and to make clear that it will not be tolerated in our game.

**The Online Safety Bill: Football's Priorities**

The football authorities called for a number of changes to the legislation when we gave our written and oral evidence to the Joint Committee in September 2021 and are pleased that many of these recommendations have been adopted by the Government. As indicated when we gave evidence before the Public Bill Committee in May 2022, we are pleased to see a number of key provisions that will specifically address the needs of those who play, watch and work in football:

1. **Sanctions framework:** the basic framework of potential fines of up to 10% of relevant turnover has been effective in other areas of regulated activity so could be a real and significant tool to ensure compliance by social media organisations

2. **Definition of "harm":** we welcome that this has been extended to include "the manner of dissemination" of information, as this appears to capture some forms of persistent trolling such as pile-ons

3. **Hate Crime:** we welcome the designation of Hate Crime as priority illegal content on the face of the Bill, which means that platforms will have an active duty to minimise exposure to such content

4. **Anonymity:** we welcome the new anonymity provisions, which mean that ID verification must be offered as an option and users will have greater control over who can contact them and what they see online

5. **Communications offences:** we are pleased that the Government has accepted the Law Commission's recommendations to reform the communications offences. In particular:
    - The threatening communications offence appears to cover the kind of death threats and rape threats to which people who play, watch and work in football have been subjected; and
    - The harm-based offence triggered by communications that cause harm without reasonable excuse appear to cover forms of trolling such as malicious tagging

6. **Content harmful to adults:** we welcome the development that Category 1 providers will be required to set out clear terms and conditions on how they will protect users from such harms. As mentioned during evidence provided to the Public Bill Committee in May 2022, we are exploring the data that football has collected (which amounts to several thousand individual items of abusive content) to consider what specific items of content may fall within this category so that we can better inform future public debate on what categories of content might be designated in this category of harm.

For the people who play, watch and work in football who are often high-profile victims of online abuse, these would be vital cornerstones of the legislation. We would encourage the Public Bill Committee, Government and parliamentarians to ensure that these provisions are retained in substantially their current form and not materially diluted.

**Strengthening the Bill:**

There are a few areas where we believe that the legislation can be strengthened even further if it is to be truly effective in mitigating the online abuse experienced by the football community and broader society. These include the following areas:

1. **Ensuring transparency reporting provides appropriate information**

While the Bill requires transparency reporting, it does not clearly establish what should be reported. There should be clear minimum standards set out in law to ensure social media companies provide relevant information as part of transparency requirements to better enable data-driven interventions to prevent harm.

This could be done by The Bill setting out minimum levels and categories of information that will need to be provided each year as part of the transparency reporting requirements set out in sections 64 and 65. This could be achieved, for example, by amending section 64(3) as shown below to require that all transparency reports contain specific pieces of information. It is worth noting that, while the transparency requirements suggested may appear numerous, in the context of data analytics businesses whose business models are to monetise precisely this data, this information should be readily available and thus would not be an excessive request.

(3) In response to a notice relating to a relevant service, the provider of the service must produce a transparency report which must—

(a) contain the following information:

(i) The number of individual pieces of content that have been prevented from being accessed by individuals, or where the length of time for which that content is present has been minimised or that have been taken down pursuant to the duties set out at section 9(3), 11(3) or 13(4) of this Bill (referred to in this subsection as "relevant content") since the date of the service provider's last transparency report, as well as further detail as to the number of individual pieces of relevant content:

(1) in each category of harmful content set out in this Bill (namely, illegal content, content harmful to adults and content harmful to children)

(2) for illegal content that is a "Relevant Offence" pursuant to paragraph 6 of Schedule 7 to this Bill (offences under the Crime and Disorder Act 1998), in each category of protected characteristic under the Equalities Act 2010 to which the relevant content relates;

(3) created in each global jurisdiction;

(4) by the time the relevant content was posted expressed by day and by hour;
(5) by longevity of the relevant accounts creating the relevant content (expressed in the number of days for which the relevant account was live and/or active prior to the relevant post)
(6) by type of content (including, but not limited to, text, emoji, video, audio and meme)
(7) that were (or were intended by the user to be) pieces of content available to all members of the public, pieces of content available to a closed group of users or pieces of content by way of direct or private messaging to a single user
(8) by relative engagement expressed as the number of impressions of any individual item of relevant content
(9) that were posted (or were attempted to be posted) by a user who has previously posted (or has attempted to post) content that the service provider has previously prevented from being accessed by individuals, or where the length of time for which that prior content was present was minimised or that was taken down pursuant to the duties set out at section 9(3), 11(3) or 13(4) of this Bill.
(10) for content removed by moderation systems, removed by each method of moderation (including by each form of proactive technology set out in section 184(1)or by human review);
(11) for relevant content about which an unsuccessful complaint was made, by reason for the full or partial denial of the complaint;
(12) for account holders of accounts creating relevant content, by such demographic data as you have about age, gender and other relevant personal characteristics (without revealing individual identities) and

(ii) any other information of a kind specified or described in the notice; […].

b) be produced in an open data or other readily accessible format to enable third parties to easily download, review and analyse the report

It is also essential that Ofcom has the ability to share reporting information as envisaged by the Bill.

**2. Ensuring that the transparency report approval is a matter of law, not guidance**

The Bill does not currently require transparency report approval and publication to be a matter of law. We believe the Bill should do this and have clear requirements for the form in which the report is published.

Whilst we note that Ofcom would be required under section 65 of the Online Safety Bill to publish guidance in relation to the transparency reporting required by section 64, the Online Safety Bill could be amended to set out (i) the process by which the transparency report(s) should be approved by service providers; and (ii) the form in which they should be published. Currently, there is no requirement in relation to (i) and (ii) is as matter of the Ofcom notice, pursuant to 64(3)(d). Instead, the transparency report approval and publication should be a matter of law (rather than guidance) and should align with the process already in place under the UK Modern Slavery Act sections 54(6) to (7), to assist compliance.

This could be achieved by making the following amendments:

- Delete the words "in the manner and" in section 64(3)(d);
- Insert new sections 64(4A), 64(4B) and 64(4C):

(4A) A transparency report —

(a) if the provider is a body corporate other than a limited liability partnership, must be approved by the board of directors (or equivalent management body) and signed by a director (or equivalent);
(b) if the provider is a limited liability partnership, must be approved by the members and signed by a designated member;
(c) if the provider is a limited partnership registered under the Limited Partnerships Act 1907, must be signed by a general partner;
(d) if the provider is any other kind of partnership, must be signed by a partner.

(4B) If the provider has a website, it must—
(a) publish the transparency report on that website, and
(b) include a link to the transparency report in a prominent place on that website's homepage.

(4C) If the provider does not have a website, it must provide a copy of the transparency report to anyone who makes a written request for one, and must do so before the end of the period of 30 days beginning with the day on which the request is received.

**3. Delivering the benefits of the Bill more quickly**

The Online Safety Bill will not substantially come into force until 2024. This will likely cause anxiety to the many victims of online abuse and risk causing the social media companies to delay further helpful interventions to minimise harm. This could be remedied relatively simply by accelerating start-dates for certain areas of the Bill within legislation.

As written, The Bill provides that the key operative parts of it come into force on such day as the Secretary of State may by regulations appoint, although different days may be appointed for different purposes (sections 193(2)-(3)).

Certain crucial and easy-to-implement aspects of the legislation might be accelerated so that they come into force a short, specified period after the day on which the Act is passed. A new subsection could be added after section 193(1) of the Bill to provide that the following provisions relating to user-to-user services, for instance, come into force [e.g. 30, 60, 90] days after the day on which the Act is passed:

- Section 6(5)(b) and section 13 (which require providers of Category 1 services to comply with the duties to protect adults' online safety);
- Section 6(2)(c) and section 17 (which require providers of regulated user-to-user services to comply with certain duties about reporting); and
- Section 6(2)(d) and section 18 (which require providers of regulated user-to-user services to operate a complaints procedure and to set out the policies and processes in relation to that procedure in the terms of service)

**4. Ensuring new social media providers meet the standards by applying "Safety by Design"**

The Bill currently separates out categories of service providers on the assumption that the larger providers create more risk, thereby missing the opportunity to ensure new entrants in the market ensure their products are designed safely.

While it is largely true at present that larger providers create more risk, rapid growth and innovation in the technology sector (which should be broadly encouraged) may mean that a new and highly

influential provider can appear and grow quickly (and this is a risk that is particularly acute with social media because of the power of network effects to enable exponential growth). Unless online safety is included at the centre of these businesses at the outset, there is a significant risk that compliance systems do not grow at the same pace as revenues, exacerbating increased risks to online safety and the perpetuation of the challenges that we see particularly on the larger platforms today.

The Online Safety Bill could include a "safety by design" component for all companies, so that it captures newer or smaller platforms, but does not stifle innovation (and indeed could assist future compliance with the more detailed aspects of the Online Safety Bill as the platform grows). In turn it would help guard against "risky by design" effects. This could be achieved, for example, by adding in a "safety by design" duty into section 9, which sets out the duties on all providers of user-to-user services in relation to illegal content as follows:

> (1) The "illegal content duties" in relation to user-to-user services are the duties set out in this section
> (1A) The duty to ensure their services comply with the latest version of the "safety by design" guidance published by OFCOM in accordance with section [9A]'

We are of the opinion that it would be best for OFCOM, as the regulator, to have discretion in terms of the content of the "safety by design" duty, so that it can more easily be amended as technology and risks evolve. However, this discretion should not be unfettered and we consider that a new Section 6A should be added to set out a non-exhaustive set of minimum standards for that duty, as informed by the UK Government's June 2021 Safety by Design guidance and the Joint Committee's Report of Session 2021-22 (see paragraph 82):

> (9A) OFCOM must prepare and maintain appropriate "safety by design" guidance that sets out the steps which all providers of regulated user-to-user services must take in order to reduce the risk of harm to all users of their services. This guidance should include, as a minimum, that all providers of regulated user-to-user services must:
> (1) take preventative steps to ensure that its services reduce each user's exposure to harm,
> (2) take steps to understand who its users are and the risks that its services might present to those users,
> (3) give users of their services the tools and information to make informed choices concerning their use of the services, including by:
> (a) avoiding the use of algorithms to promote content over which the user has limited control,
> (b) providing transparent information to users about the nature of recommendation algorithms and allowing the user to have control over the priorities those algorithms set, and
> (c) allowing users to deactivate recommendations from other users with whom they have not chosen to engage.
> (4) take steps to ensure that only users who are old enough safely to use the services are able to access the services, and
> (5) take steps to reduce the risks of geolocation, photo identification and other functionality leading one user being able to identify and/or locate another user

**5. Improving the clarity of anonymity obligations**

Whilst we welcome the provisions around voluntary ID verification and giving users greater control over interactions, we believe that the definition of verification could be helpfully clarified and to aid transparency, an individual user's verification status should be visible to other users. We have seen

some draft amendments to this effect which we understand will be proposed by Siobhan Baillie MP and endorse those.

### 6. Ensuring Hate and Discrimination are combatted through the Code of Practice

Hate and discrimination are not currently the subject of a specific code of practice. Given the volumes of such abuse on the platforms and its evolving nature, we believe it would be helpful to have such a specific Code to deal with the existing and emergent persistent threats. Rather than propose specific amendments, we are keen to work closely with the Government and Ofcom on this important issue and would request a discussion with DCMS and Ofcom to offer our support and experience on the articulation of a Code.

We want to ensure that the experiences and voices of victims of online abuse are able to provide critical insight and influence the creation of Ofcom's guidelines so that the issues are effectively tackled and addressed.

*24 June 2022*