



## **PRIVACY POLICY OF Bulls Club**

Telephone number of the club: 065 361 9618  
Email address of the club: [admin@fcabulls.club](mailto:admin@fcabulls.club)  
Information officer: Riehet Versfeld Club CVP  
Email address: [riehet@fcabulls.club](mailto:riehet@fcabulls.club)  
Deputy information officer: Abygale Versfeld  
Email address: [abygale@fcabulls.club](mailto:abygale@fcabulls.club)

## **1. Introduction**

- 1.1 Bulls ("the club") is a sports club and is managed and governed by members nominated or selected during AGM. The club is a Christian club with Afrikaans as main coaching medium. The club enter teams into leagues based on player registration ages.
- 1.2 The club needs to gather and use certain information about individuals and juristic persons (collectively referred to as "data subjects"). Section 1 of the Protection of Personal Information Act (POPIA), 2013 (Act 4 of 2013) defines a "data subject" as "*the person to whom personal information relates*". A data subject can include players, coaches, officials (umpires/scorers), administrators, members, clients/service providers of the club, suppliers, business contacts, employees, volunteers and other persons the club has a relationship with or may need to contract with.
- 1.3 This policy describes how this information must be collected, handled, and stored to meet the club's personal information protection standards and to comply with the law.
- 1.4 The club regards the lawful and appropriate processing of all personal information as crucial to successful service delivery and essential to maintaining confidence between the club, data subjects and entities/agencies/businesses/persons who deal with the club. The club therefore fully endorses and adheres to the principles of the POPIA, and the regulations promulgated in terms of the Act.
- 1.5 The information officer of the club is the club vice chairperson, Riehet Versfeld, and she can be contacted, in writing, regarding any POPIA-related matters.
- 1.6 The deputy information officer of the club, as delegated by the principal, is Abygale Versfeld and she can be contacted in writing.
- 1.7 Definitions appear at the end of this policy for the meaning of the terms used.

## **2. Purpose**

- 2.1. This privacy policy ensures that the club:
  - a) complies with the POPIA, 2013 (Act 4 of 2013);
  - b) protects the rights of data subjects as defined;
  - c) is transparent about how it collects, retains, stores, destroys, deletes and processes personal information of data subjects; and
  - d) protects the club and the data subjects' rights from the risks of a security breach.

## **3. Policy statement**

- 3.1. The club is committed to protecting the privacy of data subjects in accordance with the obligations imposed by the POPIA. The POPIA describes how the club must collect, handle and store the personal information of data subjects.
- 3.2. These principles apply regardless of whether the information is stored electronically, on paper or on other materials.
- 3.3. To comply with the POPIA the following important privacy principles apply. The personal information must:
  - a) be processed reasonably and lawfully;
  - b) be obtained for the specific, intended purpose;
  - c) be adequate, relevant and not excessive;
  - d) be accurate and kept up to date;
  - e) not be held for longer than necessary;
  - f) processed in accordance with the rights of data subjects;
  - g) be protected in appropriate ways; and
  - h) not be transferred outside South Africa unless that country or territory also ensures an adequate level of protection.

## **4. Scope**

- 4.1. This policy applies to all the club's employees, both permanent and temporary, to employees working on a contractual basis for the club, coaches, volunteers, and others who are authorised to access personal information held by the club.
- 4.2. The provisions of the policy are applicable to both on- and off-site processing of personal information and information by an operator or person acting under authority.
- 4.3. It governs all business activities that involve the processing of personal information, including special personal information, for or on behalf of the club. This personal information and special personal information may include, among others:

#### 4.3.1. Personal information:

- a) information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic/social origin, colour, sexual orientation, age, physical/mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- d) biometric information of the person;
- e) the personal opinions, views or preferences of the person;
- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the person; and
- h) the name of the person, if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

#### 4.3.2. Special personal information:

- a) the religious/philosophical beliefs, race/ethnic origin, or biometric information; and
- b) the criminal behaviour of a person as it relates to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed by a person or the disposal of such proceedings.

## 5. Risks

### 5.1. This policy helps to protect the club and data subjects from security risks, including:

- a) **Breaches of confidentiality** - information being shared inappropriately;
- b) **Failing to offer choices** - all data subjects should be free to choose how the club uses information relating to them where the personal information is not collected, used or shared in terms of a law or an agreement between the data subject and the club;
- c) **Reputational damage** - the club or the data subject could suffer reputational damage if hackers successfully gain access to the personal information of data subjects; and
- d) **Loss of personal information.**

## 6. Responsibilities

- 6.1. Everyone who works for or with the club has a responsibility to ensure that the personal information of data subjects is collected, stored and handled appropriately to ensure the confidentiality, integrity and availability thereof.
- 6.2. Everyone within the club is required to ensure that all staff who manage or have access to personal information comply with this policy. The governing body and members of the club management team are required to review procedures in their areas to ensure compliance with this policy and the POPIA as part of the annual planning process of the club.
- 6.3. Everyone that handles personal information must ensure that it is handled and processed in line with this policy and the privacy principles.
- 6.4. These persons have the following key areas of responsibility:
  - 6.4.1. The information officer is ultimately responsible for ensuring that the club meets its legal obligations.
  - 6.4.2. The information officer/deputy information officer is responsible for:
    - a) staying updated regarding information assets and personal information protection responsibilities, risks and related matters;
    - b) reviewing all personal information protection of policies and procedures;
    - c) arranging personal information protection training and advice to the relevant employees and persons covered by this policy; and
    - d) checking and approving any contracts or agreements with third parties that may collect, handle, store or destroy personal information on behalf of the club.
  - 6.4.3. The information officer/deputy information officer is responsible for dealing with requests from data subjects who want to see the personal information the club holds about them (also called "*data subject access requests*"). The identity of anyone making a data subject access request must be verified before disclosing any personal information.
  - 6.4.4. Club Chairperson is responsible for:
    - a) ensuring all Information and Communication Technology (ICT) assets used for processing personal information meet capable security standards;
    - b) performing regular checks and scans to ensure security hardware and software is functioning properly; and
    - c) evaluating any third-party services which the club is considering using to process personal information, for example, cloud computing services.

## 7. General guidelines

- a) The only persons able to access any personal information covered by this policy should be those who **need it for work or legitimate related purposes**.
- b) Personal information **should not be shared informally** and must never be shared using social media accounts such as Facebook, LinkedIn, Google Plus, WhatsApp, etc.
- c) When access to personal information is required, employees can request it from the information officer or his/her delegate.
- d) The club **will provide training** to all employees to help them understand their responsibilities when handling personal information.
- e) Employees should keep all personal information **secure**, by taking precautions and following the guidelines set out herein.
- f) Strong **passwords must be used**, and they should never be shared.
- g) Personal information **should not be disclosed** to unauthorised persons, either within the organisation or externally.
- h) Personal information must be **regularly reviewed and updated** if it is found to be out of date. If no longer required for the intended purpose, it should be deleted and disposed of in line with the disposal process.
- i) Employees **should request help** from the information officer or his/her delegate if they are unsure about any aspect of the protection of personal information.

### 7.1. Collection of information

- 7.1.1. The club collects information to support its service delivery mandate.
- 7.1.2. Personal information is collected directly from data subjects where practical, and always in compliance with the POPIA.
- 7.1.3. The club collects the following types of information:
  - a) information about players and their parents/guardians provided by players, their parents and others; and
  - b) information about job applications, employees, volunteers and visitors provided by job applicants, employees, volunteers, visitors and others.
- 7.1.4. The club collects information in several ways, including:
  - a) in person and telephonically;
  - b) from electronic and paper documentation, including job applications, emails, invoices, admission forms, letters to the club, consent forms (for example, admissions, excursions or player support services), the club's website or club-controlled social media;
  - c) through online tools, such as applications and other software used by the club; and
  - d) through any Close Circuit Television cameras located on the club premises (if applicable).

- 7.1.5. The club's primary purpose for collecting personal information about players and their parents is to:
- a) Coach players;
  - b) support players' social and emotional wellbeing;
  - c) fulfil legal requirements, including, to:
    - i. take reasonable steps to reduce the risk of reasonably foreseeable harm to players, employees and visitors (duty of care);
    - ii. make reasonable adjustments for players with disabilities, where applicable; and
    - iii. provide a safe and secure training environment,
  - d) enable the club to:
    - i. communicate with parents about players' club/team matters and celebrate the efforts and achievements of players; and
    - ii. maintain the good order and management of the club,
  - e) enable the league organization or any other authorised persons to:
    - i. ensure the effective management, resourcing and administration of the club;
    - ii. fulfil statutory functions and duties;
    - iii. plan, fund, monitor, regulate and evaluate the league organisation's policies, services and functions;
    - iv. comply with reporting requirements; and
    - v. investigate incidents in clubs and/or respond to any legal claims,
  - f) The club's primary purpose of collecting information about players, members, employees, volunteers and job applicants is to:
    - i. assess applicants' suitability for employment or volunteering;
    - ii. administer employment or volunteer placement;
    - iii. to fulfil various legal obligations, including employment and contractual obligations, occupational health and safety laws and to investigate incidents; and
    - iv. respond to legal claims against the club or the league organisation.

## 7.2. **Classification of information**

7.2.1. Club Chairperson classifies information in accordance with its legal requirements, value, criticalness and sensitivity to unauthorised disclosure, modification or loss.

- a) Personal information is usually classified as RESTRICTED.
- b) Special personal information and children's information is usually classified as CONFIDENTIAL.

## 7.3. **Use of information**

7.3.1. When personal information is accessed and used, it can be at the greatest risk of loss, corruption or theft. Therefore:

- a) When working with personal information, employees should ensure that **the screens of their computers are locked** when left unattended.
- b) Personal information should **not be shared informally**.
- c) All personal information sent via **email** (as an attachment or in an email text) should be considered sensitive and protected as such. It should not be sent to someone outside of the club unless it has been cleared by the information officer. This includes forwarding such emails to an employee's own personal email account.
- d) Before sending an email to a co-employee confirm with the information officer that the recipient is allowed to have access thereto as not all users within the club have access to the same information.
- e) Data must be **encrypted before being transferred electronically**.
- f) Personal information should **never be transferred outside of South Africa** without confirmation that the country where it is transferred to can ensure an adequate level of protection of personal information.
- g) Employees **should not save copies of personal information of data subjects to their own computers**. Always access and update the central copy of any personal information.

## 7.4. **Storage of information**

7.4.1. These principles describe how and where personal information should be safely stored. Questions about storing personal information safely can be directed to the information officer/deputy information officer.

7.4.2. When personal information is **stored on paper**, it should be kept in a secure place where unauthorised persons cannot see or access it. These guidelines also apply to personal information that is usually stored electronically but has been printed for some reason.



- a) When not required, the paper or files should be kept **in a locked drawer or filing cabinet**. Where the information is classified as **CONFIDENTIAL**, access to the information should be **restricted** and logged.
  - b) Employees should ensure that paper and printouts are **not left where unauthorised persons could see them**, such as on a printer or photocopier machine.
  - c) **Printouts that contain personal information should be shredded immediately** and disposed of securely when no longer required for the intended purpose.
- 7.4.3. When personal information is **stored electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:
- a) All electronic storage requires access controls equal to those in production, and file protection mechanisms such as **encryption** should be employed.
  - b) All electronic access must be **logged**.
  - c) Personal information should only be stored on **designated drivers and servers** and should only be uploaded to **approved cloud computing services**.
  - d) Storing personal information on any other physical devices, including but not limited to Universal Serial Bus (USB), flash drives (memory sticks), external hard drives, Compact Discs (CDs) or Digital Video Discs (DVDs) must be **pre-approved** by the information officer or his/her delegate.
  - e) If personal information is **stored on removable media** (like a memory stick, external hard drive, CD or DVD) the files should be encrypted, password protected, and the media should be locked away securely when not being used.
  - f) USB flash drives (memory sticks) that are found or have been handed out as a promotional item should not be plugged into any computer as these devices may contain hidden malware or viruses.
  - g) All lost or stolen devices (including removable media) must immediately be reported to the information officer.
  - h) Servers containing personal information should be **sited in a secure location**, away from general office space, where reasonably practicable.
  - i) Electronic files that contain personal information should be **backed up frequently**. These backups should be tested regularly in line with the club's standard backup procedures.
  - j) All servers, computers and other electronic devices containing personal information should be protected by **approved security software and a firewall**.

## 7.5. **Data accuracy**

- 7.5.1. The POPIA requires the club to take reasonable steps to ensure that personal information is kept accurate and up to date.
- 7.5.2. It is the responsibility of all employees who work with personal information to take reasonable steps to ensure that it is kept as accurate and up to date as possible.
  - a) Electronic files that contain personal information should be held in **as few places as necessary**. Employees should not create any unnecessary additional data sets.
  - b) Employees should **take every opportunity to ensure personal information is updated**, for instance, by confirming a person's details when they call.
  - c) The club will make it **easy for data subjects to update their personal information which** the club has control of or has in its possession.
  - d) Personal information should be **updated when inaccuracies are discovered**.

## 7.6. **Disposal**

- 7.6.1. Working papers and copies that may be disposed of in terms of a general disposal instruction must be disposed of by using a secure disposal container or shredder.
- 7.6.2. Copies of personal information, including special personal information, classified as **CONFIDENTIAL**, that is **stored electronically** must either be permanently destroyed or overwritten.
- 7.6.3. The disposal of all original files and electronic files must be performed in accordance with the club's Records Management Policy.

## 8. **Data subject access requests**

- 8.1. All data subjects whose personal information is held by the club are entitled to:
  - a) ask **what information** the club holds about them, why and with who it is shared;
  - b) ask **how to gain access** to it;
  - c) be informed **how to keep it up to date**; and
  - d) be informed how the club is **meeting its obligations in terms of the POPIA**.
- 8.2. If a data subject contacts the club requesting this information this is called **a data subject access request**.
- 8.3. Data subject access requests should be referred to the information officer/deputy information officer.
- 8.4. The club only provides club reports and ordinary club communications to parents who have a legal right to that information.
- 8.5. In some circumstances, an authorised representative may not be entitled to information about the player. These circumstances include when granting access would not be in the players's best interests, would breach the club's duty of care

to the player, would be contrary to a player's wishes or would unreasonably impact on the privacy of another person.

## **9. Disclosing (sharing) personal information**

### **9.1. Internal disclosure**

9.1.1. In general, personal information is shared within the club where legally permitted for reasonable and appropriate club/league purposes. However, even within the club, access is restricted to those employees or third parties who need access to carry out their assigned functions.

9.1.2. The club discloses information consistent with the POPIA, as follows:

- a) for a primary purpose as set out in paragraph 7.1;
- b) for a related secondary purpose that is reasonable to be expected, for example, to enable the governing body to fulfil its objectives, functions and powers;
- c) with consent, including consent provided on registration and other forms (the information collected will not be disclosed beyond the club/league organisation without consent, unless such disclosure is lawful or reasonable in the circumstances);
- d) when necessary to lessen or prevent a serious threat to
  - i. a person's life, health, safety or welfare; or
  - ii. the public's health, safety or welfare;
- e) when required or authorised by law, for example, to comply with a court order, subpoena or search warrant;
- f) to investigate or report an unlawful activity, or when reasonably necessary for a specified law enforcement purpose, including the prevention or investigation of a criminal offence or serious improper conduct;
- g) for research or club statistics purposes by the league organisation, or any other authorised persons; and/or
- h) to establish or respond to a legal claim.

### **9.2. External disclosure**

9.2.1. External to the club, disclosure is only made pursuant to an agreement, as permitted, or required by law or legal process, or with the consent of the data subject or a competent person, if the data subject is a minor.

9.2.2. The POPIA allows personal information to be shared without the consent of the data subject or a competent person if it involves national security or criminal activities. Under these circumstances the requested personal information will be disclosed. However, the information officer/deputy information officer will ensure that the request is legitimate and in line with the POPIA, seeking assistance from the Information Regulator, where necessary.

### **9.3. Player transfers between clubs**

- 9.3.1. When a player has been accepted at, and is transferring to another club, the club transfers information about the player to that club. This may include copies of the player's club records, except for the player's disciplinary records, including any personal information concerning the player's health, if necessary, to provide special support for a player or to make special arrangements in connection with a player's health.
- 9.3.2. This enables the receiving club to continue to provide for the coaching of the player, to support the player's social and emotional wellbeing and health, and to fulfil legal requirements.

### **10. Notification to data subjects**

- 10.1. The club aims to ensure that data subjects are aware that their personal information is being processed, and that they understand how the personal information is being used, what their rights are in terms of the POPIA and how to exercise their rights.
- 10.2. To these ends, the club has a Privacy Notice, setting out how personal information relating to a data subject is collected and used by the club.
- 10.3. The Privacy Notice is available on request.

### **11. Personal information of children**

- 11.1. The club may not process children's personal information unless:
  - a) the club has the consent of a competent person;
  - b) it is necessary for obligations under the POPIA and other legislation;
  - c) it is required for upholding local and international public law; and/or
  - d) it is necessary for research purposes.

### **12. A word of caution to parents or competent persons**

- 12.1. While laws apply to what the club and third parties can disclose about players, they do not apply to what players or their parents might disclose publicly, which means the parent and the player also have a responsibility to protect the player's privacy. What a parent and/or his/her child posts on social media, for example, could be used by others, including private companies and law enforcement in some cases, and is not protected by the POPIA.

- 12.2. Parents and players must understand and use the privacy tools on any website or application they use for club/at home to limit who can view or access their information (that includes having strong, secure and unique passwords and be sure never to post anything online that they would not want to be shared with others, including law enforcement, the club, tertiary institutions and current or future employers).

### **13. Enforcement**

- 13.1. Non-compliance with this policy by the club's members or employees may result in disciplinary action being taken against them. Consequences may include disciplinary action up and to possible termination of membership or employment, and/or legal proceedings to recover any loss or damage to the club, including the recovery of any fines or administrative penalties imposed by the Information Regulator on the club in terms of the POPIA.
- 13.2. Non-compliance with the policy by any other third-party processing personal information on behalf of the club will be dealt with in accordance with the agreement entered into between the club and such third party. Consequences may include the recovery of any fines or administrative penalties imposed by the Information Regulator on the club in terms of the POPIA.

### **14. Review**

This policy must be reviewed when the need arises or in the case of changed circumstances such as pronouncements by legislation and/or regulations and budgetary constraints.

**Definitions:**

<b>competent person</b>	means any person who is legally competent to consent to any action or decision in respect of any matter concerning a child.
<b>data subject</b>	means the identifiable natural or juristic person to whom personal information relates.
<b>deputy information officer</b>	means a person appointed by the principal of the club in his/her capacity as the information officer.
<b>employee</b>	means anyone, other than an independent contractor, who works for another person or who assists in conducting the business of an employer.
<b>information assets</b>	means the assets the club uses to create, store, transmit, delete and/or destroy information to support its educational activities as well as the information systems with which that information is processed. It includes:

	a) all electronic and non-electronic information created or used to support educational activities regardless of form or medium, for example, paper documents, electronic files, voice communication, text messages, photographic or video images. b) all applications, devices and other systems with which the club processes its information, for example telephones, fax machines, printers, computers, networks, voicemail, email, instant messaging, smartphones and other mobile devices ("ICT assets").
<b>information custodian</b>	means the person responsible for defining and implementing security measures and controls for all ICT assets.
<b>information officer</b>	means the principal of the club.
<b>information owner</b>	means a person responsible for, or dependent upon the business process associated with an information asset.

<b>personal information</b>	<p>means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to</p> <ul style="list-style-type: none"> <li>a) information relating to the race, gender, marital status, nationality, age, physical/mental health, disability, belief, culture, language and birth of the person;</li> <li>b) information relating to the education, medical, financial, criminal or employment history of the person;</li> <li>c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;</li> <li>d) the biometric information of the person;</li> <li>e) the personal opinions, views or preferences of the person;</li> <li>f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;</li> <li>g) the views/opinions of another individual about the person; and</li> <li>h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.</li> </ul>
<b>processing</b>	<p>means any operation or activity or any set of operations concerning personal information, including:</p>

	<ul style="list-style-type: none"> <li>a) the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use;</li> <li>b) dissemination by means of transmission, distribution or making available in any other form; or</li> <li>c) merging, linking, as well as restrictions, degradation, erasure or destruction of information.</li> </ul>
<b>special personal information</b>	<p>means personal information concerning:</p> <ul style="list-style-type: none"> <li>a) the religious or philosophical beliefs, race/ethnic origin, trade union membership, political persuasion, health/sex life or biometric information; and</li> <li>b) the criminal behaviour of a person as it relates to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed by a person or the disposal of such proceedings.</li> </ul>