Social Media Advice for Athletes

Introduction

This guide contains suggestions on how to keep yourself safe online. We want you to use social media to talk about athletics and have a positively experience when you do, and we can help you think about the possible advantages and pitfalls offered by social media.

In athletics there are rules for everyone about what is and isn't acceptable online behaviour. So as an athlete we ask that you please,

- be responsible for your behaviour when using your smart phone at your club and follow the rules on using it set by your coach/club.
- avoid using your smart phone during club activities such as training as that will have an impact on my safety and my opportunity to learn and achieve.
- not send anyone else in athletics material that could be considered threatening, offensive, upsetting, bullying or that is illegal.
- understand that your club staff, volunteers, and coaches should not contact you online on a one-to-one basis unless it's an emergency.
- understand that all your use of internet and social media is potentially visible to everyone and that any issues involving your behaviour online may be addressed by your club.
- not give out any of your personal information (such as name, age, address or telephone number) online, or that of anyone else.
- not share my passwords with anyone else.
- not arrange to meet someone that I have met online unless accompanied by your parent or a carer.
- contact your coach or club welfare officer if you are experiencing bullying behaviour or abuse online.

Staying safe online.

Think before you post.

Don't upload or share anything you wouldn't want your parents, carers, coaches or even future employers seeing. Once you post something, you lose control of it, especially if someone else screenshots or shares it.

Don't share personal details.

Keep things like your address, phone number, full name, school and date of birth private, and check what people can see in your privacy settings. Remember that people can use small clues like a club or school logo in a photo to find out a lot about you.

Watch out for phishing and scams.

Phishing is when someone tries to trick you into giving them information, like your password. Someone might also try to trick you by saying they can make you famous or that they're from a talent agency. Never click links from emails or messages that ask you to log in or share your details, even if you think they might be genuine. If you're asked to log into a website, go to the app or site directly instead.

Think about who you're talking to.

There are lots of ways that people try to trick you into trusting them online. Even if you like and trust someone you've met online, never share personal information with them like your address, full name, or where you train or go to school.

Keep your device secure.

- Make sure that you're keeping your information and device secure.
- Never give out your password
- You should never give out your password or log-in information.
- Make sure you pick strong, easy to remember passwords.

•

Cover your webcam.

Some viruses can let someone access your webcam without you knowing, so make sure you cover your webcam whenever you're not using it.

When things don't go as planned online.

It can and does happen that things said or done online can get out of hand.

If you are receiving upsetting messages or replies, the best response is often no response. Tempting as it is to reply, that can sometimes escalate the situation. Best to step away from your phone or computer and let off steam to a friend or family member instead.

If you are receiving messages that are threatening, offensive, upsetting, or that might be illegal then report this to your parent or carer, or another trusted adult immediately. Take screen shots of the messages wherever possible and block the abuser.

If the person sending the abusive messages is involved in athletics this should be reported to the UKA safeguarding team on safeguarding@uka.org.uk.