Information Communication Technology Policy

Overview

Use of Information Communication and Technology (ICT) by employees, board members, contractors and volunteers of Indoor Beach Volleyball Federation (IBVF) is permitted and encouraged where such use supports the goals and objectives of the organisation. This policy will assist IBVF to:

- Meet its legal obligations;
- Provide guidance to users regarding the safe and responsible use of ICT; and

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

- IBVF Social Media Policy
- VA Member Protection Policy
- VA Privacy Policy
- Australian Spam Act
- Australian Copyright Council Legislation Information

Definitions

- Account / IBVF Sign-In – access provided by IBVF to any ICT Device or any non-IBVF ICT Device utilised for IBVF purposes
- Apps - Applications downloaded from external sites
- Data - any material developed, copied and / or produced for the purpose of conducting IBVF business, including, but not limited to, emails, letters, reports, notes, website content, contacts and electronic files / folders
- Executive Director - Executive Director of IBVF;
- ICT - ICT products and services are defined as all types of technology (data, voice, video etc) and associated devices, which relate to the capture, storage, retrieval, transfer, communication or dissemination of information through the use of electronic media.
- ICT devices - includes, but is not limited to, the following:
    - Desktop computers
    - IT Servers
    - MacBook/ Laptop computers
    - iPads / Tablet PCs / Palm pilots
    - Smart Televisions
    - Electronic and interactive whiteboards
    - Smart phones / Mobile phones
    - Desk phones and Telephone servers
    - USB Flash Drives and other storage devices
    - Modems (wireless, portable & fixed)
- Nominated Officer- A person given authority by the Executive Director to carry out a task as directed
- Organisation - for the purpose of this policy, reference to ‘organisation’ means Indoor Beach Volleyball Federation
- Other Entities – external organisations which may provide IT solutions and IBVF centres and wholly owned organisations
- Portable ICT devices - includes, but is not limited to, the following:
    - MacBook / Laptop computers;
    - iPads/ Tablet PCs / Palm pilots;
    - Smart phones / Mobile phones;
    - USB Flash Drives and other portable storage devices
    - Wireless technologies (eg Portable modems)
- User - all employees, board centres, volunteers, contractors, third parties and all other people who legitimately access IBVF’s systems and/or network

Background

The Internet and Information and Communication Technologies play an increasingly important role in the delivery of IBVF business and services to members. IBVF places a high priority on the acceptable use of ICT devices/equipment which will benefit members.

Acceptable use can most easily be illustrated by examples of unacceptable use. The following includes, but is not limited to, what may be considered an inappropriate use of an ICT device. In instances where such use is required for legitimate purposes, an exception may be approved by the Executive Director.

- Destruction of, or damage to equipment, software, or data belonging to IBVF or other entities / partners (eg scratching, breaking, defacing, intentionally dropping etc)
- Attempts to gain unauthorised access to computer systems or networks (eg making any attempt to obtain another users password or access the IBVF system as a different user)
- Unauthorised monitoring of electronic communications (eg using illegal tracking devices on another user's ICT device)
- Knowingly downloading, storing, distributing and viewing of offensive, obscene, indecent, pornographic, or menacing material
- Unauthorised Acquisition, reproduction, distribution and use of copyrighted material is illegal without written permission of the owner. Software may not be used or downloaded unless appropriate licensing conditions are met
- Downloading and storage of material such as music/movie clips requires use of considerable IBVF devices and as such is unacceptable unless required for IBVF purposes and within copyright. Broadcasting or creating fileshares for such material is also unacceptable unless it is for IBVF purposes
- Accessing and use of gambling and betting internet sites
- Playing of games is not permitted by staff within work hours
- Screen Savers and wallpapers that could be considered of an offensive nature are inappropriate in a work environment.
- Downloading unlicensed software. Software may be downloaded for IBVF purposes. All licensing conditions however must be adhered to with regard to its evaluation and subsequent use
- Mass emailing across IBVF and the internet (SPAM) is not permitted except as approved by the Executive Director or Nominated Officer. The SPAM Act 2003 imposes harsh fines for unsolicited commercial electronic messages
- Sending inappropriate emails is not permitted and any emails should comply with the IBVF Communications Guidelines. Emails and stored information are considered records of the organisation.
- IBVF facilities should not be used for private business use unless written permission has been received from the Executive Director

Policy Application

1. This policy applies to all IBVF employees, board members, volunteers, contractors, third parties and all other people who legitimately access IBVF's systems and/or network
2. This policy applies to behaviour and practices occurring during the course of IBVF business, activities, competitions and events

Responsibilities

IBVF'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 acceptable use of ICT is
   b) What the Information Communication Technology 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 IBVF employees, volunteers, centres and contractors
   e) Ensuring all IBVF employees, volunteers, centres and contractors are educated and trained with the policy
   f) Including a copy of the policy in the IBVF employees, volunteers and contractors induction process
2. Provide guidance regarding the safe and responsible use of ICT;
3. Outline the nature of possible consequences associated with breaches of the IBVF Information Communication Technology Policy

IBVF employees, volunteers, centres and contractors roles and contribution are to:

1. Comply with relevant legislation
2. Ensure appropriate conduct when representing IBVF in all activity and that no electronic communication could cause offence to, harass, or harm others, put the owner of the user account at potential risk, bring IBVF into disrepute, or in any other way be inappropriate in the business of IBVF
3. Comply with this policy at all times, whether working at or outside of the IBVF Head Office, as outlined in the Acceptable Use of ICT Procedure

Policy Statement

IBVF 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 policy. Any breach that is deemed harmful to the safety of IBVF (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 IBVF and may be required to audit that equipment/ device(s).
If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Review

This policy shall be reviewed every 3 years, unless required earlier. In addition to the 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.

IBVF Acceptable Use of ICT Procedure

IBVF Authority

1. All ICT devices supplied to users is the property of IBVF and must be returned upon the request of IBVF
2. Access for authorized IBVF employees and / or other entities shall be given to allow essential maintenance security work or removal, upon request
3. All ICT devices will be supplied and installed by a delegated IBVF contractor. All Hardware **must only** be provided by IBVF
4. ICT usage may be monitored by the Executive Director or Nominated Officer

Maintenance and Configuration

1. Users will not install or update any software or hardware on to a IBVF owned ICT device without prior approval
2. Users will not install any screen savers, except IBVF-owned images, on to a IBVF owned portable ICT device, and will not disable any screen saver in use
3. Users will not change the configuration of any IBVF owned ICT device without permission of the IBVF Executive Director or Nominated Officer (personal settings may be applied)
4. Users will allow, and assist if necessary, the installation and maintenance of installed Anti-Virus and software updates required to protect the user or ICT device
5. Users of IBVF owned ICT devices will inform the Executive Director or Nominated Officer within 1 business day of pop-up dialog box messages relating to system errors and/or configuration change requests and any known faults, which effect the usability of the ICT device
6. Users must obtain approval by the Executive Director or Nominated Officer for any maintenance and/or repair work, which has associated financial costs, prior to the work commencing
7. Users will not engage third parties for the purpose of ICT support and maintenance without the Executive Directors or Nominated Officers prior approval
8. Users must not remove or deface any asset registration number

Data Storage

1. All IBVF data should be stored in a file on the IBVF Server wherever possible and not held on an ICT device. Users must ensure electronic files pertaining to IBVF business are stored in accordance with the IBVF Electronic File Management structure
2. No IBVF data should be stored on a personal ICT device, without approval of the Executive Director or Nominated Officer. In the event data has been stored on a personal ICT device, after approval, the user is required to remove all data upon ceasing employment / engagement with IBVF

Security and Usage away from IBVF Head Office

1. All ICT devices with access to IBVF emails or documents must be password protected. Passwords will be supplied and updated by a delegated IBVF contractor
2. Users must ensure that password, user names access and personal identification numbers are kept in a separate location to the ICT device at all times.
3. Access to protected or restricted information must be controlled using passwords, user logins and access levels. These levels will be set by the Executive Director, Nominated Officer and / or IBVF delegated contractor
4. Any user who has access to protected or restricted data, services or infrastructure must use a Dual-factor authentication system when remotely accessing IBVF systems. An appropriate solution will be provided by ICT, and must be using IBVF supplied IT equipment, the use of non-IBVF owned equipment is not permitted.
5. All ICT devices should be switched off, logged off, and / or the keyboard locked when left unattended, even if only for a few minutes
6. All removable media devices and paper documentation must not be stored with a portable ICT

device

7. Users must take due care and attention of portable ICT devices when moving between offices, homes and other business sites
8. Users are personally responsible for the safe and secure carriage of all IBVF ICT Devices in their possession at all times
9. Portable ICT devices should not be left where they could attract the interests of the opportunist thief

General Use

1. Users will not set-up inappropriate voice messages on IBVF ICT applicable devices
2. Users will be responsible for the replacement and /or repair costs of any damage and/or loss of portable ICT as the result of inappropriate behaviour
3. No family members, relatives or any other non IBVF authorised users may access and /or use IBVF owned ICT devices. IBVF owned ICT devices are supplied for the use by IBVF authorised users only for the purpose of IBVF business
4. Users are required to seek approval from the Executive Director or Nominated Officer before taking any IBVF ICT devices for the period of annual / personal leave and / or outside Australia. The equipment may not be covered by IBVF insurances against loss or theft and the device may be liable to be confiscated by Airport Security personnel.