# TOTTENHAM HOTSPUR FOOTBALL CLUB

## Online Safety Policy

April 2024

## Foreword

This Online Safety Policy (the "**Policy**") reflects the safeguarding ethos of Tottenham Hotspur Football and Athletic Co. Limited (trading as "**Tottenham Hotspur Football Club**"), its Group Companies, Tottenham Hotspur Foundation (a registered charity known as the "**Foundation**") and Tottenham Hotspur Women Football Club Limited – together the "**Club**". The Club places great importance on Safeguarding and believes that everyone has the right to enjoy football and participate in its activities in safe and inclusive environments, including the Club's online environments.

The board of directors of the Club endorses this Policy as part of the Club's constitution and commitment to safeguard online safety.

The purpose of this Policy is to:

- ensure and promote the safety and wellbeing of Children and Adults at Risk is paramount when individuals are using the Internet, social media or mobile devices;
- minimise the opportunity for Children and Adults at Risk to be harmed or exposed to harmful or inappropriate behaviour and content online;
- provide staff with the overarching principles that guide the Club's approach to online safety; and
- ensure that, as a Club, the Club operates in line with the Club's values and within the law in terms of how the Club uses online devices.

This Policy is adapted from the Premier League *Online Safety Policy*.

**Matthew Collecott**

STRATEGIC SAFEGUARDING LEAD
Operations and Finance Director
Board of Directors of Tottenham Hotspur Football & Athletic Co. Ltd.

Effective Date of Policy: April 2024

Policy Owner/Lead: Head of Safeguarding and Welfare

Review Date: April 2025

# Tottenham Hotspur Football Club – Online Safety
# INTERNAL ONLY

**Staff in Child and Adult at Risk facing parts of the Club should work hard to ensure that they:**

- *Empower and educate Children and Adults at Risk to keep themselves safe online.*
- *Understand reporting procedures and how to access advice and support.*
- *Understand online risks and harms and how they can protect Children and Adults at Risk.*

## Sexting images

**Sexting image is disclosed to a Staff member OR a Staff member has a Concern about suspected sexting image.**

↓

**Isolate the device to avoid others from seeing the sexting image.**

↓

**Is the Child in immediate risk of harm?**

- **Yes** → **Search the device and review the images**
- **No** → **The Concern must be referred to the Safeguarding Team immediately via email at safeguarding@tottenhamhotspur.com without reviewing the images or searching the device**

↓

**Does the incident involve:**
- **an Adult;**
- **Coercision, blackmailing or grooming;**
- **Consent;**
- **Acts that are unusual for the Child's developmental stage or are violent; or**
- **Sexual acts and the Child is, or appears, under 13?**

- **Yes** → **Make a child protection referral. Please contact the Safeguarding Team who can assist.**
- **No** → **Report the incident to the Safeguarding Team**

## Communication and use of social media

**Staff must ensure that personal data is never processed without the full and prior knowledge and agreement of the Club, including images and recordings. This includes the recordings of Online Activities.**

**Staff must never use their Personal Devices to contact Children or Adults at Risk who have been involved in Club Activities.**

**Staff should be mindful of any personal use of Social Media and the content they post. What Staff post as individuals can affect how the Club is viewed, by association, and pose risk of reputational damage to both you and the Club.**

## Online Meeting Platforms

**Staff should ensure that they abide by the following when using Online Meeting Platforms:**

- *Where Staff access Online Meeting Platforms from a personal space, they must ensure that the background is neutral where nothing personal or inappropriate can be seen or heard in the background. Staff should always consider what is visible if the Online Activity will involve sharing a screen, for example, desktop files, social media accounts, personal information or emails.*
- *Staff must always familiarise themselves with Club-Sanctioned Engagement Platform's privacy settings ensuring they are applied correctly.*
- *Staff must use secure internet connections during online communications.*
- *Staff must ensure that Online Meeting Platforms are set up to prevent unauthorised access.*
- *Staff must work in partnership with the Safeguarding Team to establish appropriate Online Activity supervision and ratios, for example, how platform breakout rooms will be supervised. The appropriate ratios will be decided on a case-by-case basis.*

*Staff must ensure that the Online Meeting Platform is secure and that safety settings have been applied, for example:*

- *Allowing or preventing participant cameras to be turned on. Consideration should be given to whether Children and Adults at Risk are comfortable turning their camera on. Some participants may be unfamiliar with technology use, may have had a bad experience using video calls or attempt to hide abuse or neglect.*
- *Setting up a 'waiting room/participant lobby' to ensure only invited participants join.*
- *Allowing or preventing the sharing of content by participants.*
- *Ensuring participants are unable to communicate with one another within the Online Meeting Platform before or after the Online Activity or without Adult supervision.*
- *Allowing or preventing participant microphones to be turned on.*

## Reporting a breach of the Online Safety Policy

**If Staff are aware of any breach of this Policy from a reporting or regulatory perspective (for example, a breach of the acceptable use section of this Policy), this should be reported to their line manager, with a copy to the HR Team and the Legal Team, as soon as practicable.**

## Reporting a safeguarding concern

**Any concerns relating to the online safety and wellbeing, Abuse or Child Sexual Exploitation of Staff, a Player, a Child, an Adult at Risk, a Visitor, or parent/carer this should be reported directly to the Head of Safeguarding & Welfare immediately, or in any event within 24 hours (with a copy to the Safeguarding Team).**

## Reporting Child Sexual Exploitation

**All forms of Child Sexual Exploitation or Abuse should be reported to the local police force as soon as possible.**

# Table of Contents

# Introduction

This Policy reflects the safeguarding vision, values and strategy of the Club.

The Club is dedicated to taking all reasonable steps to make it as difficult as possible for any form of abuse to occur in online environments and this Policy forms part of those efforts to ensure that safeguarding is firmly embedded in the values and practices of the Club and its Staff.

All additional policies referred to within this Policy can be accessed via The Shelf and the Safeguarding page.

Any Club-wide online safety concerns can be addressed to any member of the wider Safeguarding Team via the contact details contained within the table below. Other helpful external agency contact details are contained within **Appendix 1** and **Appendix 2**.

| | |
|---|---|
| **Club Safeguarding Team:** | safeguarding@tottenhamhotspur.com |
| **Foundation:** | Natalee Hibbert<br>07384 258 758<br>natalee.hibbert@tottenhamhotspur.com |
| **Women & Girls:** | Sandra Barratt<br>07384 818062<br>sandra.barratt@tottenhamhotspur.com |
| **Academy:** | Tim Ford<br>07392080266<br>tim.ford@tottenhamhotspur.com |
| **Global Football Development:** | Lauren Cotton<br>07384117643<br>lauren.cotton@tottenhamhotspur.com |
| **Club/Foundation/Match & Event Day and concerns about practice of staff:** | Shauna McAllister<br>07879997839<br>shauna.mcallister@tottenhamhotspur.com |
| **Club HR Team:** | hr@tottenhamhotspur.com |
| **Club Legal Team:** | legal@tottenhamhotspur.com |

## Definitions

The following definitions apply in this Policy:

| | |
|---|---|
| **Abuse:** | is any form of harm or maltreatment of an individual. This Policy focuses on Abuse in Online Spaces which is predominantly: Emotional Abuse, Sexual Abuse, Discriminatory Abuse or Psychological Abuse; |
| **Activity or Activities:** | means online activity, or series of activities, arranged by or in the name of a Club in which Children and/or Adults at Risk participate. |
| **Adults:** | means any person or persons who are over the age of eighteen; |
| **Adult at Risk:** | means any person aged 18 or over who has needs for care and support (whether or not the local authority is meeting any of those needs) and is experiencing, or at risk of, abuse or neglect, and as a result of those care and support needs is unable to protect themselves from either the risk of, or the experience of abuse or neglect. This may include people with learning disabilities, sensory impairments, mental health needs, older people and people with a physical disability or impairment. It may also include people who are affected by the circumstances that they are living in, for example, experiencing domestic violence. An individual's level of vulnerability to harm may vary over time depending on the circumstances they are in and their needs at that time. |
| **Back of House:** | means all areas which are not generally accessible to the public including Lilywhite House, all warehouses and store rooms at all Club shops and all similar locations on Club Premises; |
| **Child and Children:** | means any person or persons who have not yet reached their eighteenth birthday; |
| **Child Sexual Exploitation:** | is a form of Sexual Abuse which occurs against Children. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a Child into sexual activity usually in exchange for something the victim needs or wants; |
| **Club Academies:** | means both the men's and women's academies at the Club, including the Academy Development Centres; |
| **Club Channels:** | means the Club's official communications channels from time to time such as the Club's official Facebook pages, the Club's official Instagram pages, the Club's official TikTok accounts, the Club's official X (formerly known as Twitter) feeds ad the Club's official YouTube channel; |

| | |
|---|---|
| **Club Sanctioned Engagement Platforms:** | means engagement platforms as authorised by the Club from time to time; |
| **Club Premises:** | means the Stadium, the Training Centre all Back of House areas and other premises owned by the Club from time to time; |
| **Cyber Bullying:** | a form of online Emotional Abuse whereby an individual is discriminated against; |
| **Data Protection Legislation:** | all applicable laws relating to data protection, the processing of personal data and privacy, including: the Retained EU law version of the General Data Protection Regulation ((EU) (2016/679)) ("**UK GDPR**") and the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications), and any other data protection and/or privacy legislation applicable in the UK from time to time, (each as amended, updated, replaced or re-enacted from time to time and including all subordinate legislation made from time to time under or giving effect to the same) and references to "controller", "personal data", "special category data", "process", "processing" and "supervisory authority" have the meanings set out in, and will be interpreted in accordance with, such applicable laws; |
| **Discriminatory Abuse:** | including racist abuse, sexist abuse, abuse based on an individual's disability or other protected personal characteristic as defined in the Equality Act 2010, as well as other forms of harassment, slurs or similar unfair treatment; |
| **Emotional Abuse:** | the persistent emotional maltreatment of an individual such as to cause severe and persistent adverse effects on the individuals' emotional development; |
| **Events:** | means Tottenham Hotspur Football Club matches, Tottenham Hotspur Women's Football Club matchdays, third-party sporting events (such as, NFL, rugby or boxing events), third-party concerts, major non-concert events, conferences and events and visitor attractions as arranged by the Club from time to time; |
| **Extremism:** | vocal or active opposition to fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs; |
| **Football Authority Regulations:** | the rules and regulations from time to time in force of any Governing Body, national association or league under the auspices of The Football Association and/or the Premier League to the extent that they relate or apply to the Club; |
| **Live Streaming:** | is the broadcasting of real-time, live video, or audio using the Internet. Most live streaming platforms include methods for the audience to communicate with the streamer (the person/organisation broadcasting) using comments, polls and other |

| | |
|---|---|
| | interactive features. Some enable viewers to give virtual gifts which can be converted into real currency; |
| **Online Activities:** | means any learning or delivery by the Club that takes place at a distance or is delivered online through digital technology in Online Spaces; |
| **Online Meeting Platforms:** | means any software used for conducting meetings online, including but not limited to Microsoft Teams, Zoom, Skype and Adobe Classroom; |
| **Online Safety:** | (also known as internet safety, e-safety or cyber safety) is a broad umbrella term that refers to the act of staying safe online and the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media, for example, social media, text or other messaging applications, gaming devices, email etc. |
| **Online Spaces:** | means all virtual spaces where interaction between individuals can occur, this includes, but is not limited, to social media platforms, such as X (formerly known as Twitter), Facebook, Instagram, TikTok, LinkedIn, SnapChat, YouTube, Flickr, Telegram and WhatsApp; |
| **Players:** | means all players for the Club's men's and women's first team squads and all of the Club's Academy players; |
| **Psychological Abuse:** | including Emotional Abuse, threats of harm or abandonment, deprivation of contact, humiliation, blaming, controlling, intimidation, coercion, harassment, verbal abuse, isolation or withdrawal from services or supportive networks; |
| **Radicalisation:** | the process by which a person comes to support or engage with Terrorism and forms of Extremism leading to Terrorism; |
| **Sexual Abuse:** | forcing or enticing an individual to take part in sexual activities, not necessarily involving a high level of violence, whether or not the individual is aware of what is happening. The activities may involve physical contact as well as non-contact activities, such as grooming. Child Sexual Exploitation is a form of Sexual Abuse; |
| **Social Media:** | is a collective term for websites and applications that enable users to communicate and engage with others online, including but not limited to X (formerly Twitter), Facebook, Instagram and TikTok; |
| **Spectators:** | means anyone in attendance at any Event held at the Stadium, other than for work; |

| | |
|---|---|
| **Stadium:** | means both the Tottenham Hotspur Stadium, which is situated at High Road, Tottenham, London N17 0AP and the Leyton Orient Stadium, which is situated at Brisbane Road, London E10 5NF; |
| **Staff:** | any person acting for or on behalf of the Club in an official role, acting on behalf of the Club, whether as an employee, volunteer, casual workers or staff, consultant or otherwise; |
| **Terrorism:** | an action that endangers or causes serious violence to a person/ people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the Government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause; |
| **Training Centre:** | means the Club's training facilities which is situated at Hotspur way, Whitewebbs Lane, Enfield EN2 9AP; |
| **Visitors:** | means all visitors to the Stadium and Club Premises, including guests at the visitor attractions and contractors; and |
| **Vulnerability:** | being susceptible to additional risks of harm or Abuse including but not limited to racism, Radicalisation and in need of special care, support, or protection. |

## Application of the Policy

This Policy applies to all Staff.

All Staff under the jurisdiction of the Club agree to abide by all Club policies and procedures as in place from time to time including this, Policy.

## Power to change, rescind or add to the provisions of the Policy

In the event an issue arises that is not foreseen in this Policy, it will be addressed by the Club in a manner that protects and promotes the objectives identified in this Policy.

## Laws

The laws of England and Wales shall apply to this Policy.

## A Framework for Online Safety

The Club recognises that Abuse can take place online, for example, child-on-child, online sexual harassment, cyberbullying, consensual and non-consensual/lawful and illegal nude and semi-nude image sharing. Online Safety is a core part of the Club's safeguarding measures. Procedures, technology, and training should work in concert to provide an effective whole-Club preventative approach to Online Safety.

This Policy defines acceptable use of social media, mobile and smart technology and outlines procedures for responding to concerns regarding Abuse, harassment and harm perpetrated online.

## Standards of Practice and Behaviour

The Club's Safeguarding Code of Conduct applies to all Staff, both in in-person and online environments. The Safeguarding Code of Conduct can be found on The Shelf.

## Workforce Suitability and Experience

Safer recruitment procedures are in place for any Child and Adult at Risk-facing roles within the Club, both in terms of physical and online environments. For more information on safer recruitment please see the Safer Recruitment Policy which can be found on The Shelf.

## Platform/System Suitability

Staff should ensure that all Club Devices (as defined below), systems and platforms being used by Children and Adults at Risk are secure and suitable for the age, stage of development, ability and needs of Children and Adults at Risk participating.

Club user accounts should be set up and Staff should be prevented from using personal accounts or non-Club platforms and systems to communicate or engage with Children and Adults at Risk.

## Monitoring and Security

The Club has implemented appropriate filtering, monitoring, reporting, encryption, anti-virus protection and control access systems. Including URL filtering on all web traffic, advanced threat protection, endpoint security and access control lists. All connections are logged and monitored.

The Club will ensure that filtering and monitoring systems reflect and adapt to changes in platforms, apps, smart and mobile technology with effective reporting by actively reviewing filtering and monitoring system reports and responding swiftly and appropriately to identified procedural breaches and safeguarding concerns.

GoBubble has been implemented to monitor Online Spaces and in future will provide monitoring and blocking on Club Channels. This tool uses live AI monitoring to filter out harmful content before it can be seen, this includes text, emoji, image and video monitoring.

## Managing Risk

All Staff should ensure that risk assessments and risk management plans include safeguarding, data protection and technical expertise. Risk controls should be regularly reviewed.

## Consent and Data Protection

Obtaining consent for participation and image use/recording and ensuring that personal data is processed in line with Club data protection procedures and legislation. If you have any questions about obtaining consent for image use/recording please contact the legal team on legal@tottenhamhotspur.com.

## Additional Needs

Staff should identify and meet any support needs, for example, a special educational needs or disability.

## Staff Responsibilities

Staff in Child and Adult at Risk facing parts of the Club should work hard to ensure that they:

| | | |
|---|---|---|
| Empower and educate Children and Adults at Risk to keep themselves safe online. | Understand reporting procedures and how to access advice and support. | Understand online risks and harms and how they can protect Children and Adults at Risk. |

## Staff Training

The Club will provide appropriate training to Staff based on their role at the Club, the following will be applicable to those Staff who require training.

As part of Staff induction, Staff are required to complete a safeguarding module. Staff can access safeguarding training via the MyLearning system on Centre Circle. All Staff involved in direct work with Children and Adults at Risk are given annual safeguarding training, which includes Online Safety.

All Staff are given access to annual training on online risks and harms, acceptable use, professional boundaries, keeping Children and Adults at Risk safe online and how to report concerns.

The onboarding process ensures that Staff have read and understood the safeguarding policies. Staff will be notified of any updates to any Policy and there is an expectation that all Staff read these updates.

For more information, Staff should refer to the Safeguarding Workforce Development Framework which can be found on The Shelf.

## Safeguarding legislation and guidance

The Club's approach to Online Safety is based on the principles recognised within UK and International legislation and UK Government guidance. For the purposes of this Policy, the following have been taken into consideration:

### Children

- The Children Act 1989 and 2004
- Working Together to Safeguard Children 2018
- Keeping Children Safe in Education 2022
- The Children and Young Persons Act 1933
- The Protection of Children Act 1978
- The United Nations Convention on the Rights of the Child 1992
- The Safeguarding Vulnerable Groups Act 2006
- Protections of Freedoms Act 2012
- Children and Families Act 2014

### Adults at Risk

- The Care Act 2014
- Mental Capacity Act 2005
- Safeguarding Vulnerable Groups Act 2006
- Protection of Freedoms Act 2012
- Domestic Violence, Crime and Victims (Amendment) Act 2012
- Sexual Offences Act 2003
- Equality Act 2010
- Making Safeguarding Personal Guide 2014

## Other

- Equality Act 2010
- The Human Rights Act 1998
- The Data Protection Act 2018
- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- The Communications Act 2003
- Online Safety Act 2023
- The Gambling Act 2005
- The Video Recordings Act 1984
- Premier League Safeguarding Rules and Safeguarding Standards
- Premier League Prevent Duty Guidance
- The Licensing Act 2003

# Online Risks

While online gaming, social media, communication and engagement platforms offer many benefits and positive opportunities, it is important to be aware of the potential risks faced by Children and Adults at Risk which includes being exposed to illegal, harmful, explicit or inappropriate content and contact. Some of the risks associated with Social Media and Online Spaces include the following:

| | | |
|---|---|---|
| Catfishing | Cyberbullying | Grooming |
| Harmful content | Harmful online challenges | Inappropriate content |
| Harmful online communities | Online stalking | Oversharing |
| Phishing | Radicalisation and Extremism | Revenge Porn / Intimate Image Abuse |
| Sextortion | Sexual Imagery | Social Engineering |
| Social Media Addiction | Solicitation | Unrealistic sense of body image / reality |

## Child Sexual Exploitation

Social Media and Online Spaces can be used by offenders to sexually abuse Children or to facilitate offline Abuse. Online Child Sexual Exploitation and Abuse is when offenders use technology or the internet to view and share child sexual abuse material, groom children online, or live stream the Sexual Abuse of Children. This includes Abuse perpetrated by Children against any individual under the age of eighteen.

If you have any concerns about potential or actual Child Sexual Exploitation at the Club, please report these immediately but in any event with 24-hours to the Safeguarding Team.

**All forms of Child Sexual Exploitation or Abuse should be reported to the local police force as soon as possible.**

This includes, but is not limited it:

- The sharing of Child Sexual Exploitation and Abuse content, for example images, videos and streaming.

  *NBV: please note that you should **not** send indecent images of Children as part of the report to the police.*

- Sexual contact between Adults and Children, for example requests to form sexual acts on camera or send sexual images, or arrangements to meet.

- Contact between Adults relating to Child Sexual Exploitation or Abuse of Children, for example advertising or acquiring Children for sex, or offers to share images or livestreams of Abuse.

## Sexual Image Sharing

Sexual image sharing is otherwise known as "sexting" is when people share sexual messages and/or a naked or semi-naked image, video or text message with another person. Sharing sexual images includes when an individual screenshots or otherwise records an image sent.

It is a criminal offence to take an intimate image without consent or to share an intimate image without consent with the knowledge that the person does not consent to sharing, with the intention of causing the victim humiliation, alarm or distress or if the image will be looked at for the purposes of obtaining sexual gratification. It is also criminal offence to create or share explicit images of a Child, even if the person creating or sharing the image is a Child.

## Reporting concerns

Children and Adults who are involved in a sexting incident might have shared an image of themselves, received an image from someone else or have shared an image of someone else more widely. This may have happened with or without the consent of all the people involved.

In relation to Children, sometimes a Child might tell you directly that they have been involved in sexting, or they might mention something which gives you cause for concern. Never wait for a Child to tell you directly that they have been involved in sexting, if you are concerned about sexting, please report this concern to the Safeguarding Team as soon as possible.

### What to do with a sexting image

It is best practice to **never** view any sexting images. If the image is on a Club Device, you need to isolate the device so that no one else can see the image. This may involve blocking the network to all users. If you have any concerns, please contact the Safeguarding Team who can work with the IT Team to isolate the Club Device.

You should **never** copy, print or share sexual images of a Child. This is a criminal offence.

You should only search devices if the Child is at immediate risk of harm, otherwise please report to the Safeguarding Team without viewing the images or searching the devices.

### Making a child protection referral

The Club asks Staff to follow a considered and detailed process when deciding whether or not to make a child protection referral about an incident of sexting. If you have any uncertainty, please contact the Safeguarding Team who can assist you in making any decision or who can refer the concern on behalf of the Club.

Staff should make a child protection referral if:

- the incident involves an Adult;

- there is reason to believe that a Child has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent;
- what you know about the image(s) suggests that the content depict sexual acts which are unusual for the Child's developmental stage, or are violent;
- the image(s) involves sexual acts and any child in the image(s) is under 13; and/or
- you have reason to believe a Child is at immediate risk of harm due to the sharing of the image, for example, if they are presenting as suicidal or self-harming.

If you think that a Child is in immediate danger, contact the police on 999. If you are worried about a Child but they are not in immediate danger, you should share your concerns with:

- the Safeguarding Team;
- the local child protection services;
- the NSPCC Helpline; or
- inform CEOP (Child Exploitation and Online Protection Command).

## Grooming

Children can be groomed online, in person or both – by a strange or someone they know. When a Child is groomed online, groomers may hide who they are by sending photos or videos of other people. The relationship a groomer builds can take different forms. This could be:

- a romantic relationship;
- as a mentor;
- an authority figure; and/or
- a dominant or persistent figure.

Groomers typically use certain patterns of behaviour to lead a Child to believe that what is happening is normal, or to make the Child feel trapped.

It's important to remember that Children may not understand they've been groomed. They may have complicated feelings, like loyalty, admiration, love, as well as fear, distress and confusion.

### Gaining information

A groomer will use social media to learn about a Child's interests from their online profiles and posts, and then use this knowledge to help them build up a relationship.

### Gaining trust

A groomer gains the Child's trust over time in order to Abuse them by pretending to be younger, giving advice or showing understanding, buying gifts, giving attention and/or taking Children on trips, outings or holidays.

### Gaining power

Once trust is established, groomers will exploit the relationship by isolating the Child from friends or family and making the Child dependent on them. They might use blackmail to make a Child feel guilt and shame or introduce the idea of 'secrets' to control, frighten and intimidate.

### Child Sexual Exploitation

Social Media means that groomers don't need to meet Children in real life to Abuse them, after making online contact a groomer can persuade a Child to engage in online sexual activity.

## Signs of grooming

The signs of grooming are not always obvious and may be hidden, in particular older Children might behave in a way that seems to be "normal" teenage behaviour, masking underlying problems. Some of the signs you might see include:

- being very secretive about how they're spending their time, including when online;
- having an older romantic partner;
- having money or new things like clothes and mobile phones that they can't or won't explain;
- underage drinking or drug taking;
- spending more or less time online or on their devices;
- being upset, withdrawn or depressed;
- sexualised behaviour, language or an understanding of sex that's inappropriate for their age; and/or
- spending more time away from home or going missing for periods of time.

### Protecting the Child

If a Child talks to you about grooming, it is important to:

- listen carefully to what they are saying;
- let them know they've done the right thing by telling you;
- tell them it is not their fault;
- say that you will take them seriously;
- don't confront the alleged abuser;
- explain what you'll do next; and
- report what the Child has told you as soon as possible.

### Reporting grooming

If you have any concerns about potential grooming involving anyone at the Club, please report these concerns immediately but in any event with 24-hours to the Safeguarding Team.

There are also various external reporting mechanisms available.

- The Child Exploitation and Online Protection Command ("**CEOP**") allows for reporting via this link https://www.ceop.police.uk/ceop-reporting/
- Local child protection services or the police can also be contacted about any kinds of grooming.

It's important to remember that it's against the law to make or share images of child abuse. If you see a video or photo that shows a child being abused, don't comment, like or share it. Instead, you can report it to:

- the website it's on;
- the police; and
- or contact the Safeguarding Team and the Safeguarding Team will report it to the police for you.

## Whistleblowing

If any Staff witness grooming within the Club and are concerned about repercussions, disclosure of this nature will fall under the Club's Whistleblowing Policy which can be found on The Shelf.

## Sextortion

Sextortion is where an individual meets their abuser through social media, or on a dating website and forms a relationship through conversation. The blackmailer often assumes a fake identity and after gaining the victim's trust, persuades them to send intimate images or videos of sexual acts via webcam. The sexual content or information is recorded unbeknown

to the victim and then used to blackmail them for money, sexual favours, or further sexual content. This is sometimes known as webcam blackmail.

Sextortion can be committed by an individual or by organised criminal gangs, often based in foreign jurisdictions. This can result in child exploitation and trafficking.

## Phishing

Phishing can take place in many forms; some phishing methods are outlined below. As required by contracts with the Club, Staff will be required to undergo a presentation on phishing as part of their induction.

**Via fraudulent quizzes**

- Cyber-criminals often pose seemingly harmless questions on Social Media, such as asking about your first job or first car. Though these posts may seem innocent, they can be used as security questions to gain access to your personal information.
- This issue is particularly prevalent on Facebook, but also on other Social Media.
- Cyber-criminals, working individually or collaboratively, can exploit quizzes, surveys on X (formerly Twitter) and Instagram, and 'get to know you' videos on TikTok.

**Via customer support scams**

- Online chats are instant and easier than phone calls. This makes them popular among younger consumers who prefer instant messages over waiting. Many companies are expanding their service options by offering dedicated support accounts to cater to these preferences.
- Unfortunately, scammers can easily deceive people by using a stolen logo and company description to create fake accounts that look like genuine companies. They then ask for help. They might direct targets to fake login pages and steal their login credentials. Some scammers even ask for upfront payment for repair services they don't provide.

**Via Direct Message ("DM")**

- Social Media provides easy direct messages. Many apps also have an in-app messaging feature, which scammers can exploit to create fraudulent profiles and impersonate someone close to the victim, such as a family member or friend.
- By taking advantage of the direct communication channel and the user's trust, these scammers fabricate fake scenarios and ask for help. Often, these requests involve emergency payments or passwords to private accounts.

**Via crypto scams**

- A common Social Media phishing scam is a cryptocurrency investment or giveaway scam. These fraudulent activities are promoted on Facebook and X (formerly Twitter) and propagated through fake celebrity profiles.
- These impostors create Social Media accounts that look legitimate, and they use persuasive language, often with a sense of urgency, to convince people to send them cryptocurrency.

**Via email**

- Social Media platforms often send emails to update users about security protocols or account related information. Users often trust that these emails have originated from a legitimate source. These email

**Via LinkedIn**

- Scammers can also exploit LinkedIn by creating bogus company pages and job scams. These scams begin with fraudulent job postings and gathering

templates are often standard and familiar, making them an easy target for spoofing.

- Due to users' tendency to disregard the design elements of these emails, hackers benefit from this behaviour by incorporating fraudulent links and buttons within the message body. When clicked, these links direct users to malicious sites where scammers steal sensitive information.
- Scammers often employ tactics, such as setting up fraudulent password reset scams or initiating malware downloads, to trick people into giving away their personal information. sensitive information. Then, cyber-criminals use this information in future phishing attacks.
- Scammers sometimes take things a step further by offering victims a fictitious job and sending them a fraudulent initial cheque by mail. After the victim deposits the check, the scammer will provide a reason for asking the victim to return a portion of the funds. Once the cheque bounces, the scammer disappears with the victim's money.

## Radicalisation and Extremism

Prevent is one of the elements of the government's counter Terrorism strategy. The four elements are:

- Pursue;
- Protect;
- Prepare; and
- Prevent.

Prevent aims to stop people becoming involved in violent Extremism. The Prevent Strategy responds to the ideological challenge of Terrorism and aspects of Extremism, and the threat from those who promote these views. It provides practical help to prevent people from being drawn into Terrorism and ensure they are given appropriate advice and support.

The national Prevent Strategy has three specific strategic objectives:

- **Respond** to the ideological challenge of Terrorism and the threat faced from those who promote it.
- **Prevent** people from being drawn into Terrorism and ensure that they are given appropriate advice and support.
- **Work** with sectors and institutions where there are risks of Radicalisation that need to be addressed.

The Prevent Duty incorporates the responsibility to promote fundamental British Values (as identified by Ofsted):

- Democracy;
- The rule of law;
- Individual liberty; and

- Mutual respect and tolerance of those different faiths and beliefs.

The Prevent Duty covers all forms of Radicalisation, including risk from extremist faith groups, far right Extremism and some aspects of non-violent Extremism. There are different forms of extremist organisations in the UK and the world, including:

- British Defence League;
- Islamic State;
- Al-Qaeda;
- Boko Harram;
- SPEAK (animal rights);
- Irish Republican Army ("**IRA**"); and
- Anti-abortion groups.

Identifying an individual who is being exploited or Radicalised can often be difficult as there is no single factor that leads to an individual being Radicalised. The signs and indicators listed below are not exhaustive and the presence of one of these factors does not necessarily mean that an individual is or has been Radicalised or is involved in Extremist activity. However, a combination of these factors may increase Vulnerability or may indicate that an individual needs protection and/or support.

Safeguarding from Radicalisation is no different to protecting individuals from other forms of harm.

The following factors can make an individual increasingly **Vulnerable** to Radicalisation and Extremism:

- **Identity crisis:** distance from cultural or religious heritage and uncomfortable with their place in the society around them.
- **Personal crisis:** family tensions or trauma, sense of isolation, adolescence, low self-esteem, disassociating from existing friendship group and becoming involved with a new and different group of friends, searching for answers to questions about identity, faith and seeking a sense of belonging.
- **Unmet aspirations:** perceptions of injustice, feeling of failure, rejection of civic life.
- **Experienced personal trauma,** particularly any trauma associated with war or sectarian conflict.
- **Personal circumstances:** migration, local community tensions, events affecting country or region of origin, alienation from UK values, having a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of government policy.
- **Criminality:** experiences of imprisonment, poor resettlement or reintegration or previous involvement with criminal groups.
- **Experience** of poverty, disadvantage, discrimination or social exclusion.
- **Learning difficulties** and mental health support needs.

The following **behaviours** could indicate that an individual has been Radicalised:

- Using violent extremist narratives and ideology to explain personal disadvantage.
- Justifying the use of violence to solve societal issues.
- Significant shift in behaviour or outward appearance that suggests a new social, political, or religious influence.
- Conflict with family over religious beliefs, lifestyle or dress choices.
- Vocal support for terrorist attacks (either verbally or written).
- Witnessed or been the perpetrator or victim of racial or religious hate crime.
- Travel for extended periods of time to international locations known to be associated with extremist groups and activity.
- Significant changes in emotional behaviour, for example, becoming withdrawn or angry.
- Ignoring or demonising viewpoints that contradict their own.
- Expressing themselves in an 'us versus them' manner about others who have alternative beliefs.
- Increasingly secretive or unwilling to discuss views.
- Changing their circle of friends.
- Losing interest in activities they once enjoyed.
- Becoming socially withdrawn or spending a lot of time online.
- Secretive about who they talk to online and which websites they visit.
- Belief in conspiracy theories and distrust of mainstream media.
- Justifying the use of violence or expressing a desire for revenge.
- Sharing of views or trying to influence others with extremist Ideology.

The following may demonstrate that an individual has **access** to Extremism or Extremist influences:

- Association with extremist groups, associates or family engaging in Extremist activity.
- Accessing the internet for the purpose of Extremist activity, for example, use of closed network groups, access to or distribution of Extremist material, contact associates covertly via online measures, for example, Skype and email.
- Possesses or is actively seeking to possess and/ or distribute Extremist literature or other media material likely to incite racial, religious hatred or acts of violence.
- Support for groups with links to Extremist activity, for example, propaganda distribution, fundraising and attendance at meetings.
- Extremist ideological, political or religious influence from within or outside UK.

## Reporting concerns of Radicalisation and Extremism

Staff must report all concerns relating to Radicalisation and/or Extremism to the Safeguarding Team immediately and within 24-hours.

If the concern represents an immediate threat or risk, then Staff must (in addition to reporting the concern to the Safeguarding Team) contact:

- Police: 101 (999 in an emergency)
- Counter Terrorism Police: https://actearly.uk/contact/
- Report online material promoting Terrorism or Extremism: https://www.gov.uk/report-terrorism

### Risk Assessment and Action Plan

The Club will undertake a risk assessment of where and how individuals might be at risk of being drawn into Terrorism. The level of risk will vary between activities, geographical location, and profile of participants.

The risk assessment will consider information from external sources, such as the regional Prevent Co-ordinator, Local Authority and the Police.

The resulting Prevent Action Plan will mitigate the risks in a proportionate manner. The Club's Prevent Action Plan will be regularly monitored by the Head of Safeguarding and Welfare.

Where significant risks are identified, the Head of Safeguarding and Welfare in collaboration with senior managers, will consider what action might mitigate the impact/likelihood of that risk evolving and, where necessary, include it on the Prevent Action Plan.

All Staff in regulated activity will complete a biannual "Raising Awareness About Prevent" training. Staff must also complete the online Prevent training as part of their Club induction.

### Reporting Extremist narratives or Radicalisation Concerns

All Staff have a Duty of Care to report and escalate concerns using the Club's safeguarding reporting process.

For more information, see: https://www.gov.uk/government/publications/channel-guidance

## Additional Risks

Below some of the risks associated with Online Spaces are outlined in more detail.

### Social Media Risks

| | |
|---|---|
| Catfishing | is when someone assumes the identify of another person to harass, intimidate, threaten or defraud an individual or gain financial or social benefits and/or to embarrass or humiliate that person. |
| Cyberbullying | means bullying that takes place in Online Spaces which is intended to harass, threaten or intimidate someone and includes sending, posting, or sharing negative, harmful, false, or hurtful content about someone, impersonating someone and sending messages to others, sharing personal or private information about someone causing embarrassment or |

| | |
|---|---|
| | humiliation, and leaving negative comments or reactions about their performance or achievements.<br><br>Cyberbullying can often take place alongside face-to-face bullying. However, Cyberbullying is often done anonymously which can create a feeling of helplessness and increased dread in a victim.<br><br>Cyberbullying can sometimes become unlawful or criminal behaviour. |
| Harmful content | includes exposure to the following violence, sexualised content, misinformation/fake news, racism, misogyny, disablism, self-harm, suicide, pro-suicide content, antisemitism, radicalisation and extremism, harmful challenges and hoaxes, violence, inciting violence, cruelty to humans and animals, pornography, glorifying activities such as drug taking, sexual abuse and rape.<br><br>Exposure to this content can happen through active searching or accidental exposure via Social Media and pop ups. This can be monitored and controlled through the parental settings on most devices and Social Media. |
| Harmful online challenges | means online trends where people take part in or mimic games, activities, skits or dares, which can sometimes be dangerous.<br><br>Dangerous challenges could result in serious physical injury, permanent harm and some can be fatal. Online hoaxes (sometimes known as pranks or scams) are deliberate lies designed to seem truthful. They can sometimes be quite extreme and are designed to be frightening and traumatic which can have a negative impact on mental health. Some hoaxes direct viewers to carry out harmful activities, self-harm or suicide. |
| Inappropriate content | means the sending or sharing of content that could be harmful to an individual or others. This could be in the form of sexting or sharing memes and images of others without their consent.<br><br>Individuals can be pressured or coerced into sharing content of this type, sometimes without knowing the harm it may cause or the risks involved. |
| Harmful online communities | means a virtual community whose members interact with each other primarily via the Internet, sometimes these communities can be highly dangerous especially if they intend to cause harm. |
| Oversharing | means disclosing personal information through posts or profile information on Social Media, for example about an individual's home life, thoughts and feelings, live or frequent locations or other people's personal information. Particular care should be taken when sharing photographs of Children which may disclose school uniform badges etc.<br><br>This information may make someone identifiable which perpetrators can then use to groom, Abuse or exploit individuals. |

| | |
|---|---|
| Social Media addiction | shows itself through obsessive focus on likes and comments which can leave individuals feeling as though they aren't good enough or as popular as someone else.<br><br>Social Media algorithms offer extreme content, both positive and negative, showing users other people "living their best life" and popular accounts which will leave users feeling inadequate and unpopular. |
| Unrealistic body image/reality | is a result of the pressure to conform to the 'ideal' body and lifestyle creating a negative body image by being overly focussed on comparison to unrealistic ideals. This can include an include obsessive focus on likes and comments on their posts which can leave them feeling that they aren't good enough or not as popular as someone else.<br><br>Social Media is designed to stimulate dopamine hormone in humans meaning that users experience powerful emotions when viewing content, receive notifications or communicating on the platform. This leads to a dependency on certain platforms, to alter mood, escape from difficult moments or unhappy times in their life, which, in turn, becomes an addiction. These are not healthy escapes, however, and overuse of social media leads to a negative mental and physical health impact and, particularly, a negative impact on sleep and concentration. |

## Other Risks

| | |
|---|---|
| Online stalking | can be facilitated by the use of Social Media, including malware and spyware which can enabled the consensual or non-consensual tracking of locations putting individuals at risk. |
| Revenge Porn | is where an abuser humiliates, extorts or harasses a former sexual partner or someone else that they have targeted by hacking into an online account such as an iCloud or Social Media account, or through sexual images shared whilst in a relationship.<br><br>The perpetrator exacts the crime by sharing, or threatening to share, intimate images, or videos, of them online without consent. This is an extension of coercive and controlling behaviour and stalking, which can both represent significant risks to victims. |
| Social Engineering | means all video deep fakes, voice cloning, romance scams and emotional manipulation. |
| Solicitation | is a technique to convince a recipient to open a line of communication with the sender which could lead to a transfer of monies or a backdoor to compromise the Club's Devices or IT infrastructure. |

# Good Practice when operating in Online Spaces

The Club recognises that increasingly learning activities and communication will take place in Online Spaces and therefore, it is important that Staff engaging in Online Activities follow the Policy as set out below.

## Online Activities

Staff will ensure that any Online Activities are delivered with the prior knowledge and agreement of the Club via the normal management structures.

The Safeguarding Team should be included at the early stages of planning any Online Activities to identify and mitigate safeguarding risks prior to the Online Activity being delivered and to ensure adequate resources are allocated to safeguarding and welfare for all Online Activities.

Staff must ensure that Online Activities provide a safe environment and prioritises participant enjoyment, safety and wellbeing:

- Staff should introduce the Online Activity by setting ground rules explaining:
    - when participants can speak/contribute;
    - how participants can speak/contribute;
    - how participants should interact with others.
    - how they should present and conduct themselves if participant cameras and/or microphones are permitted during the Online Activity; and
    - reminding participants how to report concerns and access support.
- Staff should always challenge offensive, abusive or Bullying behaviour and adhere to Club policies, procedures and Code of Conduct.
- Staff must report any incidents of Bullying and safeguarding concerns (including Child-on-Child/peer-on-peer) and reported and recorded in line with the Club's policies and procedures.

## Communication

Staff must ensure that personal data is never processed without the full and prior knowledge and agreement of the Club, including images and recordings. This includes the recordings of Online Activities.

Staff must restrict external online communication to Club-Sanctioned Engagement Platforms. Any direct online communication by Staff to Children must also be sent to parents.

Staff must only use Club Devices and accounts to deliver Online Activities or communicate with Children and Adults at Risk via Club-Sanctioned Engagement Platforms.

Staff must never use their Personal Devices to contact Children or Adults at Risk who have been involved in Club Activities.

Staff must work in partnership with the Safeguarding Team to agree the appropriate level of parental/carer involvement in each Online Activity.

Staff should provide all participants in Online Activities with information about the Online Activity and participation in literation/invitations, including:

- how to access or join the Online Activity;
- what to expect and how the Online Activity will run or be delivered; and
- participation instructions, for example, to participate from communal areas rather than bedrooms, what will and won't be permitted, expectations of participants, how to seek advice or raise concerns.

## Online Meeting Platforms

Staff should ensure that they abide by the following when using Online Meeting Platforms:

- Where Staff access Online Meeting Platforms from a personal space, they must ensure that the background is neutral where nothing personal or inappropriate can be seen or heard in the background. Staff should always consider what is visible if the Online Activity will involve sharing a screen, for example, desktop files, social media accounts, personal information or emails.
- Staff must use secure internet connections during online communications.
- Staff must always familiarise themselves with Club-Sanctioned Engagement Platform's privacy settings ensuring they are applied correctly.
- Staff must work in partnership with the Safeguarding Team to establish appropriate Online Activity supervision and ratios, for example, how platform breakout rooms will be supervised. The appropriate ratios will be decided on a case-by-case basis.
- Staff must ensure that Online Meeting Platforms are set up to prevent unauthorised access.
- Staff must ensure that the Online Meeting Platform is secure and that safety settings have been applied, for example:
    - Setting up a 'waiting room/participant lobby' to ensure only invited participants join.
    - Ensuring participants are unable to communicate with one another within the Online Meeting Platform before or after the Online Activity or without Adult supervision.
    - Allowing or preventing the sharing of content by participants.
    - Allowing or preventing participant cameras to be turned on. Consideration should be given to whether Children and Adults at Risk are comfortable turning their camera on. Some participants may be unfamiliar with technology use, may have had a bad experience using video calls or attempt to hide abuse or neglect.
    - Allowing or preventing participant microphones to be turned on.

## Social Media

Despite the risks, Social Media can offer Children and Adults at Risk valuable opportunities to develop skills and build a good digital footprint. There are lots of benefits when using Social Media, for example, staying connected with friends and family, enabling innovative ways of learning and providing ways for individuals to express themselves. Please see the Club's Social Media and Blogs Policy for further details.

### Official Club social media accounts

Club-sanctioned communications via Club Channels are managed via the PR, Communications and Marketing teams.

For employees whose role requires the use of Social Media to make statements or communications on behalf of the Club, a member of the Board, Head of PR, Director of Communications or Director of Marketing must first approve the communication before it is published. Any question sent to a Staff Social Media by a media outlet or journalist should be referred to the communications department.

No member of Staff should make comments or answer questions to any media outlet on behalf of the Club, without proper authority to do so.

### Personal use of social media

Staff should be mindful of any personal use of Social Media and the content they post.

Even in the members of Staff's personal lives, Staff are Club ambassadors. That is particularly the case where Staff identify themselves by their full names on social media but, given the high-profile nature of the Club, Staff must accept that it is always possible that they will be identified and/or connected to the Club in Club activities. What Staff post as individuals can affect how the Club is viewed, by association, and pose risk of reputational damage to both you and the Club.

The Club strongly advises that Staff do not use Club logos within their profile photos or avatars, Staff can mention that they work with the Club in Social Media bios so long as it is made clear that it is a personal account and that all views expressed are their own and not those of the Club. Please see the Club's Social Media Policy for further details.

A good rule of thumb is to always be respectful and non-confrontational on Social Media. If in doubt, speak to your line manager or HR.

Staff may use Social Media for personal purposes during working hours, under the following conditions:

1. It is not used to share or view unprofessional or inappropriate content or anything which is likely to bring you or the Club into disrepute or negatively impact the Club or its Staff.

2. It is not used to share anything which is confidential to the Club or private to any other Staff or related third parties.

3. Social Media does not cause disruptions or distractions, such that there is interference with Staff employment, responsibility or productivity; and

4. Social Media use is compliant with this Policy and the Social Media Policy, a copy of which can be found on The Shelf.

Failure to follow this Policy could result in disciplinary action.

## Live Streaming and recording activities

Live Streaming has two available options:

- public streaming channels are areas of services where content is visible to the general public/any other user; and
- private channels are services with more privacy, such as private messaging or closed groups.

Live Streams can also occur in private one-on-one chats, which cannot be viewed by others. This type of broadcast cannot be cut or edited meaning the content is uncensored, unmoderated and can expose individuals to inappropriate content or damaging comments.

Staff should take great care before engaging in any form of Live Stream or recording activities and be aware of how this Policy applies to such activity.

## Images of Children & Adults at Risk

Any use of images of Children and Adults at Risk, will be used in accordance with the Data Protection Act 2018, and will be agreed with a parent/carer via consent forms, agreed via the Club's Legal Team.

Teams taking photographs of Children or Adults at Risk will plan ahead of time to ensure that appropriate consent is sought, and that families and individuals understand the Club's copyright, planned usage, and retention times, associated with the images taken. If you are aware of any Event that will involve images of Children and/or Adults at Risk please contact the Legal Team with as much notice as possible to arrange for consent forms.

Any images of Children or Adults at Risk used by the Club will only be published alongside Children's or Adults at Risk's first names, and no personal information about the individuals or their families will be revealed. This is subject to the exception of players selected to play for the club's first teams, under 18s or under 21s teams where players (who are still defined as Children) will be named in match reports, teamsheets and other media with the consent of their parents.

There may be reasons, safeguarding and otherwise, why individuals do not wish to have their photographs published. The Club will respect these wishes.

# Acceptable Use

The Club always expects all Staff and Visitors to any of the Club Premises, at any time, to follow this Policy when using both Club-owned electronic equipment ("**Club Devices**") and personally owned electronic equipment ("**Personal Devices**"). All Staff and Visitors should be aware of the expectations around acceptable use of Social Media and technology upon arrival on Club Premises.

## Club Devices

The Club issues and provides Club Devices, including mobile phones and laptops, for Club-related activities including work, training, and official trade union business. Club Devices can be used for limited personal use. The Club asks that all Staff using Club Devices operate such Club Devices responsibly.

## Personal Devices

Staff must also be mindful when using Personal Devices on Club Premises and while conducting work on behalf of the Club.

## Prohibited Locations

### The Training Centre

Photography is not permitted anywhere by Staff, Visitors and Players at the Training Centre, without prior agreement. Any requests for authorisation should be made to the Head of Football Communications in advance of any activity taking place. The only type of filming or photography that is likely to be authorised is partner filming, players appearances, team training, content capture, interviews etc.

*NB: Please note, if the Training Centre operations team are not made aware of the filming or photography in advance of the activity the filming or photography will be classed as unauthorised.*

The use of Personal Devices is restricted at the Training Centre due to the presence of Children and Players. Whilst Staff and Visitors are entitled to make telephone calls, send messages and send emails whilst at the Training Centre, they must **not** take photographs, recordings or divulge private or confidential information relating to Children and/or Players unless done in the course of their employment and with the authorisation of the Club.

The use of any Personal Devices is prohibited in the canteen areas at the Training Centre.

### The Stadium

No images or recordings of Events can be shared, streamed or published on Online Spaces.

Neither Personal nor Club Devices can be used for photography, recording, filming or any other similar use (or in any way that can be construed as being used for the aforementioned purposes in any of the Stadium's Back of House areas.

All Staff should abide by the Ground Rules at all times, which can be found on The Shelf.

## Prohibited Contexts

When undertaking work on behalf of the Club in Child- and Adult at Risk-facing roles, Staff should ensure that they use Club Devices at all times.

The use of Personal Devices is not permitted in the presence of:

- any Child or Adult participant in activities run by the Foundation;
- any player in the youth development phases in activities run by the Club's Academies;
- any participant/student in activities run by Global Football Development); or
- any Players.

For this reason, Personal Devices should be stored in bags, coats in all of the above situations, including off-site.

## Prohibited Activities

No Staff, Player, parent/carer, or Visitor must knowingly use devices or online spaces to:

- insult, harass, threaten or deceive other people;
- act in any way which brings the Club or its Staff into disrepute;
- request, create, access, store or send offensive, pornographic, indecent, illegal or prohibited material;
- breach copyright or licence agreements;
- connect unauthorised devices to Club Devices or networks;
- connect Club Devices to unauthorised computers;
- download, use, store or distribute software or an application that is unauthorised, not accredited for the system you are using or which is not for a justified business purpose;
- remove, disable, nullify or modify operational components, safety or security measures in Club Devices;
- try to misuse, gain unauthorised access to, or prevent legitimate access to, any ICT equipment, network, system, service or account;
- try to gain unauthorised access to, or conceal without authority, information, or release information without proper authority;
- bring the Club into disrepute or obstruct its business;
- be negligent in protecting the ICT and services, or the information you can access from it; and/or
- break the law.

## Risk, Compliance & Data Protection

The Clubs holds a variety of sensitive data including personal information, which may include:

- personal data of Staff, Players, Visitors and Spectators;
- medical information;
- protected characteristic data; and
- bank information.

If you have been given access to this information, you are reminded of your responsibilities under Data Protection Laws. You should only take a copy of data outside of Club Devices if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, memory sticks, CDs/DVDs, and any portable media or into emails. If you do need to take data outside the Club, this should only be with the authorisation of the appropriate management structures.

Sensitive or personal data should not be left in printers or displayed on monitors or be in any way easily viewable by others when away from the desk.

Sensitive information should only be given to authorised personnel e.g. passwords, user accounts and confidential documents stored in computer files.

Staff should ensure that sensitive data, both paper and electronic, is disposed of properly e.g. destroy disks, shred paper.

If you have any questions about data protection, please contact the Risk, Compliance and Data Officer. The role of the Risk, Compliance and Data Officer is to understand:

- what information is held and for what purposes;
- how information has been amended or added to over time; and
- who has access to protected data and why.

### System Security

All Staff using Club Devices should abide by the following principles:

- Staff must not make, distribute or use unlicensed software or data.
- Staff must not make or send threatening, offensive or harassing messages.
- Staff must not create possess or distribute obscene material.
- Staff must ensure they have authorisation before any private use of the Club's computer facilities.
- Staff passwords should not be revealed to unauthorised persons.

- Passwords should not be obvious or guessable and complexity should reflect the value and sensitivity of the systems and data.
- Passwords should be changed if a suspected breach of security has been noted e.g. an unauthorised person accessing a security password.
- Regular backups of important data should be made e.g. office data, staff data, policies etc.
- To help maintain security of personal and sensitive data, encryption should be used if held on a mobile device that leaves the Club Premises.
- If Staff believe that they have received a suspicious message, have been targeted by malware or similar or suspect that there has been a breach of security they must inform IT Service Desk immediately.

### Virus Protection

The IT technician will ensure current and up to date anti-virus (AV) software is applied to all Club Devices and systems where appropriate. Network machines will receive regular updates of AV protection files via the county set up. All Staff should take precautions to avoid malicious software that may destroy or corrupt data e.g. checking all incoming email attachments or internet downloads and should be made aware of how to recognise and handle email hoaxes. On notification of the need for a critical security patch, these will be applied by the IT Department.

## Personal use of Club Devices

The Club monitors its networks, so if Staff don't want the Club to see your private information, they should only use Club Devices for work.

Club email addresses should only be used for purposes related to the role of Staff.

Club Devices may only be used for personal calls on the following occasions:

- in an emergency;
- if you need to change personal arrangements because of unexpected work commitments;
- if you are away from your normal place of work and it's not practical to wait until you return home (calls within the UK only, and keep them brief); and
- for inbound personal calls (however, Staff are encouraged to keep these brief).

When making personal use of Club Devices, Staff must not:

- take part in personal commercial activity, including, but not limited to, single, network, direct referral, or multilevel marketing;
- undertake any form of share-dealing;
- undertake any form of crowdfunding or raise funds for individuals or charities, not formally supported by the Club;

- take part in any gambling or lottery, with an express prohibition of gambling relating to football;
- take part in petitions, campaigns, politics or similar activity; or
- waste Club time, money or resources.

The Club does not accept any liability for any loss, damage or inconvenience that any Staff may suffer as a result of personal use of Club Devices.

## Monitoring of Club ICT

The Club monitors Club Devices and systems to help protect its information the integrity of its Devices and online security. Any personal data collected during monitoring will only be used for the purpose for which it was gathered, and any further processing will be in accordance with Data Protection Laws.

# Acceptable Use: Under 18's

The Club deploys URL filtering on all web traffic, advanced threat protection, endpoint security and access control lists. All connections are logged and monitored. This works by means of a 'disallowed' list, so that inappropriate sites are filtered before they get to Club Devices.

The Club will ensure that filtering and monitoring systems reflect and adapt to changes in platforms, apps, smart and mobile technology with effective reporting by actively reviewing filtering and monitoring system reports and responding swiftly and appropriately to identified procedural breaches and safeguarding concerns.

GoBubble has been implemented to monitor social channels and in future will provide monitoring and blocking on Club owned channels. This tool uses live AI monitoring to filter out harmful content before it can be seen, this includes text, emoji, image and video monitoring.

## Review of content

All filters used by the Club will notify the Safeguarding Team if certain terms are searched for on Club Devices.

Once concerns are flagged and reviewed, if the searches or access is of concern, the Safeguarding Team will notify relevant managers and parents/carers.

## Under-18s' Personal Devices

Under-18s are asked not to use their Personal Devices whilst at the Training Centre, other than in the Academy Reception area, outside of start and finish times. Exceptions can be made by coaches, given appropriate circumstances.

## Social media support

Under-18s in youth development are given social media courses and, once players turn 18, they are offered Go Bubble protection.

## Under-18s' Email Accounts

Children's email accounts, where provided by the Club, are secure and monitored.

# Reporting

## Report a breach of this Policy

If Staff are aware of any breach of this Policy from a reporting or regulatory perspective (for example, a breach of the acceptable use section of this Policy), this should be reported to their line manager, with a copy to the HR Team and the Legal Team, as soon as practicable.

If Staff are concerned about any breaches of this Policy in relation to Abuse or Child Sexual Exploitation, this should be reported as a safeguarding concern (see below).

## Report a safeguarding concern

Any concerns relating to the online safety and wellbeing, Abuse or Child Sexual Exploitation of Staff, a Player, a Child, an Adult at Risk, a Visitor, or parent/carer this should be reported directly to the Head of Safeguarding & Welfare immediately, or in any event within 24 hours (with a copy to the Safeguarding Team).

The Safeguarding Team will act to investigate the concern and report it to the appropriate authorities if necessary.

## Report Child Sexual Exploitation

If you have any concerns about potential or actual Child Sexual Exploitation at the Club, please report these immediately but in any event with 24-hours to the Safeguarding Team.

**All forms of Child Sexual Exploitation or Abuse should be reported to the local police force as soon as possible.**

This includes, but is not limited it:

- The sharing of Child Sexual Exploitation and Abuse content, for example images, videos and streaming.

  *NBV: please note that you should **not** send indecent images of Children as part of the report to the police.*

- Sexual contact between Adults and Children, for example requests to form sexual acts on camera or send sexual images, or arrangements to meet.

- Contact between Adults relating to Child Sexual Exploitation or Abuse of Children, for example advertising or acquiring Children for sex, or offers to share images or livestreams of Abuse.

## Report harmful content

Report Harmful Content is a national organisation which aims to assist the reporting harmful content online. Their services can be found at https://reportharmfulcontent.com/ or for Child-specific advice, please see https://reportharmfulcontent.com/child

Report Harmful Content has two main functions:

- **Advice**:
  Empowering anyone who has come across harmful content online to report it by providing up to date information on community standards and direct links to the correct reporting facilities across multiple platforms.

- **Reporting**:
  Providing support to Children over the age of thirteen who have already submitted a report and would like outcomes reviewed. Report Harmful Content will check submitted reports and industry responses against platform-specific reporting procedures and community standards in order to provide users with further advice on actions they can take.

# Appendix 1: External Contacts

| **Organisation** | **Contact details** |
|---|---|
| Action Counters Terrorism | Online content that supports, directs or glorifies terrorism should be reported to Action Counters Terrorism: https://act.campaign.gov.uk/. |
| Barnet Mash and LADO | MASH: 020 8359 2000.<br><br>Barnet's LADO should be contacted via the Multi Agency Safeguarding Hub (MASH) Team. |
| Camhs – Barnet | 020 8702 4500.<br><br>Mental Health crisis helpline: 0800 151 0023 |
| Camhs – Enfield | 020 8702 4070.<br><br>Mental Health crisis helpline: 0800 151 0023 |
| Camhs – Haringey<br><br>(Child and Adolescent Mental Health Service) | 020 8702 3400/3401.<br><br>Mental Health crisis helpline: 0800 151 0023 |
| Camhs – Waltham Forest | Contact: 0300 5551247 / walthamforest@camhs@nhs.net |
| CEOP | CEOP is a command of the National Crime Agency and works to pursue and prosecute child sex offenders. Children, their parents/carers and those working with Children can access advice or report a concern about child sexual abuse or grooming online to CEOP: https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/. |
| Childline | 0800 1111 / WWW.CHILDLINE.ORG.UK |
| CPSU | 0116 636 65580 / WWW.THECPSU.ORG.UK |
| Enfield Mash and LADO | MASH: 020 8379 5212<br><br>LADO: 0208 379 4392 / safeguardingservice@enfield.gov.uk |
| Enfield PREVENT | Email: prevent@enfield.gov.uk / Sujeevan.Ponnampalam@enfield.gov.uk |
| Haringey Mash<br><br>LADO | MASH: 020 8489 4470 / mashreferral@haringey.gov.uk<br><br>LADO: 020 8489 2968/1186 / LADO@haringey.gov.uk |

| | |
|---|---|
| Haringey PREVENT | Call 020 8489 3884 / 020 8489 1280<br><br>prevent@haringey.gov.uk<br><br>Karina Kaur – Strategic Lead of communities - 07976953191 |
| Internet Watch Foundation (IWF) | Child sexual abuse images or videos online can be reported anonymously to the IWF: https://www.iwf.org.uk/report/.<br><br>Reports to the IWF are accepted as reports to a relevant authority in accordance with a Memorandum of Understanding between the Crown Prosecution Service and the Association of Chief Police Officers.<br><br>The IWF and NSPCC have developed the Report Remove tool to support Children with reporting and removing sexual images or videos of themselves shared online and enables them to get the image removed if it is illegal: https://www.iwf.org.uk/our-technology/report-remove/. |
| NSPCC | Contact: 0808 800 5000 / WWW.NSPCC.ORG.UK |
| Premier League Safeguarding Team | Jess Addicot (Head of Safeguarding): 07917 204890 or 0207 864 9000 or email jaddicot@premierleague.com or safeguarding@premierleague.com |
| Report Harmful Content | Information for adults: https://reportharmfulcontent.com/<br><br>Information for Children: https://reportharmfulcontent.com/child |
| Revenge Porn Helpline | For victims of Sextortion, Revenge Porn and/or Intimate Image abuse the Revenge Porn Helpline offers practical advice and support.<br><br>https://revengepornhelpline.org.uk/ |
| The Football Association | David Gregson (Safeguarding Investigations Manager): 0800 1691863 extension 6838 / david.gregson@TheFA.com |
| Waltham Forest Mash and LADO | MASHrequests@walthamforwest.gov.uk<br><br>LADO: 020 8496 3646 / 07791 559 789 / lado@walthamforest.gov.uk |

# Appendix 2: Further Information

| Organisation | Website |
|---|---|
| Ann Craft Trust | https://www.anncrafttrust.org/category/digital-safeguarding/ |
| Ann Craft Trust How to Stay Safe Online | https://www.anncrafttrust.org/how-to-stay-safe-online-guidance-for-adults-and-young-people-with-learning-disabilities/ |
| CEOP Thinkuknow | https://www.thinkuknow.co.uk/professionals/ |
| CEOP Thinkuknow 4-7-year olds | https://www.thinkuknow.co.uk/4_7/ |
| CEOP Thinkuknow 8-10-year olds | https://www.thinkuknow.co.uk/8_10/ |
| CEOP Thinkuknow 11-18-year olds | https://www.thinkuknow.co.uk/11_18/ |
| Department for Education - Teaching Online Safety in schools | https://www.gov.uk/government/publications/teaching-online-safety-in-schools. |
| Department for Education - Harmful online challenges and online hoaxes | https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes. |
| Educate Against Hate | https://educateagainsthate.com/ |
| HM Gov - UK Council for Internet Safety: Online Safety in schools and colleges | https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1105569/Online_safety_in_schools_and_colleges.Questions_from_the_Governing_Board__2022_.pdf |
| HM Gov - Guidance on responding to incidents and safeguarding children and young people | www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people. |
| HM Gov Guidance | https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing- |

| | |
|---|---|
| | nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people. |
| HM Gov - Safeguarding and remote education | https://www.gov.uk/guidance/safeguarding-and-remote-education |
| Ineqe Safeguarding Group - Guidance on delivering secure lessons | https://ineqe.com/2021/01/28/secure-lessons/ |
| Ineqe Safeguarding Group - Social media and apps | https://ineqe.com/online-safety/social-media/ |
| NSPCC - Social media and Online Safety | https://learning.nspcc.org.uk/safeguarding-child-protection/social-media-and-online-safety. |
| NSPCC Keeping Children Safe Online | https://www.nspcc.org.uk/keeping-children-safe/online-safety/ |
| NSPCC CPSU - Online safety | https://thecpsu.org.uk/help-advice/topics/online-safety#creating-a-safer-online-environment |
| NSPCC - Sexting advice for professionals | https://learning.nspcc.org.uk/research-resources/briefings/sexting-advice-professionals |
| NSPCC - Undertaking remote teaching safely | https://learning.nspcc.org.uk/news/covid/undertaking-remote-teaching-safely#skip-to-content |
| Online Safety Guidance and Advice Clubs Premier League | https://www.premierleague.com/safeguarding |
| Ofsted - Remote education research | https://www.gov.uk/government/publications/remote-education-research/remote-education-research |