CRICKET VICTORIA

CHILD SAFETY FRAMEWORK USER GUIDE

eSafety Guide to Keeping Kids Safe
June 2020

The following Child Safe resource is provided as a reference only.

This document and its content is provided as a guide for your organisation as of July 2020. Your organisation should also consider referencing any information, documents and strategies that might be specifically required for your organisation and relevant to its circumstances, structure and operations.

The information contained in this document is general in nature and should not be considered or relied upon as a substitute for legal advice.

Please note that references in [square brackets] throughout this document should be tailored for your organisation's policies and procedures.

Cricket Victoria recommends using this resource with due consideration and consulting a child safe expert or legal advisor to assist with any questions.

In a global and domestic context that is increasingly reliant on online connection and education, the safety of our children in the sporting cyber world is now more critical than ever. This resource collates extracts and provides adaptations of some of the more practical and specific eSafety tips for:

- Parents
- Children and Young People
- Sporting Organisations/Clubs when delivering online training or forums for children and young people.

1. Types of Online Risks

Being online these days is complex – for many of us. The sheer number of apps, sites, connection forums and platforms is immense. Parents, educators and those running clubs or sporting organisations are navigating this web for themselves, and also for their kids. There is a lot to digest.

Online activity has the potential to result in harm and/or abuse to children such as:

- Cyberbullying;
- Grooming;
- Exposure to, or engagement with, pornography or sexually explicit images;
- Privacy breaches; or
- Scams targeting children.

While abuse to children occurring in the physical world is more often than not perpetrated by people that children know and trust, in the online world, it is the opposite – the overwhelming majority of abuse is perpetrated by people that children do not know.

According to *Australian Cybersafety expert Susan McLean, 80% of online abuse also has an offline component. These days, kids can be on a number of online platforms that heighten the risks of harm or abuse to children, including:

a) Social Media – eg, Facebook, Instagram, Snapchat, Houseparty, TikTok;

b) Games – eg, Fortnite, Minecraft;

c) Chat rooms/apps or Bulletin Boards – eg, WhatsApp, Facebook Messenger;

d) Email; and

e) Video messaging and conferencing services – Zoom, GoToMeetings, Facetime.

2. Mitigating the Risks

There are a number of things that can be done to reduce online risks for children. They include:

a) **Education** - as to the risks, indicators of harm, the cyber world generally, child safeguarding policies and procedures, as well as strategies available, such as online controls.

b) **Ongoing communication** – normalising discussion about the online world, risks and strategies by keeping open lines of communication.

c) **Accessing resources –** finding and using the best resources for your organisation.

d) **Implementing controls, policies and strategies to reduce risks –** ensuring that any club/organisation-based platforms are "filtered" to be as safe as possible and that policies exist to guide online communication with kids.

e) **Responding to and reporting actual or potential risks of online harm to children** – knowing what to do if dangers or harm arises and who to report it to.

Susan McLean (Child Safe Australia), 2020,* **Interview and Q&A with Susan McClean (webinar)

eSafety Tips for Parents & Guardians
Victoria Police Online Safety Advice Extract

1. Steps for improving your child's safety:
    a) Be aware of the programs and files children use.
    b) Consider installing filtering software on computers used by young people.
    c) Be aware of the programs and files that are on your family's computers.
    d) Place the computer in a public area of the home, such as a living room.
    e) Ensure you are able to access your child's email and randomly check the contents.
    f) Check your phone bill for unusual outgoing calls or consider using a 'caller ID' device to identify incoming calls.
    g) Discuss online safety with your child's school, public library or anywhere that you believe your child accesses the Internet.
    h) Make sure children are aware of some of the issues involved with spending time on the Internet.
    i) Show children what sites they can go to and what information they can send out.
    j) Sit down with your children and discuss the issues.

2. Risk factors

The following may be signs that your child has been targeted by an online predator:

    a) You find pornography on your child's computer.
    b) Your child is receiving phone calls from people you don't know or is calling numbers you don't recognise.
    c) Your child is spending a large amount of time on the Internet.
    d) Your child is receiving gifts or mail from people you do not know.
    e) When you enter the room your child changes the screen or turns the computer off.
    f) Your child is becoming withdrawn or displaying behavioural problems.

3. Advice for your children

It is advisable to tell your children:

    a) Not to send a picture of themselves to someone they do not know.
    b) Never place a full profile and picture of themselves anywhere on the Internet.
    c) If using a Facebook page or similar, ensure your child blocks everyone's access to the page and only allows friends to have access.
    d) Never give out personal information including their name, home address, phone number or school.
    e) Never arrange a face-to-face meeting with someone they have chatted with on the Internet.

Youth Central Online eSafety Tips for Children and Young People Victoria Police Extract

PROTECT YOUR PRIVATE INFORMATION

Only give your mobile phone number and email address to people you can trust. Think about the information you have in your online profiles - if it includes your home address, your mobile number and a photo of you, it makes you very easy to find.

And when it comes to things like bank details or credit card numbers, you should make double-sure that you don't give that information out without thinking about the possible negative consequences first.

KEEP YOUR PASSWORDS TO YOURSELF

Never share your password - ever. Make sure your password is at least eight characters long, a mix of letters and numbers and not the name of your favourite band, pet or football team.

PHOTOS

Think twice before sending or posting a photo. A private joke can become a public embarrassment in one click. Once it's out there you can't take it back and it can travel a long way very quickly.

CHATTING TO STRANGERS

It's not necessarily bad to chat to strangers online, but be aware they might not be who they say they are. Don't share private information and if you are planning to meet them, take a friend, choose somewhere busy and, if possible, meet during the day.

MODERATE COMMENTS

If you've got a blog, make sure you moderate comments. You might consider publishing a blog comment policy, so people know what's okay to discuss and why you have deleted their comments.

ARGUMENTS

If an online argument is turning into a flame war, let it go. Step away, take a few deep breaths and remember what you are posting is probably not something you'll be proud of tomorrow.

IS IT TIME TO ACT?

No matter how prepared you are, sometimes, bad things happen to careful people. If any of these things have happened, it might be time to take a stand:

- Having a friend pass on a private online conversation to someone else without your permission
- Being harassed via messages, Facebook, Twitter, email or in-game chat
- Being tricked into giving out a secret online
- Having an embarrassing picture of you posted or sent around online
- Being signed up to receive unwanted emails, like pornography, by someone else
- Having someone break into your account or steal your password
- Finding out that the person you're emailing, texting or messaging isn't the person you thought they were
- Having someone pretend to be you online
- Being entered in an online poll or contest without your knowledge
- Having someone post nasty comments on your guestbook, blog, or on a discussion board

WHAT TO DO

If you find yourself on the wrong end of some suspect, nasty, or even illegal, online activity, there are steps you can take to start sorting out your digital issues:

Let Someone Know

Tell someone you trust or contact a support service such as Kids Helpline (1800 55 1800) or eSafety. Don't retaliate or reply - this can lead to a flame war and only encourages the other person.

You can also access help through Victoria Legal Aid's Below the Belt Android app, which has advice about things like sexting and cyberbullying.

Change Your Password

If you think someone has been accessing your email or social media accounts, change your password and see if things settle down. Make sure your new password is at least eight characters long, a mix of letters and numbers and not the name of your favourite food, pet or football team.

Block or Report

If the bullying is happening via social media, you can use your account settings to block the accounts being used to bully you. If this doesn't stop the bullying, you can report the bullying to your Internet Service Provider or mobile phone provider to ask for more advice.

If you are receiving threatening messages and feel in danger, you should call 000 and report it to the police.

Save The Evidence

Learn how to keep records of offending online conversations, messages and images. To do this you can print out emails and web pages or take screen captures.

HELPFUL LINKS AND RESOURCES

- Below the Belt: Sex, Selfies & Cyberbullying - A free Android app with info about laws on sex and consent, sexting and cyberbullying.
- eSafety - The Australian Government's eSafety site is designed to help empower you to be safe online.
- ThinkUKnow - Helpful site full of tips on how to stay in control on the web.
- eheadspace - eheadspace is a confidential, free and secure space where young people 12 - 25 or their family can chat, email or speak on the phone with a qualified youth mental health professional.
- Lifeline - If you or someone you know need someone to talk to, for any reason, about anything, you can call Lifeline on 13 11 14, 24 hours.
- Kids Helpline - 1800 55 1800 - Kids Helpline is a free, 24-hour counselling service for young people aged 5-25 years. Counselling is offered by phone, email and over the web.
- Tagged - An Australian film about a group of high-school friends who post a rumour about a rival and spark a chain reaction that leaves no one untouched. Will these friends avoid being tagged forever?

Guide for Sporting Organisations - Online Training Delivery for Children & Young People

Adaption of Football Victoria - online do's and don'ts

1. CONSENT

DO

a) **Obtain written permission** (e.g. by email) for the child or young person **(CYP)** to participate in online training directly **from their parent/guardian and retain on file**.

b) Advise the CYP and their parents/guardians that a **parent/guardian must (recommended)/should be in the room for training sessions** [where possible].

c) **Provide parents/guardians with the name of the person leading the training** session and his/her credentials, including currency of their Working with Children Check.

DON'T

d) Rely on a CYP advising you that their parent/guardian has granted permission.

e) Engage in any form of communication a parent/guardian has not given **express permission** for their CYP to participate in or is unscheduled.

f) **Publish recordings of CYP** to social media channels without express written parent/guardian consent.

2. COMMUNICATION/PRESENTATION

DO:

a) Limit online communication to **issues directly related to delivering online training**, such as advising the time of a session or, when conducting the session, to explaining drills and providing instruction.

b) **Copy all communications to a child's parent/guardian** [where possible].

c) Ensure all training sessions are led by a person engaged by your club with a current **Working With Children Check**, which you have on file.

d) Clearly **communicate expectations to CYP and their parents/guardians.** Eg, who is leading the session, what sessions consist of, what equipment or space will be needed.

e) Ensure that **appropriate security features** are being used for video calls. Eg:

- lock online forums so that they can only be accessed using a password that has been distributed via email to participating players.
- Mute participants on entry.
- Disable the record function.
- Set platform settings to use one way interaction where possible (eg, CYP can see you but you can't see them).

f) Make sure all **presenters know how to apply platform security and privacy settings** to online classes or sessions. Adults should know how to prevent uninvited attendees accessing online sessions, how to block video, audio or chat functions, and how to avoid exposing personal information.

g) Encourage presenters to practise the session before running it.

h) Use **organisation/club accounts** for coaches to use (eg. Zoom) as opposed to personal accounts.

i) Ensure that a presenter's **physical location is in a common area** such as living rooms, rather than private spaces (eg. bedrooms).

j) **Keep communication professional and avoid using emojis** to CYP in electronic chat functions in case they are misinterpreted.

k) If needing to share something on screen, **share individual applications rather than your entire screen.**

l) **Disable email alerts and other notifications** whilst presenting.

m) Ensure that **presentation material to CYP is reviewed** by another official or more senior person in your organisation or club where possible.

n) Try to make sure that there are **at least two officials/club or organisation representatives** on each online forum. This also allows one official/representative to monitor the chat function and/or questions during the forum and ensure that it is appropriate.

o) **Keep to the allocated times** for the online forum.

DON'T

a) **Add as a friend, accept friend requests from, follow or engage with CYP** on social media, video-conferencing or gaming platforms or via other communication channels outside of training.

b) **Communicate** with CYP using chat rooms, social networking sites, game sites or instant messaging **from personal profiles or accounts.**

c) **Engage in one-on-one sessions or communications** with CYP. All communications should be with the team or group as a whole.

d) Use any communications to **promote unauthorised 'social' activity or to arrange unauthorised contact**.

e) **Communicate anything** (verbally, in writing or via images or footage) that a reasonable observer could view as being of a **sexual or inappropriate nature**, or which **suggests the use of tobacco, alcohol or prohibited drugs.**

f) Allow CYP to **share their screens or other files** during/using the online forum.

g) Request a CYP to **keep a communication secret** from their parents.

h) **Require attendance** at online training – if a CYP does not wish to participate or their parent/guardian does not consent, that is the individual choice and they should not be discriminated against or excluded on that basis.

i) **Record training sessions** unless express and informed consent has been given by the CYP's parent/guardian for a specified organisation/club-approved purpose (eg. for posting on the organisation/club's official social media channels, with consent). Any recordings should be deleted once the purpose has been expended.

Note: If a CYP decides not to participate or their parent/guardian does not consent to their participation in video training, consider sending a training program with the drills and exercises from each session so that the CYP can continue to train at home.

3. HEALTH AND SAFETY

a) Ensure that the online training is conducted in a safe outdoor or indoor area that is free of hazards.

b) Wear suitable and **appropriate clothing and footwear**.

Note: Inappropriate clothing/footwear or a training area that is not clear of hazards may affect insurance.

4. COMPLIANCE

a) Abide by applicable **codes of behaviour.**

b) Abide by **rules issued by the government** in relation to social distancing.

c) Consider random online training 'spot checks' or regular moderation to ensure that they are safe.

d) Remind participants that the **standard sport/club policies** will apply to these sessions and participants are expected to behave appropriately and treat their fellow participants and club staff accordingly.

e) **Report any inappropriate behaviour** of CYP or presenters of online forums to the relevant senior person within your organisation/club.

5. RESPONDING TO ESAFETY CONCERNS

The Office of eSafety provides support for children and young people to report online abuse:

- Cyberbullying: eSafety can help remove material that seriously threatens, intimidates, harasses or humiliates a child or young person under 18. eSafety also works with parents, schools and police to stop further cyberbullying.
- Image-based abuse: if someone shares or threatens to share an intimate image or video of a person without their consent, eSafety can help to have it removed. In some cases, eSafety can also impose civil penalties against the abuser or the platform they used.