CHILD SAFETY FRAMEWORK PARENTS & GUARDIANS GUIDE

eSafety Guide to Keeping Kids Safe – Tips for Parents & Guardians

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 <u>not</u> 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)**