VOLLEYBALL WESTERN AUSTRALIA

Cybersafety Policy

Date of Issue	9th April 2014
Last Reviewed	December 2016
Controlling Body	VWA Board

Overview

Volleyball WA (VWA) endeavours to meet all its responsibilities and relevant legislation for the physical and emotional safety of employees and members. This includes the need to establish and maintain a cybersafe environment. This policy will assist VWA to:

- Meet its legal obligations;
- Provide guidance to employees and members regarding the safe and responsible use of ICT; and
- Educate members of the VWA community regarding the safe and responsible use of ICT.

This policy is to be read in conjunction with the following documents:

- VWA Induction Manual and Communications Guide
- VWA Information Communication Technology Policy
- VWA Social Media Policy
- VA Member Protection Policy
- VA Privacy Policy

Definitions

- ICT - 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
- ICT equipment/devices – 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
- 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

Background

The Internet and Information and Communication Technologies (ICT) play an increasingly important role in the delivery of VWA business and services to members. Responsible use of technology can include:

- Use of the VWA website to provide information about competitions / events, committees, policies, rules or other important sport related issues
- Use of SMS and / or email by VWA employees and volunteers to communicate VWA business matters (via parents in the case of juniors)
- Use of VWA's social network pages to promote positive news and events (with permission obtained from featured individual)

VWA 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.

What is Cybersafety?

Cybersafety is the safe and responsible use of ICT. A cybersafe 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 the use of technology to bully a person or group with the intent to hurt them socially, psychologically or even physically." (Office of the Children's eSafety Commissioner)[1]

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.

VWA's employees and 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. Employees and 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 VWA employees and members 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 Application

1. This policy applies to all VWA members and all other people or organisations which by agreement or otherwise, are bound to comply with this policy
2. This policy applies to behaviour and practices occurring during the course of VWA business, activities, competitions and events

Responsibilities

VWA'S role and contribution in making this policy work is to:

1. Take all reasonable steps necessary to ensure that everyone in the organisation knows:
   a) What cyber safety issues are
   b) What the Cyber Safety Policy is and understands their roles and responsibilities

   This will be achieved by:
   c) Including a copy of the Policy in the Policy and Procedures Manual
   d) Distributing the Policy to all Associations and Clubs
   e) Ensuring all VWA and Club / Association personnel are educated and trained with the policy
   f) Including a copy of the policy on the VWA website

[1] https://www.esafety.gov.au/esafety-information/esafety-issues/cyberbullying

g) Notifying participants in all VWA activities / events that they will be required to comply with this policy

2. Provide guidance regarding the safe and responsible use of ICT;
3. Outline the nature of possible consequences associated with breaches of the VWA Cybersafety Policy

Clubs / Associations roles and contribution are to:

1. Comply with this policy and ensure information is made available.
2. Ensure all significant personnel are familiar with the policy and required procedures at each level of the VWA Network.
3. Collaborate with VWA employees to implement best practice.
4. Report any areas of concern to VWA within a timely manner.

Employees and Member's roles and contribution are to:

1. Ensure appropriate conduct when representing VWA in all activity including:
   a) That no electronic communication could cause offence to, harass, or harm others, put the owner of the user account at potential risk, bring VWA into disrepute, or in any other way be inappropriate in the business of VWA;
   b) For personal safety, be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Such information should not be passed on about others.

Policy Statement

VWA will take all policy breaches and complaints seriously and will ensure they are dealt with promptly, sensitively and confidentially in accordance with the Member Protection and Misconduct policies. Any breach that is deemed harmful to the safety of VWA (for example, involvement with inappropriate material, or the use of ICT to facilitate anti-social behaviour such as harassment) may constitute serious misconduct. If there is a suspected breach of this Policy involving privately-owned ICT device/s, the matter will be investigated VWA and may be required to audit that equipment/ device(s).

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 VWA or an individual will not abrogate VWA of its responsibility to fully investigate a complaint and such investigation may be conducted alongside any Police investigation.

VWA's Cybersafety Policy will be breached if:

- VWA's name, motto and/or logo are used in a way that would result in a negative impact for the association 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

Review

This policy shall be reviewed by the Board annually. In addition to the annual review of this policy, recommended changes to the policy may be submitted to the Board for consideration, at any time. If the amendments are approved by the Board, the policy shall be updated, dated and circulated to all relevant stakeholders.

VWA Cybersafety Procedure

Inappropriate Activities / Material

1. While using the VWA network, Internet facilities or ICT equipment/devices, or using any privately-owned ICT equipment/device for VWA business it is inappropriate to:
   a) initiate access to, or have involvement with, inappropriate, dangerous, illegal or objectionable material or activities; or
   b) save or distribute such material by copying, storing or printing.
2) In the event of accidental access to any inappropriate material by a employees member, board member, volunteer or contractor, the Executive Director (or nominated officer) should be consulted
   a) In the event of accidental access of inappropriate material at the lower range of seriousness (eg SPAM), the user should delete the material
   b) If the nature of the material is somewhat more serious (eg SPAM containing inappropriate but not illegal images) delete it and log it as an incident on the Incident Report Form and pass to a Manager. When in doubt, log the incident.
   c) Where the material is clearly of a more serious nature, or appears to be illegal, users should:
      I. remove the material from view (by closing or minimising the window, turning off the monitor, or shutting down the device); and
      II. report the incident immediately to the Executive Director (or nominated officer)

Persons under the age of 18 year use of the Internet and email

In the event a person under the age of 18 years is required to use VWA ICT devices and equipment, the person will be actively supervised by the Executive Director or an officer nominated by the Executive Director.

Posting material

1. All material submitted for publication on the VWA website, Facebook page, Twitter account, Instagram account, Youtube or other social media outlets should be appropriate to VWA business
2. Such material can be posted only by those given the authority to do so by the Executive Director;
3. The Executive Director (or nominated officer) must be consulted regarding links to appropriate websites being placed on the VWA website;
4. Any content, which is deemed inappropriate or offensive and reported to the Executive Director, will be dealt with under the VWA Misconduct Policy.

Reporting Concerns

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

1. In the case of sexually explicit material
   a) Save and store the inappropriate/abusive material on their computer, mobile phone or other device (do not print or share this content).
   b) Immediately report the content to Western Australian Police followed by a report to the Executive Director. Parents should report on behalf of a child.
2. In the case of other abusive content
   a) Save and store the inappropriate/abusive material on their computer, mobile phone or other device.

b) Print a copy of the material.
c) Report the content / picture directly to the site (e.g. Facebook or Twitter).
d) Report the matter to the Executive Director

Further information about the reporting and complaint handling procedure can be found in the Member Protection Policy.

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.