CYBERSAFETY POLICY

for

Pinjarra Swimming club

'The organisation' refers to *Pinjarra Swimming Club*

RATIONALE

The organisation has an obligation to ensure that affiliated clubs and organisations maintain a safe physical and emotional environment for club members, coaches, officials, registered players, sponsors, support personnel and umpires. The internet and Information and Communication Technologies (ICT) devices/equipment can bring great benefits to users and can contribute to the effective operation of the organisation and its members through the ability to disseminate information, the ability to promote the sport and clubs and to provide members with the ability to connect with others within the organisation. Responsible use of technology can include:-

- Use of the organisation or affiliated club websites to provide information about competitions, committees, policies, rules, social events or other important sport related issues.
- Use of SMS and/or email by officials, managers, coaches etc to communicate club business and club sanctioned social events (via parents in the case of juniors).
- Use of the organisation or affiliated club's social network pages to promote positive club news and events (with permission obtained from featured individual).

This responsibility for the provision of a safe sporting environment is no longer solely confined to the playing field and the organisation has seen the emergence of a number of cybersafety issues related to the use of ICT. Although we acknowledge that there are numerous positive outcomes associated with the use of ICT within sport, we also recognise that this usage has the potential to have a negative impact.

The organisation places a high priority on the acceptable use of ICT devices/equipment which will benefit members. However it recognises that the presence in the sporting environment of these technologies can also facilitate anti-social, inappropriate, abusive, threatening and even illegal behaviour and activities. The organisation aims, therefore, to maximise the benefits of these technologies, while at the same time minimising the dangers and manage the risks.

UNDERLYING PRINCIPLES

This policy is written with the underpinning of the organisation's core values:

- Promote, encourage and develop participation in swimming and other related activities and to teach and encourage its teaching to children and adults.
- To contribute to the wellbeing, health and safety of the people of the community.
- To arrange programs of competition within the club and participation by club members in competitions with other clubs and clubs with like objects.

WHAT IS CYBERSAFETY?

Cybersafety is the safe and responsible use of ICT. A cyber safe environment can be achieved by building on and promoting the respectful use of technology whilst at the same time working to minimise any risks.

WHAT IS CYBERBULLYING?

"Cyberbullying is a way of delivering covert psychological bullying. It uses information and communication technologies to support deliberate, repeated and hostile behaviour, by an individual or group that is intended to harm others" (Belsey 2007).

Cyberbullying includes, but is not limited to, the following misuse of technology:

- harassing, teasing, intimidating or threatening another person via electronic means.
- sending or posting inappropriate digital pictures or images, e-mail messages, instant messages, phone messages, text messages, or website postings (including social network sites e.g. Facebook or blogs) and is irrespective of whether the page could be viewed by the wider public or not. It can also include the sending, receiving and/or possession of naked or sexually explicit images of a person.

The organisation's members must also be aware that postings, comments and/or messages from their individual accounts such as email, social networking (e.g. Facebook) micro blogging (e.g. Twitter) video sharing (e.g. YouTube), picture sharing (e.g. Instagram) and mobile phones, will remain the responsibility of the account owner unless the account owner can prove that their account has been accessed by an unauthorised person and by a method outside of their control. Members must understand that they should be vigilant about the security of their account(s) and take all steps deemed reasonable to protect themselves such as not sharing passwords and not allowing others to log onto their individual accounts.

All members of the organisation must be aware that in certain circumstances where a crime has been committed, they may also be subjected to a criminal investigation by Police. This particularly applies to 'sexting' where the registered member is in possession of an inappropriate sexualised image of a person under the age of 18 years. In this case the Western Australia Police should be informed immediately.

POLICY

The organisation takes seriously its responsibility in providing this robust policy. These guidelines provide advice and direction in relation to what is considered acceptable electronic communication between and by members of the organisation. The provision of education for all members of the organisation about this policy will be an important element of the success of this cybersafety policy.

BREACHES OF THE POLICY

The organisation's cybersafety policy will be breached if:-

- the organisation's name, motto, crest and/or logo is used in a way that would result in a negative impact for the organisation, clubs and/or its members.
- the use of any electronic communication between members is considered to be offensive, abusive, harassing, threatening or demeaning towards another person.
- the content of a posting or an electronic message which if said in person during the playing of the game would result in a breach of the rules of the game.
- the posting or sending of an electronic communication would be in breach of the organisation's anti-discrimination, racial discrimination, sexual harassment or other similar policy.
- the content of electronic communication is a breach of any state or commonwealth law.

PROCEDURE FOR REPORTING

All reports of cyberbullying and other online or mobile telephone harassment will be investigated fully by the organisation and may result in a notification to Police. A notification to Western Australian Police by either the organisation or an individual will not abrogate the organisation of its responsibility to fully investigate a complaint and such investigation may be conducted alongside any Police investigation.

Members of the organisation who feel that they have been the victim of such misuse of technology should:-

In the case of sexually explicit material

- save and store the inappropriate/abusive material on their computer, mobile phone or other device (do not print or share this content).
- immediately report the content to Western Australian Police followed by a report to the President. Parents should report on behalf of a child.

In the case of other abusive content

- save and store the inappropriate/abusive material on their computer, mobile phone or other device.
- print a copy of the material.
- report the content/picture directly to the site (e.g. Facebook or Twitter).
- report the matter to the relevant representative President.

RESOLUTION PROCEDURES

The range of processes available to expedite the investigation of a breach of the cybersafety policy will include all current procedures from informal through to formal.

PENALTY

Under the organisation's *Cyberbullying Policy* a proven charge arising from the findings of a disciplinary hearing/tribunal hearing for an online breach of the code of conduct as per this policy may attract one or more of the following penalties;

- Removal from the sporting facility
- Cancellation of club membership
- Suspension of attendance at future competitions, training and social events.

In deciding the final penalty, consideration will be given to the seriousness of the act, the impact on the complainant, the impact on *swimming* and its affiliated associations and/or clubs, and the prior good history or otherwise of the person.

A member presented before a disciplinary hearing / tribunal on a cyberbullying or online abuse allegation must be aware that the penalties available to the tribunal/disciplinary hearing members will cover the complete range available.

In the case of *a non-playing member*, if an allegation is proven, they will be disciplined to the full extent possible which may include, but is not limited to, the removal from the

facility, cancellation of club membership, banning attendance at future competition/training/social events etc.

APPEALS

To lodge an appeal for a hearing pertaining to any matter listed above refer to Swimming Western Australia for further advice.

Important terms used in this document:

- *The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.'*
- ***'Cybersafety'** refers to the safe and responsible use of the internet and ICT equipment/devices, including mobile phones.*
- *The term **'ICT equipment/devices'** used in this document includes but is not limited to computers (desktop, laptop, netbook, PDA's, Tablet), storage devices (such as USB, flash memory devices, CD's, DVD's, floppy discs, iPods, MP3 players), cameras (such as video, digital, phone, webcams) all types of mobile phones, gaming consoles and any other, similar technologies as they become available.*
- *The term **'sexting'** refers to the act of sending sexually explicit or naked messages or photos/videos electronically, primarily between mobile phones, but can include internet applications such as MSN, Skype, email, or social networking sites.*

Contacts:

- ***Australian Communications and Media Authority*** - www.acma.gov.au
- ***Cybersafety Solutions*** – www.cybersafetysolutions.com.au
- ***Cybersmart*** – www.cybersmart.gov.au
- ***Kids Help Line*** - www.kidshelp.com.au or 1800 55 1800
- ***Western Australia Police:***
    - ***General Enquiries – 131 444***
    - ***For cyberbullying, online stalking or other technology crimes*** - if you believe you are the victim of any form of technology crime please email full details of the incident to the WA Police Assessment Officer at **Technology.Crime@police.wa.gov.au**. Please include your full name, address and contact details to enable follow-up action.

This cybersafety policy was prepared by Susan McLean www.cybersafetysolutions.com.au;
+61 419887741 or susan@cybersafetysolutions.com.au