VOLLEYBALL WESTERN AUSTRALIA

Information Technology Systems and Equipment Policy

Policy Name: Information Technology Systems and Equipment Policy		
Policy Number: 360GEN2013	Document Type: Policy	Effective Date: 1 December 2013
Last Reviewed: November 2021	Next Review: November 2024	
Applicable Legislation: • Telecommunications (Interception and Access) Act 1979 *(Cth)* • Privacy Act 1988 *(Cth)* • ISO 27001:2013 *(international)*		
This policy will be reviewed every three years or earlier if required by the organisation. The review will ensure it reflects both the community expectations and all legal requirements.		

Purpose Statement

The purpose of this policy is to.

- Ensure VWA employees, contractors, work experience placements, volunteers and board members understand the acceptable use of VWA's IT systems and equipment.
- Support VWA through the management and IT resources and systems
- Outline how to protect VWA's reputation and safeguard its resources.
- This policy, where relevant, operates in conjunction with an employee's contract of employment. However, it is not incorporated into and does not form part of the employment contract.

Policy Application

This policy applies to all VWA employees, contractors, volunteers, board members, work experience placements and all other people or organisations that access VWA's information systems and networks by agreement or otherwise.

This policy applies to behaviour occurring during VWA business, activities, competitions, and events.

Definitions

The following definitions are listed to provide clarity for this policy.

- **Information Technology (IT) equipment** is IT equipment owned or leased by VWA to use for VWA business and event purposes. This includes but is not limited to:
  - Laptops
  - Mobile Phones
  - Desktop Computers
  - Printers
  - Tablets
  - Cameras
  - Portable storage devices
- **Information Technology (IT) system** means systems including but not limited to:
  - All internet, email and computer facilities accessed using VWA owned or leased equipment
  - Desktop and laptop computers owned or leased by VWA
  - Tablets and mobile phones owned or leased by VWA
  - Personal mobile phones used for work purposes
  - Any other means of accessing VWA email, internet, and computer facilities (including using personal IT equipment to access VWA's IT System)
  - Cloud-hosted platforms operated by VWA.
- **Internal social network** means programs and networks (e.g., Share Point, Teams) that are only available to employees, contractors, work experience placements, volunteers, and board members provided with VWA Systems Access.
- **Personal use** means the use of VWA IT equipment or systems outside VWA work responsibilities.
- **Use** means to create, access, view, upload, download, post, share, store and transmit information or data.

- **User** means all employees, board members, volunteers, contractors, work experience placements, third parties, and other people who legitimately access VWA's systems and/or network

Background

Information technologies (IT) play an essential role in delivering VWA business and services to members. Therefore, VWA places a high priority on the acceptable use of IT equipment and services which will benefit members and the workplace.

Policy Statement

VWA's commitment is to manage employee, contractor, work experience placements, volunteers, and board members use of VWA IT systems and equipment to promote professional, ethical, and lawful behaviour.

IT Systems

- VWA's IT systems are to be used primarily for business related purposes.

- Use of VWA' s IT Systems must always be professional.
    - A user of VWA's IT Systems must not:
        - Use material that may be offensive.
        - Use material that may be defamatory.
        - Use material that may impact VWA's storage capacity or decrease network performance.
        - Use material that may adversely impact the image or reputation of VWA, its employees, contractors, stakeholders, volunteers, or members.
        - Use the IT system to bully, threaten, harass, or intimidate or intend to bully, threaten, harass, or intimidate.
        - Use the IT system to violate intellectual property rights, including copyright.
        - Use the IT system in any way that may be illegal or unlawful.

- Employees, contractors, work experience placements, board members or volunteers may not use VWA's IT System to conduct commercial activities that do not relate to the business of VWA.

- Any content composed, sent, or received using VWA's IT System is and will always remain VWA property. VWA reserves the right to intercept, access, review and disclose all messages or content created, received, or sent via VWA's IT system without prior notice.

- All sensitive information such as passwords, usernames and confidential information must be securely stored. Usernames and passwords should not be shared with any other person, whether that person is a VWA employee or not.

- Employees, contractors, work experience placements, board members and volunteers must report any security related incidents to VWA Operations Manager or the CEO.

Internal Collaboration Systems

- VWA may, from time to time, make available internal social network sites to foster collaboration between people and teams and allow employees to share ideas, information and seek feedback easily.

- Professional standards of language and VWA's Code of Behaviour must be adhered to whilst using an internal social network.

    - It is not permissible to post or comment on any material that:
        - Others may find offensive
        - Maybe defamatory
        - Threatens, harasses, or intimidates or intends to threaten, harass, or intimidate
        - Is unlawful
        - Could violate copyright
        - Is a virus
        - Confidential or commercially sensitive information; or
        - Breaches any other VWA Policy.

IT Equipment

- Employees, contractors, work experience placements, board members and volunteers are not permitted to install software on VWA laptops, desktops, or other IT devices without the express permission of the Operations Manager and or CEO.

- VWA Laptops, cameras, tablets, and other event IT devices must be secured either:
    - Overnight on the VWA premises; or
    - When taken home by the employee, must be kept in a secure place and out of public view.
    - When at an event, the IT Equipment must be kept in a secure place when not in use.

- Employees, contractors, work experience placements, board members and volunteers are responsible for the proper use, care, maintenance, and safekeeping of any IT Equipment issued to them. VWA may require employees, contractors, work placements, board members, and volunteers to replace, at their own expense, any equipment and any associated accessories supplied to them by VWA if it has been damaged or lost due to carelessness or negligence.

- Personal use of VWA IT Equipment during working hours is prohibited except for emergencies and allocated breaks.

- Employees, contractors, work experience placements, board members and volunteers may not use VWA's IT Equipment to conduct commercial activities that do not relate to the business of VWA.

- All other IT Equipment must be kept on VWA premises and can only be removed with authorisation by the Operations Manager or the CEO.

- VWA will be responsible for the maintenance and configuration of all VWA IT Equipment and software. Employees, contractors, work experience placements, board members and volunteers are not permitted to make any changes without authorisation by the Operations Manager or the CEO.

- Users of VWA ICT devices will inform the Operations Managers of any messages relating to system errors, faults, damage that affect the usability of the ICT device.

Monitoring

- VWA reserves the right to intercept, access, review and disclose all content created, sent, or received using VWA's IT System, irrespective of whether it was created, sent, or received inside or outside business hours or using VWA owned or personal equipment.

- VWA may regularly monitor content published on publicly available Social Media sites and may take misconduct action if a VWA employee has published content in breach of this policy, contractor, volunteer, and member.

Policy Breaches

VWA will take all breaches of the policy seriously and will ensure they are dealt with promptly, sensitively, and confidentially.

Disciplinary action may be taken against a person who is found in breach of this policy, in accordance with the Complaints Management Procedure.

If a criminal offence is considered to have been committed, the appropriate authorities will be contacted for advice and guidance.

Document Control

Version History

Date	Version number	Executive Summary of changes
December 2013	1.0	• This policy was adopted at the December VWA Board Meeting.
December 2016	2.0	
November 2021	3.0	• Change of name to Information Technology Systems and Equipment as more relevant as of 2021. • Major updates to reflect IT changes since 2016.

Appendix & Relevant Procedures

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

- VWA Cybersafety Policy
- VWA Social Media Policy
- VWA Staff Misconduct Policy
- VWA Complaint Handling Policy
- VA Member Protection Policy
- VA Privacy Policy